Как цитировать: Цифровые технологии и право: сборник научных трудов III Международной научно-практической конференции (г. Казань, 20 сентября 2024 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 4. – Казань: Изд-во «Познание» Казанского инновационного университета, 2024. EDN: SDYGLW. http://dx.doi.org/10.21202/978-5-8399-0844-4_4 – 1 CD-ROM. – Загл. С титул. экрана. – Текст: электронный.

For citation: Digital Technologies and Law: collection of scientific papers of the III International Scientific and Practical Conference (Kazan, 2024, September 20) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 4. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2024. EDN: SDYGLW. http://dx.doi.org/10.21202/978-5-8399-0844-4_4 – 1 CD-ROM. – Title from the title screen. – Text: electronic.

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
III Международной научно-практической конференции

20 сентября 2024 г.

г. Казань

В шести томах
Том 4

Казань ▪ КИУ ИЗДАТЕЛЬСТВО «ПОЗНАНИЕ» ▪ 2024

DIGITAL TECHNOLOGIES AND LAW

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

2023, September 22

Kazan

In 6 volumes

Volume 4

Казань ▪ KIU "POZNANIYE" PUBLISHERS ▪ 2024

УДК 004:34(063)
ББК 67с51я43
Ц75

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

Рецензенты:

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

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

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

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

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

Ц75 **Цифровые технологии и право: сборник научных трудов III Международной научно-практической конференции** (г. Казань, 20 сентября 2024 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 4. – Казань: Изд-во «Познание» Казанского инновационного университета, 2024. EDN: SDYGLW. http://dx.doi.org/10.21202/978-5-8399-0844-4_4 – 1 CD-ROM. – Загл. С титул. экрана. – Текст: электронный.

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

ISBN 978-5-8399-0859-8
ISBN 978-5-8399-0844-4 (Vol. 4)

Вошедшие в сборник научные труды приурочены к III Международной научно-практической конференции «Цифровые технологии и право», состоявшейся 20 сентября 2024 г. в Казани в рамках Международного форума Kazan Digital Week 2024, организуемого Правительством Российской Федерации совместно с Кабинетом Министров Республики Татарстан.

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

Научные труды представленного тома 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 на основе достижений цифровых технологий, молодым исследователям-студентам, магистрантам и аспирантам, всем интересующимся вопросами взаимовлияния цифровых технологий и права.

УДК 004:34(063)
ББК 67с51я43

ISBN 978-5-8399-0859-8
ISBN 978-5-8399-0844-4 (Vol. 4)

Научное издание

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов II Международной научно-практической конференции

20 сентября 2024 г.
г. Казань

В шести томах
Том 4

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

Электронное издание

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

Дата подписания к использованию: 13.12.2024. Объем издания 4,3 Мб. Тираж 11 экз. Заказ № 11/2024.
ISBN 978-5-8399-0844-4

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

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 III International Scientific and Practical Conference (Kazan, 2024, September 20) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 4. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2024. EDN: SDYGLW. http://dx.doi.org/10.21202/978-5-8399-0844-4_4 – 1 CD-ROM. – Title from the title screen. – Text: electronic.
ISBN 978-5-8399-0859-8
ISBN 978-5-8399-0844-4 (Vol. 4)

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

The scientific works included in this collection are timed to coincide with the III International Scientific and Practical Conference "Digital Technologies and Law", held on September 20, 2024 in Kazan as part of the International Forum "Kazan Digital Week 2024", organized by the Government of the Russian Federation jointly with the Cabinet of Ministers of the Republic of Tatarstan.

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

The scientific works of this volume reflect the views and approaches formed among young people, mainly students, whose research interest in modern issues of digital technology development in the system of legal relations is noticeably increasing.

Taken together, the ideas and proposals reflected in this multi-volume publication are the key to understanding the intellectual map of meanings that will be of interest to legal scholars and experts in the field of digital technologies; practicing lawyers; representatives of law-making and law enforcement agencies; civil servants and participants in the real sector of the economy, including developers and manufacturers of products based on digital technologies; to young researchers: undergraduates, graduates, and postgraduates; to all those interested in the mutual influence of digital technologies and law.

UDC 004:34(063)
LBC 67с51я43

ISBN 978-5-8399-0859-8
ISBN 978-5-8399-0844-4 (Vol. 3)

Scientific publication

DIGITAL TECHNOLOGIES AND LAW

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

2024 September 20
Kazan

In 6 volumes

Volume 4

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

Electronic publication

Editor-in-Chief *G. Ya. Darchinova*; Editors *G. A. Tarasova*, *E. A. Mannapova*;
Technical Editors *O. A. Aimurzaeva*, *S. A. Karimova*; Cover designer *G. I. Zagretdinova*

Date of signing for usage: 13.12.2024. Volume of the publication 4.3 Mb. Number of copies: 11. Order No. 11/2024.
ISBN 978-5-8399-0844-4

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

СОДЕРЖАНИЕ

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ПРАВОВЫХ ОТНОШЕНИЙ (МОЛОДЕЖНОЕ ПРОСТРАНСТВО НАУКИ)

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ПРАВОВЫХ ОТНОШЕНИЙ (МОЛОДЕЖНОЕ ПРОСТРАНСТВО НАУКИ)

К. Д. Алленова,
студент,
Российский государственный университет правосудия,
Северо-Кавказский филиал

ВЛИЯНИЕ СОЦИАЛЬНЫХ СЕТЕЙ НА УГОЛОВНЫЙ ПРОЦЕСС

Аннотация. В работе рассматривается влияние социальных сетей на уголовный процесс, анализируется, как современные технологии меняют традиционные механизмы расследование и предупреждения преступлений. В последние годы социальные сети стали мощным инструментом коммуникации между людьми, а также новостным ресурсом для граждан, что во многом дало возможность использовать их в качестве источника информации по поиску и поимке преступников.

Ключевые слова: социальные сети, уголовный процесс, расследование преступлений, предупреждение преступлений, Интернет, подозреваемые, потерпевший

THE IMPACT OF SOCIAL MEDIA ON THE CRIMINAL PROCESS

Abstract. This work examines the impact of social networks on the criminal process, analyzes how modern technologies are changing traditional mechanisms for investigating and preventing crimes. In recent years, social networks have become a powerful tool for communication between people, as well as a news resource for citizens, which in many ways made it possible to use them as a source of information on the search and capture of criminals.

Keywords: social networks, criminal proceedings, crime investigation, crime prevention, internet, suspects, victim

Введение. Социальные сети стремительно завоевывают популярность среди населения нашей страны и становятся неотъемлемой частью повседневной жизни. Мы уже не можем представить ни дня без проверки уведомлений в известной социальной сети «ВКонтакте» или пришедших сообщений в популярных мессенджерах [1. С. 151; 6]. Развитие Интернета во многом изменило способы общения [2], обмена информацией и восприятия окружающего нас мира из-за появления различных источников получения сведений, которые, по нашему мнению, сейчас могут носить и негативный характер – в социальных сетях активно распространяется дезинформация. В уголовном процессе эти технологии также становятся важным инструментом расследования преступлений правоохранительными органами. Одним из наиболее заметных аспектов влияния социальных сетей на

уголовный процесс является их использование в качестве источников доказательств.

Основная часть. Важно не забывать, что информация из социальных сетей может быть недостоверной или искаженной, что ранее было уже отмечено. Следствие должно учитывать подлинность данных и то, как эти данные были получены. Примером может являться недавний захват заложников в исправительной колонии № 19 в городе Суровикино Волгоградской области. В социальных сетях активно шло информирование со стороны СМИ о ситуации на месте совершения преступления, и правоохранительные органы внимательно следили за ситуацией в социальных сетях. Однако в Телеграм-каналах также в этот день было опубликовано большое количество неподтвержденной информации, что во многом вводило в заблуждение граждан нашей страны.

Кроме того, социальные сети могут помочь правоохранителям в поиске и поимке особо опасных преступников [10]. 3 апреля 2024 г. произошел террористический акт в «Крокус Сити Холле». Злоумышленники вели общение через мессенджер «Телеграм», и оперативные сотрудники ФСБ России отслеживали всю информацию, которая появлялась в этой социальной сети, что также помогло быстро найти и арестовать преступников. Данная информация была публично раскрыта в средствах массовой информации [8]. В дальнейшем данные из этого источника информации стали доказательствами причастности иных лиц к данному террористическому акту и способствовали привлечению их к уголовной ответственности.

Немаловажно отметить, что социальные сети стали пространством для обсуждения множества вопросов: от того, какой оператор связи предоставляет лучший Интернет, до того, как продвигается расследование уголовного дела. Публичное внимание может заставлять следственные органы действовать более результативно. Приведем в пример поиск пропавшего мальчика Вячеслава Люкшина в Усолье-Сибирском в 2019 г., что было освещено в СМИ [9]. Благодаря повсеместной информации из социальных сетей неравнодушные граждане помогли полицейским найти потерявшегося ребенка быстро и оперативно.

Одним из серьезных последствий активного использования социальных сетей в уголовном процессе является угроза конфиденциальности и нарушения прав человека. Публикация личной информации о подозреваемых до вынесения приговора может привести к самосуду и несправедливому осуждению.

Так, в 2023 г. в средствах массовой информации появилась новость, что виновный по делу «Лесопаркового маньяка» Алексей Корочкин оказался невиновным в совершении преступления, за которое он отбывал наказание 25 лет в тюрьме, так как появились доказательства виновности по этому делу уже умершего человека: «Вдова бывшего сотрудника МВД Александра Болотова после смерти мужа принесла в отделение полиции оружие супруга, поскольку хранить такое наследство дома законно она не могла. Полицейские провели стандартную процедуру и внезапно обнаружили среди оружия тот самый пистолет, из которого лесопарковый маньяк совершал свои преступления». Ранее, в 2004 г., в средствах массовой информации были обсуждения о виновности гражданина Корочкина в данных преступлениях, в результате чего он был осужден и отправлен отбывать наказание в исправительное учреждение.

Также важно рассмотреть возможность использования технологий и аналитику больших массивов данных, которые были выгружены из социальных сетей в расследовании уголовных дел. Правоохранительные органы используют специальные программные средства для мониторинга активности в социальных сетях, что позволяет быстро реагировать на криминальные угрозы [3. С. 265].

В связи с использованием новых технологий возникает необходимость актуализировать законодательство, чтобы обеспечить защиту прав граждан, а также предотвратить возможные злоупотребления со стороны государственных органов [4. С. 354].

Помимо этого, считаю важным осветить вопрос использования преступником социальных сетей в качестве «орудия преступления». Часто онлайн-платформы населены так называемыми онлайн-троллями, которые могут совершать преступления: кибербуллинг, который может привести к ужасным последствиям для жертвы (ст. 110 УК РФ); мошенничество, связанное с инвестициями в Интернете, с такими новейшими валютами, как криптовалюта (ст. 159–159.6 УК РФ). Все это создает новые вызовы для правоохранительных органов, которые должны владеть современными цифровыми технологиями для предотвращения потенциальных преступлений [7. С. 66–72].

Заключение. Таким образом, социальные сети оказывают значительное влияние на уголовный процесс, открывая новые возможности для расследований и получения доказательств. Одновременно с этим они создают новые вызовы, касающиеся приватности, прав человека и соблюдения законности [5. С. 15–25].

Список литературы

1. Абрадова Е. С. Молодежь в социальных сетях // Власть. 2018. Т. 26, № 3. С. 150–153.
2. Елин В. М., Жарова А. К. Правовые аспекты торговли в сети Интернет // Право и государство: теория и практика. 2012. № 10. С. 139–151. EDN: NVSBLB.
3. Бадамшин И. Д., Литвина А. В., Кулиев И. Б. Преступления в сфере информационно-телекоммуникационных технологий: тенденции и противодействие // Евразийский юридический журнал. 2022. № 2(165). С. 265–266.
4. Бурганова Г. В. Использование электронных документов в качестве доказательств в уголовном и гражданском процессе // Вестник гражданского процесса. 2018. № 1. С. 354–361.
5. Головко Л. В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция // Вестник экономической безопасности. 2019. № 1. С. 15–25.
6. Залоило М. В., Власова Н. В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2014. № 5. С. 140–145.
7. Сергеев А. Б. «Цифровое» доказательственное право при производстве по уголовным делам о преступлениях в сфере компьютерной информации: вопросы целесообразности // Юридическая наука и правоохранительная практика. 2022. № 3(61). С. 66–72.
8. Юлия Овчинникова // РБК. URL: https://amp.rbc.ru/rbcnews/politics/28/03/2024/6605094a9a794743ef5caa48 (дата обращения: 28.03.2024)

9. IRK.ru. URL: https://www.irk.ru/news/20190506/search/ (дата обращения: 06.05.2019).

10. Аранда Серна Ф. Х. Социально-правовые риски шерентинга в процессе формирования цифровой идентичности ребенка в социальных сетях // Journal of Digital Technologies and Law. 2024. Т. 2, № 2. С. 394–407. EDN: GBFHOR

Д. Ж. Аманиязова,
студент,
Российский государственный университет правосудия,
Казанский филиал

РОЛЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ В СИСТЕМЕ ПРАВОВЫХ ОТНОШЕНИЙ

Аннотация. В статье рассматривается роль цифровых технологий в системе правовых отношений и анализируется современное состояние правового регулирования в этой области. Обсуждаются проблемы отсутствия единого определения цифровых технологий в законодательстве и правовой доктрине. Выявлены основные характеристики комплексной отрасли права, и проведен анализ на соответствие этим критериям цифрового права. Сделан вывод, что, несмотря на развитие нормативной базы, цифровое право сталкивается с вызовами, связанными с отсутствием единого предмета регулирования. Также в рамках проведенного исследования рассмотрены вопросы потенциального субъектного статуса искусственного интеллекта как особой цифровой технологии. В статье предлагаются направления совершенствования законодательства в контексте цифровизации общества.

Ключевые слова: цифровые технологии, правовое регулирование, цифровое право, нормативно-правовые акты, межотраслевое правовое регулирование, комплексная отрасль права, цифровизация

THE ROLE OF DIGITAL TECHNOLOGIES IN THE SYSTEM OF LEGAL RELATIONS

Abstract. The article examines the role of digital technologies in the system of legal relations and analyzes the current state of legal regulation in this area. The problems of the lack of a single definition of digital technologies in legislation and legal doctrine are discussed. The main characteristics of a complex branch of law are identified and an analysis of digital law compliance with these criteria is conducted. The author concludes that, despite the development of the regulatory framework, digital law faces challenges associated with the lack of a single subject of regulation. Also, within the framework of the study, the issues of the potential subject status of artificial intelligence as a special digital technology are considered. The article suggests directions for improving legislation in the context of the digitalization of society.

Keywords: digital technologies, legal regulation, digital law, regulatory framework, intersectoral legal regulation, complex branch of law, digitalization

Введение. Право по своей природе, как правило, действует ретроактивно в отношении тех социальных отношений, которые подлежат правовому регламентированию. Это означает, что в большинстве случаев сначала развиваются те или иные общественные отношения, подлежащие правовому регулированию, и лишь затем законодатель, реагируя на общественный запрос, устанавливает правовую основу тех или иных отношений.

Вышеуказанная ситуация характерна и для правовой регламентации цифровых технологий. Очевидно, что правовое регулирование таких технологий ретроактивно по отношению к их появлению. Так, например, базисная цифровая технология современности – технология Интернета – получила широкое распространение еще в 1990-х годах, в то время как системное правовое регулирование цифрового пространства пришлось на 2000-е и 2010-е годы [8]. Таким образом, в течение длительного периода времени правовое регулирование Интернета находилось в серой зоне правового регулирования, что привело как к положительным, так и отрицательным последствиям.

Цифровые технологии стремительно меняют различные сферы жизни общества, включая систему правовых отношений. В последние десятилетия мы наблюдаем значительное влияние информационных технологий на правовую сферу, что выражается в автоматизации правовых процессов, внедрении искусственного интеллекта, использовании блокчейна для хранения данных и создании новых цифровых прав. Эти изменения стимулируют трансформацию традиционных правовых институтов, создавая новые вызовы и возможности для правоприменения.

Следует признать, что практически любое правовое регулирование новой технологии в той или иной степени приводит к ограничению скорости развития такой технологии. И, напротив, отсутствие правового регулирования предоставляет полную свободу в развитии той или иной сферы цифровых технологий. В то же время очевидно, что если на первом этапе развития цифровой технологии отсутствие правового регулирования можно считать достоинством, то в дальнейшем такая ситуация может привести к ряду нежелательных последствий.

В рамках данной работы рассмотрим, какую роль играют цифровые технологии в системе правовых отношений на современном этапе развития правового регулирования.

Основная часть. Вместе с тем, по нашему мнению, вся полнота сфер применимых цифровых технологий укладывается в вышеуказанное обозначение, которое может быть имплементировано на законодательном уровне [1, 3, 5].

Исходя из вышеизложенного, правовому регулированию подлежит не сама цифровая технология, а общественные отношения, возникающие из этой технологии. Очевидно, что технология является вторичной, представляя собой исключительно способ достижения того или иного результата, необходимого субъектам правового регулирования. При этом процесс достижения такого результата регламентируется правом лишь в той мере, в которой данный процесс влияет на те или иные общественные отношения.

Это означает, что право не может охватывать все аспекты человеческой деятельности, но должно сосредотачиваться на тех моментах, которые имеют значение для поддержания порядка, защиты прав и свобод граждан, а также обеспечения справедливости в обществе.

Таким образом, право выступает как инструмент, регулирующий взаимодействия между индивидами и группами, устанавливая нормы и правила, которые способствуют гармонии и стабильности. Важно отметить, что правовые нормы должны быть адаптивными и учитывать изменения в общественных отношениях, чтобы оставаться актуальными и эффективными.

Кроме того, правовая регламентация должна быть сбалансированной: она должна защищать интересы всех сторон, минимизируя конфликты и способствуя сотрудничеству. Это требует постоянного анализа и пересмотра действующих норм, а также активного участия общества в процессе их формирования и изменения.

При этом важно учитывать, что вышеуказанный баланс правового регулирования также состоит из нескольких составляющих элементов. Во-первых, данный баланс должен регламентировать соотношение частных и публичных интересов. Очевидно, что права и свободы человека (в том числе в контексте реализации права собственности) могут быть ограничены лишь в минимально необходимой степени для защиты интересов государства и общества, а также иных публично-правовых интересов. Кроме того, правовое регулирование должно защищать интересы частноправовых субъектов в отношениях друг с другом, устанавливая путем как императивно-правового, так и диспозитивного регулирования правила осуществления правоотношений, призванные защищать субъектов соответствующих правоотношений.

Следует отметить, что в системе действующего правового регулирования существует комплекс правовых отношений, возникающих вследствие применения цифровых технологий. Исходя из вышеизложенного, среди исследователей возникают дискуссии относительно возможности и целесообразности выделения комплекса правовых норм, регламентирующих соответствующие правоотношения в отрасль (или, возможно, подотрасль) цифрового права.

В научной доктрине существуют различные мнения относительно возможности признания цифрового права отраслью права, при этом ряд исследователей склоняются к тому, чтобы признать цифровое право комплексной отраслью права [2]. Комплексные отрасли права отличаются от материальных и процессуальных некоторой неоднородностью правовых норм и методов правового регулирования, что приводит к существенному увеличению в последнее время различных комплексных отраслей права. Вместе с тем к такому подходу следует отнестись критически, исходя из следующих соображений.

Комплексная отрасль права характеризуется следующими признаками:

– наличие совокупности нормативных правовых актов, регламентирующих такую отрасль;

– косвенным признаком существования комплексной области права является существование соответствующей учебной дисциплины;

– для комплексной отрасли права характерно межотраслевое правовое регулирование отношений;

– комплексная отрасль права объединена единым предметом правового регулирования. В то же время используемые методы правового регулирования в рамках комплексных отраслей права могут существенным образом отличаться [6].

Рассмотрим вышеуказанные признаки применительно к цифровому праву.

Наличие совокупности нормативных правовых актов, регламентирующих такую отрасль: в рамках цифрового права можно выделить ряд нормативно-правовых актов, регламентирующих данную отрасль. Это в том числе законы о защите персональных данных, кибербезопасности [10], электронной коммерции и интеллектуальной собственности в цифровой среде. Следовательно, можно говорить о соблюдении данного критерия.

Также цифровое право все чаще преподается в вузах в качестве отдельного предмета, что является косвенным признаком существования такой области права. Введение курса цифрового права в учебные программы позволяет студентам лучше понимать, как законодательство адаптируется к новым вызовам, связанным с Интернетом, данными и технологиями.

В условиях стремительного развития технологий, таких как искусственный интеллект и робототехника [3], важно не только изучать существующее законодательство, но и предвидеть возможные изменения и нововведения. Это требует от юристов гибкости мышления и способности адаптироваться к новым условиям. Таким образом, цифровое право становится неотъемлемой частью юридического образования, что подчеркивает его значимость в современном обществе и необходимость подготовки специалистов, способных эффективно работать в этой области.

Можно также согласиться с тем, что цифровое право является ярким примером межотраслевого правового регулирования, поскольку включает нормы из различных областей права: гражданского, административного, уголовного и международного частного права. Оно регулирует отношения, пересекающие традиционные границы отраслей [12. С. 140–142], что является характерной чертой комплексных отраслей права.

Комплексная отрасль права объединена единым предметом правового регулирования, но методы могут различаться: данный критерий, по нашему мнению, является наиболее проблемным. Все комплексные отрасли права (например, спортивное право либо земельное право) основаны, прежде всего, на единстве предмета, в рамках которого формируются те или иные правоотношения. Так, например, предметом спортивного права являются спортивные отношения, а предметом земельного права, соответственно, земельные. В то же время предметом условного цифрового права могут быть спортивные, земельные, трудовые, гражданские и иные правоотношения. Таким образом, возникает логичный вопрос, имеет ли цифровое право свой предмет либо же является лишь специфическим способом осуществления правоотношений.

По сути, цифровое право связано в большей степени с технологическими способами реализации прав на объекты, регламентируемые другими сферами законодательства, чем имеет собственный предмет правового регулирования. С дальнейшей цифровизацией общества сфера применения цифрового права постоянно бы расширялась. Именно разнообразие предметов правового регулирования (от электронной торговли, до блокчейна, криптовалюты, доменных имен или искусственного интеллекта) не позволяет выделять цифровое право в качестве единой отрасли права, так как очевидно, что дальнейшее расширение цифровых технологий может привести к тому, что, по сути, практически все правовое регулирование можно будет считать «цифровым правом».

В то же время совокупность цифровых правоотношений активно развивается в рамках разных отраслей права. Поэтому можно согласиться с мнением исследователей, «относящих цифровое право к категории объективно существующей правовой реальности» [7].

Предметом правового регулирования являются только правовые отношения, которые складываются в сфере тех или иных технологий, ситуация может кардинальным образом измениться с широким развитием искусственного интеллекта (далее – ИИ).

В условиях быстрого прогресса в области искусственного интеллекта возникает необходимость пересмотра существующих правовых рамок. ИИ может не только изменять характер правовых отношений, но и создавать новые, ранее не существовавшие правовые вызовы.

Уже на сегодняшний день в научной доктрине ведется дискуссия относительно возможного признания искусственного интеллекта субъектом права. Так, как отмечает М. И. Хохлова, если такая правовая фикция, как юридическое лицо может быть субъектом права, то вполне возможно, что субъектом права можно признать и искусственный интеллект [9].

Следует отметить, что одной из основных причин субъективизации юридического лица стала необходимость разграничения юридической ответственности [10]. Для частноправовых отношений и для большинства организационно-правовых форм справедливым представляется утверждение об ограниченной ответственности участников (собственников) юридического лица за действия такого лица. Подобная проблема может возникнуть и в сфере искусственного интеллекта: очевидно, что существующие системы искусственного интеллекта значительным образом усложняются, а их разработчики имеют весьма ограниченный контроль за деятельностью искусственного интеллекта.

Вместе с тем ряд исследователей обоснованно возражают против наделения искусственного интеллекта правосубъектностью. Так, как отмечает М. С. Зуйкова, наделение искусственного интеллекта правосубъектностью невозможно по следующим причинам: современный искусственный интеллект лишь имитирует когнитивные способности человека, несмотря на то обстоятельство, что такая имитация становится все более и более правдоподобной. На сегодняшний день, наиболее распространенным является искусственный интеллект на основе нейросетей. Принцип действия программ такого рода состоит в анализе огромного массива данных и выработке ответов на основании такого массива данных, в то время как высшие когнитивные функции на данный момент недоступны даже наиболее развитым программам искусственного интеллекта.

Искусственный интеллект не обладает таким важным критерием правоспособности, как деликтоспособность [4, 5]. Очевидно, что искусственный интеллект не может нести самостоятельную ответственность за совершенные им действия, вследствие чего его субъективизация будет лишена важнейшей составляющей – юридической ответственности. Последняя будет осуществляться, возможно, на принципах страхования рисков; кроме того, по аналогии с владельцем источника повышенной опасности юридическая ответственность может быть возложена на владельца и (или) создателя соответствующего цифрового субъекта.

Таким образом, несмотря на то обстоятельство, что на сегодняшний день вопрос субъектного статуса искусственного интеллекта выглядит преждевременным [11], существуют все основания считать, что дальнейшее его развитие может привести к изменению позиций в научной доктрине и законодательстве по этому вопросу, что кардинально изменит всю парадигму субъектного состава правовых отношений.

Заключение. Цифровые технологии стремительно развиваются, охватывая все новые сферы правоотношений. Вместе с тем при рассмотрении вопроса правового регулирования необходимо помнить, что регулированию подлежит не сама цифровая технология, а отношения, возникающие на ее основе.

Существенным недостатком действующего правового регулирования является отсутствие законодательного определения понятия цифровой технологии. Исходя из вышеизложенного, нами предложено понятие цифровой технологии как совокупности методов, инструментов и процессов, которые используют цифровые данные для создания, хранения, обработки и передачи информации. Данное понятие является универсальным, а его имплементация в действующее правовое регулирование позволит осуществить четкую регламентацию данного понятия.

Проблемным аспектом остается вопрос признания цифрового права отдельной отраслью права. По нашему мнению, на сегодняшний день цифровое право не может быть признано комплексной отраслью права в связи с тем, что оно не имеет единого предмета правового регулирования и неразрывно связано с цифровой технологией как способом реализации тех или иных общественных отношений. Очевидной правовой проблемой является также разнородность потенциальных цифровых технологий, что также затрудняет их объединение в рамках того или иного единого базиса. Комплексной отраслью права можно признать лишь «интернет-право», однако данное понятие является намного более узким по сравнению с цифровым правом. Так, интернет-право регламентирует комплекс правоотношений, связанных с функционированием самой сети Интернет (например, правоотношения, связанные с доменными именами, организацией доступа в Сеть и т. д.). Очевидно, что такие правоотношения имеют свой отдельный предмет, и, соответственно, интернет-право может признаваться отдельной нормой права.

Также следует отметить, что цифровые технологии отличаются чрезвычайно высокой скоростью развития. При этом некоторые из таких технологий, как, например, искусственный интеллект, приводят к научным дискуссиям относительно изменения самих основ правоотношений и расширению субъектного состава таких правоотношений. Несмотря на спорность данных правовых позиций на нынешнем этапе развития как данной технологии, так и правовой науки, невозможно отрицать потенциальное изменение вышеуказанного правового регулирования в будущем.

Вместе с тем, по нашему мнению, отсутствие места для цифрового права в системе комплексных отраслей права не означает отсутствие необходимости развития законодательства, регулирующего применение цифровых технологий.

Список литературы

1. Банакас С., Петров Д. А., Попондопуло В. Ф., Силина Е. В. Цифровые отношения как предмет правового исследования // Вестник СПбГУ. Серия 14. Право. 2023. № 2.
2. Грудцына Л. Ю. Цифровое право как комплексная отрасль российского законодательства // Образование и право. 2023. № 3.
3. Бегишев И. Р. Криминологическая классификация роботов: риск-ориентированный подход // Правоприменение. 2021. Т. 5, № 1. С. 185–201. EDN: TBUVGY
4. Бегишев И. Р. Искусственный интеллект и робототехника: глоссарий понятий / И. Р. Бегишев, З. И. Хисамова. М.: Проспект, 2021. 64 с. EDN: HQELSK
5. Ковалевич И. О. Понятие и содержание цифровых технологий и цифровых прав в законодательстве России // Образование и право. 2023. № 3.
6. Коваленко А. Ю. К вопросу о признании комплексных отраслей права // Вестник Московского университета МВД России. 2015. № 5.
7. Курманалинов Е. Ж. Становление и развитие цифрового права в эпоху глобализации в Российской Федерации и Республике Казахстан: к постановке проблемы // Аграрное и земельное право. 2019. № 12(180).
8. Магомадова Э. И., Саркарова М. М. Правовое регулирование сети Интернет. Сеть Интернет: ее архитектура // Журнал прикладных исследований. 2023. № 7.
9. Хохлова М. И., Проскурина Д. С., Сафин Н. И. Искусственный интеллект как субъект права // Право и государство: теория и практика. 2020. № 1(181).
10. Bokovnya A. Yu. et al. Motives and Objectives of Crime Commission Against Information Security // Ad Alta. 2020. Vol. 10, № 2 S13. Pp. 7–9. EDN: SCSEBN
11. Бегишев И. Р. Криминологическая классификация роботов: риск-ориентированный подход // Правоприменение. 2021. Т. 5, № 1. С. 185–201. EDN: TBUVGY
12. Смена технологических укладов и правовое развитие России: монография. М.: ИЗиСП: Норма: ИНФРА-М, 2024.

О. К. Антропцев,
студент,
Московский государственный юридический
университет имени О. Е. Кутафина (МГЮА)

НЕЙРОСЕТИ – ВОЗМОЖНОСТИ ИЛИ УГРОЗА ДЛЯ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ?

Аннотация. Развитие нейросетей приобрело стремительный характер и охватывает с каждым днем все больше сфер. В настоящей статье рассматриваются два подхода к определению значения нейросетей с точки зрения их потенциала для государственного управления. В исследовании обосновано, что на совре-

менном этапе нейросети следует рассматривать именно как инструмент повышения эффективности государственного управления, который имеет ряд преимуществ, но и отдельные недостатки.

Ключевые слова: алгоритм, государственное управление, искусственный интеллект, машинное обучение, нейронные сети, субъект государственного управления, цифровые технологии, государственное управление

NEURAL NETWORKS - OPPORTUNITY OR THREAT TO PUBLIC ADMINISTRATION?

Abstract. The development of neural networks has become rapid and covers more and more spheres every day. In this article, the author considers two approaches to determining the place of neural networks from the point of view of public administration. The study substantiates that at the present stage neural networks should be considered precisely as a tool for improving the efficiency of public administration, which has a number of advantages, but also some disadvantages.

Keywords: algorithm, public administration, artificial intelligence, machine learning, neural networks, public administration subject, digital technologies, public administration

Введение. Мир сделал огромный шаг в направлении создания и развития искусственного интеллекта, машинного обучения и нейронных сетей за последние пару лет. Казалось бы, несколько десятилетий назад было сложно представить, что человечество сможет создавать изображения всего за несколько секунд, лишь вводя текст, у людей будет универсальный консультант, который сможет создавать решения казусов любой сложности, нейросети, которые будут помощником в бесчисленном множестве сфер деятельности людей, в том числе и в государственном управлении, а иногда и заменять человека.

Наука не стоит на месте, множество ученых работают над развитием и совершенствованием технологий. В настоящее время представлено значительное количество разнообразных нейронных сетей, которые могут оказать содействие в разрешении все более сложных задач.

Перед государством во все времена стоит вопрос по обеспечению эффективного государственного управления, поиску путей прогнозирования развития и последствий принимаемых тех или иных управленческих решений. Нейросети могут также использоваться и в государственном управлении. При этом возникает закономерный вопрос: нейросети – возможности или угроза для государственного управления [7, 11]?

Основная часть. Попробуем определиться с понятием нейронных сетей. Приведем несколько определений. Нейронная сеть – это программа или модель машинного обучения, которая принимает решения аналогично человеческому мозгу, используя процессы, имитирующие совместную работу биологических нейронов для поиска явлений, оценки вариантов и принятия решений. Таким образом, «фактически нейронная сеть – это технология, которая работает аналогично человеческому мозгу, в основе которого заложены технологии искусственного интеллекта и машинного обучения» [13].

На самом деле история нейросетей начинается не в XXI веке и даже не в XX, а еще в XIII веке. В течение всего существования человечества исследовался вопрос мышления, и Раймунд Луллий был первым, кто выдвинул теорию о том, что мышление фактически можно имитировать механическим путем [3. С. 52]. Спустя множество длительных исследований первые крупные шаги были сделаны уже в середине XX века. В 1943 г. у Уоренна Маккалока и Уолтера Питтса выходит статья, где описывается работа нейронов, а также была создана и описана первая модель простой нейронной сети с использованием электрических целей [10]. Позднее Алан Тьюринг предлагает тест, который предполагал, что в итоге искусственный интеллект нельзя будет отличить от настоящего человека [3. С. 53]. Кунихито Фукусима в 1975 году разработал первую настоящую многослойную нейронную сеть [8].

Современные нейронные сети активно развиваются, что расширяет возможности их применения как во всех отраслях народного хозяйства, так и в сферах жизни.

Вопрос применения технологий в государственном управлении стоит очень остро, поскольку возможности их применения безграничны, но и риски в том числе присутствуют в силу отсутствия четкого понимания человеком механизма их функционирования и алгоритмов принятия решений [14]. Если вернуться к теории нейронных сетей, то они в перспективе могут ничем не отличаться от человека при принятии решения и высока вероятность того, что они превзойдут людей, что вызывает вопросы о потенциальной угрозе.

В теории административного права категория «государственное управление» рассматривается в двух аспектах:

– как деятельность совокупности всех ветвей власти, т. е. акцент делается именно на «общую функциональную характеристику государственной власти» [5], на все ветви власти распределяются те функции, которые должно выполнять государство, на характерности отдельных функций многим органам [1. С. 24];

– как деятельность исключительно исполнительной ветви власти [4. С. 185–186].

Государственное управление, по мнению Г. В. Атаманчука, заключается в «практическом, организующем и регулирующем воздействии государства на общественную и частную жизнедеятельность людей в целях ее упорядочения, сохранения или преобразования, опирающееся на его властную силу» [2. С. 62].

Представляется, что нейросети применительно к государственному управлению можно рассматривать, с одной стороны, как инструмент, который позволяет повысить эффективность государственного управления, с другой – как субъект управления.

В настоящее время нейронные сети и искусственный интеллект уже применяются для аккумулирования и обработки огромных массивов данных, но это лишь верхушка айсберга. Правительства всех стран мира заинтересованы в изучении возможности нейросетей и их использования как инструмента государственного управления для более эффективного решения задач, стоящих перед государством. Приведем примеры использования нейросетей в зарубежных странах и полученных результатах:

– Федеральная государственная служба здравоохранения использует нейросети для прогнозирования уровня инфекций, заполненности больничных коек, обеспечивает пропускную способность больниц;

– в Джакарте органы власти используют алгоритмы для прогнозирования наводнений в реальном времени на основе сбора и анализа информации из 1500 датчиков;

– Государственная служба надзора за гидротехническими сооружениями Нидерландов применяет для проведения аналитики в реальном времени для принятия наиболее эффективных решений по поддержке инфраструктуры и решения водных проблем [6];

– Служба доходов Джорджии использовала синтетический генератор данных, функционирующий на основе алгоритма и статистических методов для имитации данных реальных налоговых операций, в который были размещены данные налогоплательщиков, и модель выявила лиц, которые могут потенциально уклоняться от уплаты налогов с точностью 63 % [9];

– в Пекине нейронные сети использовались для применения мер по борьбе с загрязнениями [12].

Оцифровка документов на бумажном носителе – длительный процесс, кроме того, различается уровень технической оснащенности граждан, не у всех есть смартфоны, компьютеры и возможность в электронном виде взаимодействовать с государством. Это обусловило поиск новых способов оцифровки информации, которыми стали оптическое распознавание символов и обработки естественного языка. Нейросети как раз и становятся таким инструментом. При этом если обратить внимание на приведенные примеры, можно выделить следующие преимущества использования нейросети государственными органами при выполнении возложенных на них задач:

– извлечение из различных источников неструктурированной информации и данных с последующим их упорядочиванием и аналитики, а также принятия соответствующих управленческих решений, делать их прозрачными;

– на основе извлеченных данных составлять прогнозные модели, моделировать результаты принятия различных управленческих решений;

– преобразовывать сложные данные в доступный графический интерфейс, понятный населению, т. е. людям без каких-либо специальных знаний.

Внедрение нейросетей в государственное управление требует понимания и прозрачности принимаемых алгоритмом решений и прогнозов, наличия возможности контролировать их функционирование. Необходимо наличие четкого понимания, чем именно руководствуется нейросеть при предоставлении решений, ответов.

Соответственно, нейронные сети могут собирать информацию, анализировать ее и предлагать для органов государственной власти возможные пути решения для каждой из ситуаций, в том числе и выявлять проблемные зоны, которые требуют внимания со стороны государства. Подобное применение нейросетей будет способствовать более эффективной деятельности органов публичной власти, но в то же время для принятия решения все еще необходимо участие человека, и роль нейронных сетей скорее должна заключаться в использовании ее как инструмента.

Представляется, что принятие отдельных управленческих решений может быть делегировано нейросетям. В таком случае можно будет рассматривать нейросети как субъект управления, т. е. лицо, возможно, электронное лицо, наделенное полномочиями по совершению управленческого воздействия.

Следует учитывать, что все решения принимаются нейронными сетями, базируясь исключительно на рационализме и логике. У данного подхода есть ряд преимуществ и недостатков. Если первым является возможность избежать коррупции, потери части данных, недостаточный объем проанализированной информации, исключение субъективизма при принятии решения, то ко вторым следует отнести необходимость восприятия человека как живого существа, понимания его жизни как высшей ценности. Например, решение, которое может спасти человеческие жизни, поставив их выше стоимости имущества или затрат на их спасение. Представляется, что именно в выделенном недостатке использования нейронных сетей и содержится главное противоречие в выборе ответа за или против использования нейронных сетей в государственном управлении, т. е. в отношении человека к действительности, его личному восприятию мира и конкретной ситуации. Кроме того, необходимо обратить внимание на еще один риск. Нейросети в силу их способности к быстрым темпам обучения могут выйти из-под контроля человека и выдавать, и реализовывать решение не в пользу, а во вред человека, что также свидетельствует об осторожном их применении и необходимости оценки.

Нейронные сети в настоящий момент лишены восприятия мира в человеческом понимании и до этого еще далеко, поэтому в ближайшей перспективе они не смогут заменить человека, но могут стать неотделимой частью набора инструментов, которые используются публичными органами для повышения эффективности публичного управления и решения задач, стоящих перед государством.

Заключение. В результате проведенного исследования можно сделать вывод, что нейронные сети, по крайней мере, в настоящее время следует рассматривать именно как инструмент, способный повысить качество государственного управления. Использование нейросетей открывает действительно новые возможности, о чем свидетельствуют отдельные приведенные примеры их использования на практике.

В то же время необходимо обратить внимание, что использование нейросетей должно находиться под контролем человека и использоваться после проведения критической оценки, что связано с отсутствием четкого понимания человеком, каким образом нейросеть приходит к тем или иным выводам, своего рода непрозрачность алгоритма. Данный риск создает угрозу для причинения вреда жизни и здоровью человека, а также интересам государства.

Список литературы

1. Административное право: учебник / Б. В. Россинский, Ю. Н. Старилов. М.: Норма: ИНФРА-М, 2020. 640 с.

2. Атаманчук Г. В. Теория государственного управления. М., 2004. 525 с.

3. Горбачевская Е. Н., Краснов С. С. История развития нейронных сетей // Вестник Волжского университета имени В. Н. Татищева. 2015. № 1(23). С. 52–56.

4. Попов Л. Л., Мигачева Е. В., Тихомиров С. В. Государственное управление в России и зарубежных странах: административно-правовые аспекты / под ред. Л. Л. Попова. М., 2012. 320 с.

5. Уманская В. П., Малеванова Ю. В. Государственное управление и государственная служба в современной России: монография. М.: НОРМА, 2020. 176 с.
6. Analytics for government and the public sector. URL: https://www.sas.com/content/dam/SAS/documents/product-collateral/industry-overview/en/analytics-for-government-and-public-sector-113116.pdf (дата обращения: 01.08.2024)
7. Artificial Neural Network: what they are & why they matter. URL: https://www.sas.com/en_hk/insights/analytics/neural-networks.html (дата обращения: 01.08.2024).
8. Fukushima K. Cognitron: A self-organizing multilayered neural network // Biol. Cybernetics. 1975. № 20. Pp. 121–136. URL: https://doi.org/10.1007/BF00342633 (дата обращения: 01.08.2024).
9. Okahashi A., Blanco C. How is the World Bank using AI and Machine Learning for Better Governance? URL: https://blogs.worldbank.org/en/governance/how-world-bank-using-ai-and-machine-learning-better-governance (дата обращения: 01.08.2024).
10. Warren S. McCulloch, Walter Pitts A logical calculus of the ideas immanent in nervous activity // Bulletin of Mathematical Biophisics. 1943. № 5. Pp. 115–133. URL: https://marlin.life.utsa.edu/mcculloch-and-pitts.html (дата обращения: 01.08.2024).
11. Бегишев И. Р. Криминологическая классификация роботов: риск-ориентированный подход // Правоприменение. 2021. Т. 5, № 1. С. 185–201. EDN: TBUVGY
12. Yuan G., Yang W. Evaluating China's Air Pollution Control Policy with Extended AQI Indicator System: Example of the Beijing-Tianjin-Hebei Region // Sustainability. 2019. № 11. 939 p. URL: https://www.mdpi.com/2071-1050/11/3/939 (дата обращения: 01.08.2024).
13. Джабир Х., Лагтати К., Поэ-Токпа Д. Этическое и правовое регулирование использования искусственного интеллекта в Марокко // Journal of Digital Technologies and Law. 2024. Т. 2, № 2. С. 450–472. EDN: FSFSNQ
14. Концепция цифрового государства и цифровой правовой среды: монография. М.: ИЗиСП: Норма: ИНФРА-М, 2024.

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

ЦИФРОВЫЕ ПРАВА И НАСЛЕДНИКИ

Аннотация. В современных реалиях человек как субъект, вне зависимости от его пола, национальности и прочего, сталкивается с различными правоотношениями, в том числе и с цифровыми. Если посмотреть на несколько десятков лет назад, то никто не мог подумать не то что о необходимости регулирования цифровых прав, не было даже и самих цифровых технологий, что говорит о совершенно недавно созданном новом предмете. К цифровым технологиям можно отнести

большой круг интересов, начиная от секрета технологических процессов, операционных программ для оборудований и заканчивая цифровыми технологиями для поддержания электронных сайтов. То есть круг интересов затрагивается большой, в котором присутствуют и различные государства, юридические и физические лица.

Ключевые слова: право, цифровые технологии, цифровые игры, аккаунты, технологии, наследство, последствия

DIGITAL RIGHTS AND HEIRS

Abstract. In modern realities, a person, as a subject, regardless of his kind, gender, nationality, is faced with various legal relations, including digital ones. If you look a few decades ago, no one could even think about the need to regulate digital rights, there was not even digital technology itself, which indicates a completely newly created new subject. Digital technologies include a wide range of interests, ranging from the secret of technological processes, operating programs for equipment, to digital technologies for maintaining electronic sites. That is, the range of interests is affected by a large one, in which various states, legal entities and individuals are present.

Keywords: law, digital technologies, digital games, accounts, technologies, inheritance, consequences

Введение. По мере совершенствования цифровых технологий и самой цифровизации у правотворческих органов возникает вопрос о необходимости урегулирования данной области отношений [1, 2, 4], так как происходят различного рода противоправные действия, которые влекут большие неприятности.

Основная часть. Существует проблема в урегулировании игровых сайтов и самих компьютерных и иных цифровых игр [3, 5], так как игроки, все те субъекты правоотношений, вкладывают туда деньги, время и все другие возможные ресурсы. Изучая нормативную базу того или иного игрового сервера, можно встретить особенности в правилах, к которым относится запрет:

– на допуск иного лица к аккаунту, в случае наступления такого события аккаунт попадает в вечный бан. То есть все достижения, все денежные средства, вложенные лицом, теряются и пропадают;

– на проявление индивидуализации в целях сохранения стабильности среди игроков. В данном пункте правил можно найти в основном дискриминацию российских игроков, ведь за флаги иных государств никто никого не наказывает.

Данные правила были приведены как самые цепляющие и негативные для игроков, в частности игроков Российской Федерации. Говорить про цензуру чата и существующие оскорбления как государства и личности нет смысла, ведь по закону это не преследуется, что является негативным последствием неприменения норм права, где они действительно были бы нужны, в целях сохранения стабильности, культуры и другие нематериальных, а в некоторых случаях и материальных ценностей.

Если рассматривать с точки зрения наследственного права и сравнивать его с цифровым правом, возникает вопрос о том, является ли аккаунт в таких играх элементом, попадающим под переход к наследникам. С точки зрения ГК РФ в состав наследства не будут включены: права и обязанности, связанные с личностью

наследодателя, а также права и обязанности как долговые, так и по возмещению вреда. С точки зрения гражданского права, аккаунт не является ни творчеством, ни обязанностью, ни долгом. Рассматривается как инструмент для реализации себя в пространстве с другими игроками. В то же время можно определить как нечто личное для лица, ведь там он создает своего персонажа, которому строит самостоятельно жизнь. С другой стороны, он вкладывает туда денежные средства, как и в недвижимое имущество, которое создает для себя. А в случае передачи другому лицу аккаунт попадает в бан-список. Такая ситуация встречается довольно часто, так как со стороны государства есть нормы, регулирующие общие отношения, с другой стороны, существует группа программистов, создающих ту или иную цифровую игру со своими правилами, не подпадающими под санкции государства.

Заключение. Для решения данных проблем государствам в целом необходимо создать меры пресечения таких действий. Со стороны Российской Федерации необходимо более точно и корректно создать нормы законодательства по урегулированию практически всех сфер применения. Так, с одной стороны, регулируются переписки и сообщества социальных сетей, с другой – отсутствуют цензура и регулирование цифровых игр, в которых никак не меньше осуществляются пропаганда изъятых из гражданского оборота вещей, межрасовые конфликты, унижение чести и достоинства лиц. Необходимо дополнить нормы ГК РФ в сфере наследственного права возможностью завещания аккаунта от цифровых игр, их передачи по закону.

Таким образом, рассмотрев новые дополнения к законодательству в сфере цифровых технологий, государство повысит сохранность существующего или уже переходящего по правилам наследования имущества и сохранит стабильность и нравственность в обществе.

Список литературы

1. Филиппова И. А., Коротеев В. Д. Будущее искусственного интеллекта: объект права или правосубъектность? // Journal of Digital Technologies and Law. 2023. №1 (2). С. 359–386. EDN: IMMOAM. DOI: https://doi.org/10.21202/jdtl.2023.15

2. Ерахтина О. С. Подходы к регулированию отношений в сфере разработки и использования технологий искусственного интеллекта: особенности и практическая применимость // Journal of Digital Technologies and Law. 2023. № 1(2). С. 421–437. EDN: LBWSXW. DOI: https://doi.org/10.21202/jdtl.2023.17

3. Будник Р. А. Риски и перспективы токенизации творчества // Journal of Digital Technologies and Law. 2023. № 1(3). С. 587–611. EDN: XHASAW. DOI: https://doi.org/10.21202/jdtl.2023.25

4. Концепция цифрового государства и цифровой правовой среды: монография. М.: ИЗиСП: Норма: ИНФРА-М, 2024.

5. Пор С. Опыт правового регулирования лутбоксов в различных странах: сравнительный анализ // Journal of Digital Technologies and Law. 2024. № 2(2). С. 345–371. EDN: UXQADO

А. К. Баяндурян,
магистрант,
Балтийский федеральный университет имени Иммануила Канта
А. В. Шевченко,
магистрант,
Балтийский федеральный университет имени Иммануила Канта

ВИРТУАЛЬНОЕ ПРАВОСУДИЕ: ВОЗНИКНОВЕНИЕ НОВЫХ РЕАЛИЙ В ЦИФРОВУЮ ЭПОХУ

Аннотация. Внедрение цифровых технологий в судебную систему значительно изменило работу судов, повысив их эффективность и доступность. Целью исследования являются анализ и оценка влияния цифровизации на современные судебные системы, с особым акцентом на интернет-суды, внедрение искусственного интеллекта и автоматизированных систем правосудия. В данной статье анализируются такие технологические инновации, как электронные слушания, интернет-суды и электронная отчетность. Рассматривается внедрение этих технологий в различных странах, включая разработку Китаем «умных» судов, эксперименты Эстонии с роботами-судьями и проект Швейцарии Justitia 4.0. Отмечаются плюсы и минусы подобных нововведений.

Ключевые слова: электронные слушания, электронный документооборот, виртуальные судьи, интернет-суды, технологические инновации, цифровое правосудие, кибербезопасность

VIRTUAL JUSTICE: THE EMERGENCE OF NEW REALITIES IN THE DIGITAL AGE

Abstract. The introduction of technology into the judicial system has significantly changed the work of courts, increasing their efficiency and accessibility. The aim of the study is to analyze and assess the impact of digitalization on modern court systems, with a special focus on internet courts, the introduction of artificial intelligence and automated justice systems. This article analyzes technological innovations such as e-hearings, internet courts, and electronic reporting. The implementation of these technologies in various countries is examined, including China's development of smart courts, Estonia's experiments with robot judges, and Switzerland's Justitia 4.0 project. The pros and cons of such innovations are highlighted.

Keywords: electronic hearings, electronic document management, virtual judges, internet courts, technological innovation, digital justice, cybersecurity

Введение. В последние годы внедрение технологий в судебную систему изменило работу судов, значительно повысив ее эффективность и доступность. Среди наиболее значимых инноваций – видеоконференции, электронная отчетность и внедрение электронных судей [11]. Видеоконференции позволяют сторонам, свидетелям и даже судьям участвовать в судебных разбирательствах дистанционно, сокращая задержки и расходы на поездки и обеспечивая своевременное отправление правосудия. Электронная отчетность произвела революцию в ведении и доступности судебных документов, обеспечив документирование в режиме

реального времени и упростив поиск информации по делу. Эти достижения не только повышают скорость и удобство судебных процессов, но и помогают поддерживать непрерывность правосудия во все более цифровом мире.

Основная часть. Совет судей РФ определяет ключевые направления и цели для цифровизации судебной системы с целью повышения ее эффективности, доступности и прозрачности. Оптимизация процессов рассмотрения дел, ускорение рассмотрения дел и снижение бюрократической нагрузки за счет внедрения электронных систем и автоматизации рутинных операций. Создание удобных цифровых инструментов для граждан, включая электронные обращения, доступ к судебным материалам и онлайн-сервисы, что позволит обеспечить более широкий доступ к правосудию.

Концепция информационной политики акцентирует внимание на важности прозрачности и публичного доступа в судебных разбирательствах. Совет судей отметил, что достижение информационной открытости требует обеспечения надежной информационной безопасности. Это включает внедрение конкретных ограничений и запретов для защиты конфиденциальных данных.

Задача нахождения баланса между прозрачностью и адекватными мерами защиты стала особенно актуальной. Концепция подчеркивает необходимость согласования принципа открытости судебной деятельности с необходимостью обеспечения информационной безопасности. Этот баланс крайне важен для защиты данных при сохранении доступа для общественности.

В свете растущего объема информации Концепция рассматривает необходимость эффективных решений для хранения данных [1]. Совет судей считает облачное хранилище наиболее подходящим вариантом на сегодняшний день. Указывается, что при условии соответствия облачных сервисов требованиям законодательства в области защиты информации они предлагают несколько преимуществ по сравнению с традиционными методами хранения данных, такими как физические носители или внутренние серверы.

Электронное (виртуальное) слушание представляет собой безбумажный формат проведения судебных заседаний, где все процедуры осуществляются в цифровом виде. В этом случае адвокатам не требуется приносить с собой тяжелые книги и документы для объявления решения, так как решения судьи выводятся на экраны компьютеров или ноутбуков.

Электронный суд – это судебное учреждение, где правовые вопросы рассматриваются с участием назначенных судей, используя передовые технологические средства. Важно отметить, что электронный суд имеет полноценную цифровую инфраструктуру, что позволяет проводить судебные процессы в онлайн-формате.

Электронные и компьютеризированные суды различаются по своей сути. Электронный суд полностью функционирует в онлайн-среде, используя Интернет и современные информационно-коммуникационные технологии для проведения всех судебных процессов. В противоположность этому, компьютеризированный суд представляет собой традиционное судебное учреждение, где в работу интегрированы компьютеры и базовое программное обеспечение, но возможность проведения онлайн-заседаний отсутствует.

Термины E-Hearing и E-Court обозначают цифровые платформы, используемые для проведения различных юридических процедур [2. С. 16]. Эти приложения позволяют:

– обрабатывать иски;

– оплачивать судебные сборы;

– готовить простые иски;

– предоставлять доступ к судебным решениям и другим юридическим услугам, утвержденным Верховным судом;

– реализовывать новые правила для системы E-Litigation.

С введением новых правил система E-Litigation теперь охватывает не только подачу дел, оплату сборов и вызовы сторон, но и обмен ответами, представление доказательств, а также электронную доставку судебных решений. Более того, система обеспечивает возможность участия в судебных процессах через электронные средства, что значительно упрощает и ускоряет процесс правосудия.

Основной целью создания электронных судов является не только упрощение, ускорение и снижение стоимости правосудия, но и удовлетворение потребностей делового сообщества как на национальном, так и на международном уровне. Благодаря электронным судам юристы больше не обязаны лично присутствовать в суде для подачи исков, что значительно экономит время и ресурсы, делая правосудие более доступным и удобным [9, 10].

В 2019 году Пекинский интернет-суд создал специализированный центр для предоставления «умных» судебных услуг в режиме онлайн [3. С. 622]. Этот центр включает:

«– онлайн-центр услуг по ведению умных судебных процессов – платформа для проведения судебных процессов онлайн с использованием передовых технологий;

– мобильный микросуд – приложение, обеспечивающее доступ к судебным услугам через мобильные устройства в любое время и в любом месте;

– виртуальный судья – инновационный инструмент, объединяющий искусственный интеллект и образ реального судьи для предоставления автоматизированных ответов и поддержки в судебных процессах» [3. С. 622].

Интернет-суды обладают широкой компетенцией, охватывающей различные правовые вопросы, связанные с предпринимательской деятельностью в Интернете. В их юрисдикцию входят:

– споры по онлайн-договорам купли-продажи, предоставлению онлайн-услуг и малым финансовым займам;

– дела о нарушении авторских прав в Интернете;

– споры, касающиеся нарушения прав и свобод личности в Интернете;

– споры по ответственности производителей товаров в рамках интернет-торговли и договоров купли-продажи;

– споры о доменных именах;

– административные споры, связанные с взаимодействием с органами власти через Интернет.

Таким образом, интернет-суды – это не просто учреждения, где дела рассматриваются онлайн. Это независимые судебные органы, в которых все процессы

и документы обрабатываются исключительно с использованием цифровых технологий.

Например, в Эстонии в настоящее время проводятся эксперименты с роботом-судьей, предназначенным для разрешения споров, связанных с договорными соглашениями. Аналогичные системы уже используются или внедряются в таких странах, как Франция, Сингапур, Китай и др. Однако, как правило, эти программы выступают в качестве дополнительных инструментов, помогая в первую очередь анализировать судебные документы.

В 2018 году в Аргентине был внедрен робот-судья по имени Prometea [4. С. 212]. Эта система способна в течение 10 секунд анализировать соответствующие судебные документы и выносить решения по различным гражданским и административным делам. Примечательно, что каждое решение, принятое Prometea, получало одобрение местных судей.

Швейцария разрабатывает проект Justitia 4.0, целью которого является создание универсального портала для швейцарской судебной системы [5. С. 17]. В данный момент проект находится на стадии концепции и ожидается, что он будет полностью реализован к 2026 году. В рамках реализации проекта также проводится пересмотр швейцарских кодексов гражданского и уголовного процесса.

Что касается инвестиций в информационные технологии, то в 2018 году примерно 2,78 % бюджета швейцарского правосудия было выделено на компьютеризацию судов. Название Justitia 4.0 заимствовано от термина «Индустрия 4.0», который был представлен немецким правительством на выставке Hannover Fair в 2011 году. Этот термин описывает компоненты четвертой промышленной революции, включая большие данные, автономные роботы, дополненную реальность, аддитивное производство, облачные вычисления, кибербезопасность [7, 8], интернет вещей, интеграцию систем и моделирование.

Важно отметить, что проект Justitia 4.0 реализуется в судебной сфере, которая представляет собой значительные барьеры для инноваций из-за своей консервативной структуры, отклонений от целевых показателей и склонности к избеганию рисков.

Особого внимания заслуживает интернет-суд в Гуанчжоу, который создал «Электронные юридические павильоны» на основе технологии 5G и 4K. Эти павильоны обеспечивают четкое и стабильное изображение рабочего процесса на всех этапах судебного разбирательства. Это значительно повысило эффективность взаимодействия суда с участниками процесса, которые могут находиться в разных странах.

Вице-президент Пекинского интернет-суда Ли Цзинвэй стал пионером в создании интеллектуальных онлайн судебных разбирательств. Под его руководством были внедрены технологии для хранения данных, видеомедиации, управления судебными процессами в режиме реального времени.

В ходе презентации интернет-суда Ли Цзинвэй ответил на вопросы пользователей и прессы. Один из главных вопросов касался возможностей разрешения судебных дел с помощью «виртуального судьи». Ли Цзинвэй пояснил, что виртуальный судья представляет собой комбинацию различных технологий искусственного интеллекта и внешнего образа реального судьи Лю Шухана.

Судья Лю Шухан продемонстрировал возможности виртуального судьи, отметив важность круглосуточной работы Пекинского интернет-суда. Благодаря искусственному интеллекту судебные службы могут продолжать работу 24/7, обеспечивая дополнительную защиту и непрерывное предоставление услуг.

Виртуальный судья выполняет следующие функции:

– отвечает на вопросы сторон, связанные с подачей иска, ответом на иск, процедурой посредничества и другими юридическими вопросами;

– поиск и выдача ответов основаны на базе данных, включающей более 20 тысяч слов и 120 возможных ответов.

Применение мобильного микросуда значительно упростило доступ к судебным услугам. Теперь граждане могут обращаться в суд «в любое время и в любом месте», включая: видеомедиации, аудит, консультационные процедуры.

Эти услуги доступны через мобильное приложение, которое также предоставляет возможность просмотра всех материалов дела, ознакомления с доказательствами, связи с участниками процесса.

Среднее время рассмотрения дела в интернет-судах Китая составляет около 40 дней, а судебное заседание обычно длится 37 минут. Интересно отметить, что почти 80 % истцов в китайских интернет-судах – физические лица и только 20 % – юридические лица. Более того, 98 % вынесенных решений остаются без обжалования, что свидетельствует о высокой удовлетворенности пользователей новыми судебными услугами.

Одним из основных преимуществ системы электронного правосудия является способность справляться с растущей нагрузкой на судебную систему. Объем дел постоянно увеличивается, и для его обработки требуется эффективное решение. Видео-конференц-связь (VC) стала таким решением, позволив значимо сократить время, затрачиваемое на организацию транспортировки заключенных и свидетелей. Эта технология позволяет избежать длительных задержек, связанных с ожиданием перевозки, что особенно важно для своевременного проведения судебных заседаний.

Использование технологий в судебных процессах способствует увеличению количества дел, которые могут быть рассмотрены в ограниченные сроки. Это позволяет заключенным быстрее получать решения по вопросам условно-досрочного освобождения, испытательного срока или других юридических процедур, что делает правосудие более оперативным и доступным.

Отсутствие необходимости личного присутствия и подачи документов в суд существенно экономит деньги и время участников процесса. Видеоконференции требуют лишь единовременных затрат на установку оборудования, которые в дальнейшем окупаются многократно. Это также снижает расходы на транспортировку участников судебного процесса, что особенно важно для людей из различных слоев общества, которые могут не иметь возможности покрыть эти расходы самостоятельно. В итоге судебные процессы проходят быстрее и эффективнее.

Обеспечение безопасности при транспортировке заключенных – сложная задача для полиции. Путешествие из одного места в другое может быть рискованным как для заключенных, так и для свидетелей и полиции. Видеоконференции устраняют необходимость такой транспортировки, значительно снижая риски и обеспечивая безопасность участников судебных процессов.

Термин «электронное судопроизводство» охватывает различные уровни внедрения цифровых технологий в судебный процесс. Это может варьироваться от предоставления доступа к информации о деятельности судов в онлайн-режиме, возможности ознакомления с судебными решениями и подачи отдельных процессуальных документов в электронном виде до полного перехода на безбумажное взаимодействие суда с участниками процесса и организации дистанционного участия в судебных заседаниях. В более узком смысле электронное судопроизводство подразумевает обязательство или право сторон и суда совершать процессуальные действия в электронной форме, как это предусмотрено законом.

На европейском уровне успешно функционирует Европейский портал электронного правосудия (https://e-justice.europa.eu). Этот портал играет ключевую роль в обеспечении прозрачности судебных систем государств – членов ЕС. Он предоставляет гражданам Европейского союза доступ к практической информации о судебных процедурах и системах правосудия на различных языках. Основная цель портала – повышение уровня прозрачности и облегчение доступа граждан к правосудию.

Международный опыт показывает, что многие страны уже начали законодательное регулирование электронного судопроизводства. Этот процесс включал многолетние и комплексные исследования, результатом которых стало создание самостоятельных электронных систем правосудия. Эти системы разработаны с учетом необходимости защиты персональной информации и соблюдения конфиденциальности [6].

Электронные инновации в сфере правосудия оправдывают свое внедрение, поскольку они значительно упрощают процессы и предлагают эффективную модель взаимодействия между гражданами и государственными органами, а также между различными структурами системы правосудия.

Оценка последствий технологических изменений в сфере правосудия, включая использование искусственного интеллекта, должна учитывать баланс между новыми возможностями и потенциальными угрозами, такими как нарушения конфиденциальности, подрыв безопасности и эрозия структур правосудия.

Список литературы

1. Концепция информационной политики судебной системы на 2020–2030 годы // СПС «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_196819 (дата обращения: 02.09.2024).

2. Гертнер А. В. К вопросу об использовании искусственного интеллекта в системе электронного правосудия: pro et contra // Молодой ученый. 2020. № 49(339). С. 211–215.

3. Ruchi Sharma. E-Hearing- Pros and Cons // Legal Express an International Journal of Law. 2020. Vol. 6, Iss. 2. Pp. 16–23.

4. Rusakova E. P. Integration of “smart” technologies in the civil proceedings of the People’s Republic of China // RUDN Journal of Law. 2021. № 25(3). Pp. 622–633.

5. Sousa M., Kettiger D. and Lienhard, A. 2022. E-justice in Switzerland and Brazil: Paths and Experiences // International Journal for Court Administration. 2022. Vol. 13, № 2. Pp. 1–23.

6. Varynskyi V. Use of the “electronic court” service as a means of citizens’access to the judiciary // Lex Humana. 2024. Vol. 16, № 1. Pp. 1–18.

7. Bokovnya A. Yu. et al. Motives and Objectives of Crime Commission Against Information Security // Ad Alta. 2020. Vol. 10, № 2 S13. Pp. 7–9. EDN: SCSEBN

8. Бегишев И. Р. Криминологическая классификация роботов: риск-ориентированный подход // Правоприменение. 2021. Т. 5, № 1. С. 185–201. EDN: TBUVGY

9. Эффективность отправления правосудия в Нигерии в условиях развития цифровых технологий / П. А. Айдоноджи, С. А. Вакили, Д. Аюба // Journal of Digital Technologies and Law. 2023. Т. 1, № 4. С. 1105–1131.

10. Исследования инноваций и цифровой трансформации в правосудии: систематический обзор / П. М. А. Р. Коррейя, С. П. М. Перейра, Ж. А. д. Ф. Билхим // Journal of Digital Technologies and Law. 2024. Т. 2, № 1. С. 221–250.

11. Цифровизация правоприменения: поиск новых решений: монография. М.: Инфотропик Медиа, 2022.

А. Э. Бесперстов,
курсант,
Военный университет имени князя Александра Невского
Министерства обороны Российской Федерации

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ ДОКАЗЫВАНИЯ

Аннотация. В целях исследования проблематики применения законодательства в условиях активной цифровизации в Российской Федерации в статье рассматриваются особенности использования цифровых технологий в процессе доказывания по уголовному делу. Делается вывод о том, что цифровые технологии должны не только облегчать создание доказательств, но и помогать в расследовании, рассмотрении и вынесении приговора по судебным делам. Уголовно-процессуальное законодательство нуждается в модернизации путем внедрения новейших технологий, которые помогут сделать систему правосудия более доступной, открытой и эффективной.

Ключевые слова: цифровые технологии, цифровые права, цифровые данные, цифровые доказательства, процесс доказывания, уголовный процесс

DIGITAL TECHNOLOGIES IN THE PROOF PROCESS

Abstract. In order to study the problems of the application of legislation in the context of active digitalization in the Russian Federation, the article examines the features of the use of digital technologies in the process of proving a criminal case. It is concluded that digital technologies should not only facilitate the creation of evidence, but also help in the investigation, consideration and sentencing of court cases. Criminal procedure legislation needs to be modernized by introducing the latest technologies that will help make the justice system more accessible, open and effective.

Keywords: digital technologies, digital rights, digital data, digital evidence, proof process, criminal procedure

В настоящее время информационные и цифровые технологии оказывают огромное воздействие на процесс раскрытия и расследования преступлений, а электронные доказательства стали новым видом доказательств, при помощи которых обеспечивается установление всех обстоятельств, подлежащих доказыванию.

Цифровые технологии сегодня охватывают весь спектр человеческой деятельности: от личных взаимодействий до технических достижений и недавно электронные носители информации были включены в качестве новой формы вещественных доказательств в уголовно-процессуальный закон России [9]. Как правило, цифровые данные генерируют электронные следы, представляющие собой отдельные видеозаписи расследуемого события, а также камеры видеонаблюдения, цифровые фотографии, видео, аудиозаписи и пр. Цифровые технологии позволяют проводить мониторинг радиоэлектронной установки, проводить исследование записей и разговоров телефонов, получать улучшенные фото- и видеоматериалы, а также космические снимки, что позволяет улучшить процесс доказывания и ускорить возможность принятия решения по судебному делу [3, 6].

Однако объективная реальность такова, что в настоящее время в уголовно-процессуальном законодательстве первоочередное внимание оказывается выявлению актуальных проблем к поиску эффективных решений, связанных с использованием цифровых технологий в судопроизводстве, а виртуальная природа цифровых данных такова, что их можно изменять, уничтожать, модифицировать, поэтому в настоящее время невозможно с достаточной точностью говорить о достоверности полученных цифровых данных [3. С. 461–464].

Любое использование различных цифровых технологий должно ограничиваться обеспечением следственных и судебных действий, направленных на установление объективной истины. В настоящее время количество полученных информационных и электронных данных в ходе того либо иного расследования с использованием цифровых технологий ежегодно увеличивается, поэтому возникает необходимость создания эффективного механизма взаимодействия процесса доказывания и ИТ-технологии, иначе говоря, необходимо выстроить оптимальную модель в системе российского уголовно-процессуального права с использованием цифровых технологий [4].

Цель модернизации уголовного судопроизводства должна включать, во-первых, внедрение новейших информационных технологий, которые помогут сделать систему правосудия более доступной, открытой и эффективной, а во-вторых, совершенствование самого процесса за счет сокращения его излишнего формализма.

В большинстве случаев электронный документ, приобщенный в судопроизводстве, обычно классифицируется на основе материала, который он поддерживает, а не информации, содержащейся в нем. Юридический аспект электронных доказательств не так осязаем, как личные вещи, а скорее основан на информации, содержащейся в электронных доказательствах, а не на каком-либо физическом ве-

ществе или сущности. Представление и сбор электронных данных может привести к проблемам на практике из-за проблем с визуализацией и сбором электронных данных.

Например, в отличие от физической копии, простой снимок экрана интернет-сайта не будет рассматриваться судом как доказательство из-за возможности изменения или удаления данных. Российское процессуальное законодательство не требует критериев достоверности электронных документов, а это означает, что не всегда возможно проверить достоверность документа, а также возможны случаи, когда он не признается законным. Разумеется, данные проблемы требуют дополнительного рассмотрения законности электронных доказательств [1].

Обнаружение мошеннической деятельности является также сложной задачей – несмотря на наличие программ обнаружения мошенничества, существующие инициативы и разработки таких программ все еще находятся в стадии реализации. Все больше и больше стран во всем мире признают опасности, связанные с созданием поддельных компьютеров, заявляя, что такие идеи угрожают их государствам, и работают над регулированием данного вопроса [4].

Важно также сформировать систему использования современных ИТ-инструментов, которые смогут идентифицировать различные методы подделки электронных доказательств и определять, являются ли они подлинными или нет. Спрос на виртуальную реальность растет, особенно с развитием передовой технологии дипфейков, которая позволяет использовать генеративно-состязательные нейронные сети для создания виртуального лица или голоса.

Электронным базам данных судов и правоохранительных органов необходимы электронные базы данных с электронными компонентами, обеспечивающими высочайший уровень защиты от несанкционированного вмешательства извне и эффективный контроль над любыми изменениями в базе данных или хранящейся в них информации.

По нашему мнению, информационные технологии должны не только облегчать создание доказательств, но и помогать в расследовании, рассмотрении и вынесении приговора по судебным делам [2].

Подводя итог, следует отметить, что регулирование на конституционном и законодательном уровнях использования информационных технологий является позитивным шагом на пути к созданию динамичного информационного общества. Законодательство играет решающую роль в регулировании категории цифровых технологий, однако быстрое развитие информационной сферы создает правовые пробелы, которые требуют своего законодательного закрепления.

Список литературы

1. Апостолова Н. Н. Доказывание по уголовным делам с помощью цифровых технологий // Вестник юридического факультета Южного федерального университета. 2023. № 2. URL: https://cyberleninka.ru/article/n/ dokazyvanie-po-ugolovnym-delam-s-pomoschyu-tsifrovyh-tehnologiy (дата обращения: 29.08.2024).

2. Зуев С. В. Цифровое видеопротоколирование в расследовании преступлений: проблемы и перспективы // Технологии XXI века в юриспруденции: материалы Второй международной научно-практической конференции (Екатеринбург, 22 мая 2020 г.) / под ред. Д. В. Бахтеева. Екатеринбург: УрГЮУ, 2020. С. 461–464.

3. Киричек Е. В. Информационно-цифровая сфера общественной жизни: взгляд через призму конституционно-правовой действительности // Труды Академии управления МВД России. 2020. № 4(56). С. 23–29.

4. Макаров А. Исследование облачных хранилищ при расследовании преступлений. URL: https://www.antimalware.ru/analytics/Technology_Analysis/analysis_cloud_storage_investigation_ of_crimes (дата обращения: 29.08.2024).

5. Основы теории электронных доказательств: коллективная монография / А. Н. Балашов [и др.]; под ред. С. В. Зуева. М.: Юрлитинформ, 2019. 400 с.

6. Жарова А. К. Достижение алгоритмической прозрачности и управление рисками информационной безопасности при принятии решений без вмешательства человека: правовые подходы // Journal of Digital Technologies and Law. 2023. Т. 1, № 4. С. 973–993. EDN: OPPOBG. DOI: https://doi.org/10.21202/jdtl.2023.42

7. «Цифровой поворот» в правовых исследованиях / И. Р. Бегишев, А. К. Жарова, Е. А. Громова [и др.] // Journal of Digital Technologies and Law. 2024. Т. 2, № 1. С. 7–13. EDN: IWWUBP

8. Современная зарубежная правовая мысль о новых феноменах цифровой трансформации / И. Р. Бегишев, А. К. Жарова, Е. А. Громова [и др.] // Journal of Digital Technologies and Law. 2024. Т. 2, № 2. С. 257–261. EDN: BPDCHT

9. Цифровизация правоприменения: поиск новых решений: монография. М.: Инфотропик Медиа, 2022.

К. С. Благодыр,
магистрант,
Санкт-Петербургский государственный экономический университет

РИСКИ В ПРИМЕНЕНИИ ЦИФРОВЫХ ТЕХНОЛОГИЙ ОБЩИМ СОБРАНИЕМ АКЦИОНЕРОВ

Аннотация. В эпоху цифровизации начали повсеместно применяться цифровые технологии, и корпоративное управление не стало исключением. Стремясь усовершенствовать процедуру принятия решений общим собранием акционеров, законодатель ввел дистанционное и заочное голосование, которые повлекли проблему с идентификацией субъектов как акционеров, а также проблему с обеспечением неизменности выражения права голоса акционера при принятии решения на общем собрании. Данная работа имеет своей целью найти возможный путь улучшения проведения голосования акционеров и тем самым приблизиться к решению вышеуказанных проблем. Автор приходит к выводу, что идентифицировать акционеров должен проктор как контролирующее лицо в системе прокторинга, которая в настоящий момент используется только образовательными организациями, а обеспечить волеизъявление акционера в неизменном виде будет возможно при использовании системы распределенного реестра.

Ключевые слова: общее собрание акционеров, недостатки блокчейна при голосовании, дистанционное голосование, заочное голосование, риски цифровых технологий, акционеры, право голоса

RISKS IN THE APPLICATION OF DIGITAL TECHNOLOGIES BY THE GENERAL MEETING OF SHAREHOLDERS

Abstract. In the era of digitalization, digital technologies have started to be applied everywhere and corporate governance has not become an exception. In an effort to improve the decision-making procedure of the general meeting of shareholders, the legislator introduced remote and absentee voting, which caused a problem with the identification of subjects as shareholders, as well as a problem with ensuring the invariability of the expression of the shareholder's voting rights when making a decision at the general meeting. This paper aims to find a possible way to improve the conduct of shareholder voting and thus come closer to solving the above problems. The author comes to the conclusion that the identification of shareholders should be done by the proctor in the proctoring system, which is currently used only by educational organizations, and ensuring the expression of the shareholder's will in invariable form will be possible by using the distributed register system.

Keywords: general meeting of shareholders, blockchain disadvantages in voting, remote voting, absentee voting, digital risks, shareholders, voting rights

Введение. Одним из корпоративных прав, удостоверяемых акцией, является право голосовать за принятие или непринятие определенного решения на общем собрании акционеров. Решение по вопросу принимается большинством голосов акционеров, принимающих участие в собрании. Именно поэтому акционеры – владельцы голосующих акций заинтересованы в том, чтобы присутствовать на месте собрания. Другое дело, что люди не властны над обстоятельствами и осуществление ими своих прав может быть затруднено, поэтому законодатель ввел в Федеральный закон «Об акционерных обществах» возможность заочного голосования и голосования с использованием дистанционных технологий. Данные цифровые технологии способствуют снижению материальных, временных и организационных издержек, связанных с осуществлением корпоративных прав [6. С. 61]. Наравне с установленными в законодательстве способами голосования будет рассмотрено использование одной из технологий распределенного реестра. При использовании цифровой платформы возможно возникновение проблем идентификации акционеров, взломов цифровых платформ недобросовестными лицами и фальсификация ими результатов голосования. Именно поэтому изучение рисков в применении цифровых технологий на общем собрании акционеров и мер их предупреждения необходимо на данный момент.

Основная часть. В работах, «посвященных внедрению цифровых технологий в деятельность хозяйственных обществ, в основном освещается проблема идентификации участников голосования и обеспечение достоверности информации при ее передаче» [6. С. 66; 3. С. 34]. Теория рисков цифровых технологий довольно емко раскрыта в работе [10]. Данные проблемы будут рассмотрены и в нашем исследовании, а также будут предложены пути их решения.

Среди исследователей есть различные мнения, как можно улучшить процесс голосования акционеров на общем собрании. Так, Е. В. Ельникова предлагает создать и использовать личный кабинет акционера на сайте общества, голосова-

ние в котором проходит путем заполнения электронной формы бюллетеня в установленное время доступа [6. С. 63]. О. В. Гутников придерживается такой же позиции [4. С. 70], которая соответствует установленному Правительством РФ Плану мероприятий по совершенствованию корпоративного управления. Кроме этого, предложение Е. В. Ельниковой и О. В. Гутникова похоже на осуществление заочного и дистанционного голосования, регламентированного законодательством, и поэтому новизной не отличается.

«Дистанционное голосование – это проведение общего собрания акционеров в форме совместного присутствия акционеров, при котором используются информационные и коммуникационные технологии, позволяющие обеспечить возможность дистанционного участия в нем, без присутствия в месте проведения общего собрания акционеров» [3]. Из легальной дефиниции мы видим, что общее собрание акционеров в форме совместного присутствия все-таки проводится, из чего мы делаем вывод, что дистанционно голосуют те, кто не смог присутствовать на собрании.

Заочное голосование – это участие в общем собрании акционеров посредством отправки бюллетеней заказным письмом, электронным сообщением по электронной почте, или заполнение их электронной формы на указанном в сообщении о проведении общего собрания акционеров сайте в информационно-телекоммуникационной сети Интернет до даты окончания приема бюллетеней. Таким образом, отграничение данных форм голосования друг от друга происходит следующим образом: при определении голосования в заочной форме законодатель не придает значения такому признаку, как фактическое присутствие или отсутствие в месте общего собрания акционеров, либо законодатель имел в виду, что при дистанционном голосовании акционер может участвовать посредством видео-конференц-связи, т. е. он имеет возможность высказать свою точку зрения по тому или иному вопросу на собрании, а при заочном голосовании у него эта возможность отсутствует.

Интересно мнение исследователя В. А. Лаптева по этому вопросу, он отмечает, что существует два условия, при наличии которых можно считать собрание состоявшимся, и это «возможность идентификации и аутентификации акционера, а также наличие технических средств у акционерного общества либо третьих лиц для администрирования данного формата корпоративных процедур» [7. С. 85].

Б. С. Батаева отождествляет данные формы голосования [1. С. 74]. При этом исследователь выделяет разновидности электронного голосования – голосование с помощью технических средств, расположенных в местах проведения собраний акционеров и дистанционное интернет-голосование, которое позволяет присылать бюллетени с компьютера, подключенного к Интернету [1. С. 76].

Общим недостатком проведения дистанционного голосования О. В. Осипенко считает невозможность осуществления прямого диалога между акционерами на месте собрания, акционерами, присутствовавшими в дистанционном формате и в том числе между последними [9. С. 76]. Данный существенный недостаток связан со свойствами современных технических устройств связи: в общем собрании акционеры участвуют посредством цифровых технологий, т. е. опосредованно, они лишены возможности самостоятельно и оперативно выразить свою

точку зрения, из-за технических сбоев существует риск неполучения нужной информации, которая обсуждалась на общем собрании, и другие риски. Так, Арбитражный суд города Москвы рассмотрел дело № А40-264435/2019-104-207 о признании решения общего собрания акционеров незаконным ввиду того, что его акционера не пустили на место проведения собрания. Суд отказал в удовлетворении требований на том основании, что акционеру не препятствовали присоединиться к общему собранию посредством цифровых технологий. Однако совместное присутствие является традиционной формой и если акционер выразил свою волю на участие в общем собрании в виде личного присутствия, тогда данная ситуация должна толковаться как препятствование акционеру в осуществлении им своих прав, так как цифровые технологии на настоящий момент не могут дать те же возможности, что и личное присутствие в общем собрании.

Представляет интерес мнение В. В. Долинской, которая разграничивает дистанционное голосование от заочного ввиду того, что первое – вид присутствия на заседании, а второе – это порядок принятия решения собранием [5. С. 81]. То есть дистанционное голосование на самом деле не голосование, а заседание – дистанционное заседание. Позволим себе не согласиться с В. В. Долинской, п. 11 ст. 49 ФЗ «Об акционерных обществах» устанавливает порядок проведения дистанционного участия, в результате которого может быть принято решение по вопросам, поставленным на голосование.

В. А. Габов также придерживается легального отграничения форм голосования [3. С. 31, 38], при этом он использует в качестве синонима к заочному голосованию слово «электронное». Автор также приводит отграничение форм голосований при избирательном процессе. Поскольку голосование в избирательном праве является одним из основных институтов, необходимо рассмотреть тот опыт, который накоплен в данной сфере. Итак, ученый-правовед отмечает, что электронное голосование осуществляется в месте проведения выборов с использованием специальных устройств, а дистанционное голосование подразумевает голосование не в месте мероприятия [3. С. 30]. В связи с этим он считает, что необходима единая платформа для голосования наподобие тех, что используются в избирательном процессе [3. С. 53]. Например, Общероссийское голосование по внесению изменений в Конституцию РФ в 2020 г. было проведено именно по технологии блокчейна [2. С. 145].

С. В. Пушкарев придерживается мнения, что электронное голосование с использованием технологии блокчейн поможет разрешить проблему вовлеченности акционеров, снизит транзакционные издержки для корпорации и ее участников, а голосование станет более прозрачным и надежным [11. С. 30]. Д. Е. Матыцин, цитируя Л. А. Новоселову в части обязанности акционеров иметь на своем «счете» в распределенном реестре-блокчейн определенное количество единиц – голосующих акций, соглашается с преимуществами голосования с использованием блокчейн [8. С. 168]. Прежде чем принять решение о применении системы распределенного реестра, в том числе блокчейн, при заочном и дистанционном голосовании акционеров, необходимо соотнести положительные стороны блокчейна с отрицательными. Е. В. Былинкина среди преимуществ блокчейна выделяет именно его децентрализацию и закодированность – данные о голосе каждого акционера хранятся не в одном месте, а на нескольких серверах [2. С. 146], в которых каждый

блок информации кодируется с помощью криптографических алгоритмов, и для их изменения потребуются закрытые ключи, которые принадлежат только авторам блока [2. С. 147]. В этом случае изменить результат голосования в одностороннем порядке будет невозможно, что снижает риск искажения результатов голосования. Среди недостатков Е. В. Былинкина выделяет высокую стоимость разработки, внедрения и использования блокчейн-технологии [2. С. 147–148]. Недостатком является и низкая скорость обработки информации, блокчейн биткоин обрабатывает 240 000 транзакций в день [2. С. 148]. Автор не исключает и возможность кибератак на блокчейн [2. С. 148]. Кроме всего вышеперечисленного, блокчейн, хоть и обеспечивает анонимность пользователя при открытости транзакций, но если одному субъекту станет известно о личности пользователя, тогда он сможет увидеть все его транзакции – в нашем случае голоса за то или иное решение на том или ином собрании [2. С. 148]. Это будет существенным недостатком, к примеру, если данные о пользователе получил его конкурент в предпринимательской деятельности, а также если пользователь-акционер проголосовал в противоречие с положением акционерного соглашения и об этом узнали стороны акционерного соглашения.

Таким образом, для акционеров очень важно реализовывать свои корпоративные права, и еще важнее быть уверенными, что их голос на общем собрании будет учтен, а этому способствует технология распределенного реестра, поэтому она станет действенным механизмом голосования для акционеров.

Заключение. Ввиду того, что в корпоративном законодательстве преобладает императивное регулирование, цифровые технологии не могут оперативно использоваться в корпоративном управлении посредством фиксации в уставных документах [6. С. 62], поэтому внедрение законодателем цифровых технологий должно осуществляться заблаговременно [6. С. 62].

Во-первых, исследовав вопрос идентификации участников голосования, можно сделать вывод, что идентификация является условием для надлежащего проведения голосования с использованием цифровых технологий (заочного, дистанционного, на основе системы распределенного реестра).

Данную проблему можно решить посредством проведения прокторинга: проктор посредством видеосвязи удостоверяет соответствие субъекта, изображенного в документе, удостоверяющем личность, субъекту, находящемуся в системе прокторинга. Проктором может выступать нотариус, регистратор или секретарь общего собрания акционеров. Предлагается распространить правила проведения прокторинга образовательными организациями на его проведение общим собранием акционеров в части идентификации субъекта.

Во-вторых, исследовав вопрос обеспечения достоверности информации при ее передаче в процессе голосования, можно сделать вывод, что система распределенного реестра является наиболее действенным способом для осуществления акционерами права голоса, поскольку обеспечивает децентрализованную фиксацию транзакций. Использование данной технологии позволит решить проблему признания решений, принятых на общем собрании акционеров, недействительными, а также подачу в связи с этим необоснованных исковых заявлений акционеров в судебные органы.

Список литературы

1. Батаева Б. С. Развитие корпоративного управления с помощью сервисов электронного голосования // Управленческие науки. 2020. № 2.
2. Былинкина Е. В. Блокчейн: правовое регулирование и стандартизация // Право и политика. 2020. № 9.
3. Габов А. В. Электронное взаимодействие и цифровые технологии в корпоративном управлении акционерным обществом в России // Право. Журнал Высшей школы экономики. 2021. № 2. С. 24–64.
4. Гутников О. В. Тенденции развития корпоративного права в современных условиях // Журнал российского права. 2020. № 8.
5. Долинская В. В. Новеллы гражданского законодательства о собраниях и их решениях // Вестник Университета имени О. Е. Кутафина. 2021. № 11(87).
6. Ельникова Е. В. Использование цифровых технологий при голосовании на общем собрании участников (акционеров) хозяйственного общества // Вестник Университета имени О. Е. Кутафина. 2020. № 7(71).
7. Лаптев В. А. Извещение участников о проведении общего собрания: юридическое значение и последствия // Актуальные проблемы российского права. 2023. № 8(153).
8. Матыцин Д. Е. Правовые конструкции сделок, используемые по особым информационным технологиям для минимизации конфликтов в инвестиционных отношениях // Труды Института государства и права РАН. 2022. № 1.
9. Осипенко О. В. Управление предпринимательскими структурами в России в контексте преодоления коронавирусного карантина // Современная конкуренция. 2020. № 4(80).
10. Бегишев И. Р. Криминологическая классификация роботов: риск-ориентированный подход // Правоприменение. 2021. Т. 5, № 1. С. 185–201. EDN: TBUVGY.
11. Пушкарев С. В. Развитие корпоративного права под влиянием вызовов цифровой эпохи // Инновационные технологии управления и права. 2021. № 1(30). С. 28–32. EDN FZCGQZ.

С. С. Близнякова,
бакалавр,
Санкт-Петербургский государственный университет

ОБЗОР ТРЕНДОВ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ, СВЯЗАННОЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. Статья посвящена анализу современных угроз, которые представляет злонамеренное использование технологий искусственного интеллекта в киберпреступлениях, а также обзору международного сотрудничества по противодействию такого рода преступлениям.

Ключевые слова: киберпреступность, кибербезопасность, злонамеренное использование искусственного интеллекта, уголовное правосудие, Интерпол, ЮНОДК, Будапештская конвенция

OVERVIEW OF TRENDS IN COUNTERING ARTIFICIAL INTELLIGENCE-POWERED CYBERCRIME

Abstract. This article analyses the current threats posed by the malicious use of artificial intelligence technologies in cybercrime, as well as international cooperation to counter such crimes.

Keywords: cybercrime, cybersecurity, misuse of AI, criminal justice, Interpol, UNODC, Budapest Convention

In the last decade, solutions based on artificial intelligence (AI) have deeply integrated in our lives. It is likely that this trend will continue to grow in popularity over the next 10 years: AI solutions are already being integrated not only into routine tasks, but are also widely used in the performance of some particularly important government tasks, such as ensuring national security. Thus, a number of governments uses AI to tackle the challenges of countering (detection and prediction) cybercrime [10]. In addition, machine learning technologies can create AI capable of securing critical infrastructure. Such AI is actively used by the US Department of Energy, which has the most powerful supercomputers in the world to secure critical infrastructure. Moreover, national security and intelligence agencies have recognized the potential of AI technologies to assist in achieving objectives related to national and public security [3]. Today, many governments are successfully working on creation worldwide legislation to regulate particularly sensitive cybersecurity issues.

Since the COVID-19 pandemic, organized criminal groups have significantly enhanced their crime-as-a-service capabilities, allowing them to generate greater financial gains while minimizing the chances of being detected by law enforcement and held accountable for their actions [14]. For example, hackers use AI technologies to scan networks, find vulnerabilities and then attack; resort to social engineering using AI to generate more convincing and personalized phishing emails; and create malware. In general, cybercrime is being democratized as more and more powerful algorithms fall into the hands of inexperienced hackers. It is important to note that the offences continue to involve experienced hackers hired anywhere in the world via Internet.

To counter AI-related cybercrime and obtain cybersecurity as a whole, international applicable instruments are used. Such instruments may be considered as legal frameworks, treaties, agreements, and guidelines established by countries or international organisations that facilitate cooperation, coordination, and effective responses to cybercrime across borders.

The aim of this study is to explore the emerging problem of AI-related cybercrime during 2019-2024, and to analyse global responses to obtain cybersecurity. So, this study revolves around four key objectives:

1. To make a review of AI-powered cybersecurity trends in world;
2. To give possible vectors of strategic partnership between inter-governmental organisations on countering AI-powered cybercrime;
3. To signify international applicable instruments to counter AI-powered cybercrime;
4. To outline the ongoing work of international organisations in terms of international cybersecurity cooperation.

The landscape of digital threats has undergone a profound transformation over the past few decades, driven by technological advancements and the digital interconnectedness of the world. As society increasingly relies on digital technology for communication, commerce, and critical infrastructure, the threat landscape has evolved in complexity and sophistication.

Artificial Intelligence as a Tool

Artificial Intelligence now wields a dual-edged influence reshaping the cybersecurity landscape. This dynamic necessitates continuous innovation in defence strategies to counteract increasingly sophisticated threats. On the attack front, AI is empowering adversaries with more complex methods such as advanced phishing schemes and deepfakes. Noteworthy incidents include a Russian deepfake of the U.S. Ambassador and a deceptive deepfake impersonating a CFO to prompt an HSBC employee to transfer $25 million [18,20]. A report by cybersecurity firm SplashNext reveals a dramatic increase in these tactics: malicious phishing emails rose by 1,265%, and credential phishing surged by 967% since the fourth quarter of 2022 [18]. Cybercriminals are exploiting generative AI tools like ChatGPT to create highly targeted business email compromise (BEC) and other phishing campaigns. And we are already seeing widespread use of other AI tools like voice cloning services to deliver more impactful social engineering attacks. The rapid evolution of these AI-based threats–in speed, volume, and complexity – signals a pressing need for advanced defensive mechanisms in the cybersecurity sector.

Conversely, AI is also bolstering cybersecurity defences. Through automation and sophisticated AI-based security modules, these tools can detect and take the first steps in responding to threats thus helping security teams respond faster and more efficiently, enhancing cybersecurity resilience. There has been an explosion of AI-related security products over the past 12 months, including both tools leveraging AI to help empower security analysts and tools to help protect employees using AI [8]. Long term, AI-powered security services will accelerate threat detection and prediction, alert aggregation, and behavioural analysis, among other capabilities [ibid]. By integrating these advanced technologies, organisations can establish a more robust and proactive defence mechanism against evolving cyber threats, ensuring greater security and resilience in an increasingly digital world.

Ransomware-as-a-Service. Ransomware is a type of malware cybercriminals use to disrupt a victim’s organisation. Ransomware encrypts an organisation’s important files into an unreadable form and demands a ransom payment to decrypt them. Ransom demands are often proportional to the number of systems infected and the value of the encrypted data: the higher the stakes, the higher the payment. In late 2019, attackers evolved their ransomware tactics to include data exfiltration, commonly referred to as a “double extortion” ransomware attack [1]. In these attacks, if victims choose not to pay the ransom to decrypt the data and, instead, attempt to restore the data from a backup, the attackers threaten to leak the stolen data [ibid]. In late 2020, some ransomware attackers added another attack layer with DDoS tactics that bombard the victim’s website or network, creating even more business disruption, thus pressuring the victim to negotiate [ibid]. Ransomware activity alone was up 50% year-on-year during the first half of 2023 with so-called Ransomware-as-a-Service (RaaS) kits, where prices start from as little as $40, a key driver in the frequency of attacks [11]. Most ransomware

attacks now involve the theft of personal or sensitive commercial data for the purpose of extortion, increasing the cost and complexity of incidents, as well as bringing greater potential for reputational damage. According to IBM's X-Force Threat Intelligence Index, ransomware was the second most common type of cyberattack in 2022 [ibid]. Many experts believe the rise of RaaS has played a role in keeping ransomware so prevalent. Additionally, the 2022 report from Zscaler found that 8 of the 11 most active ransomware variants were RaaS variants [1].

The WannaCry and NotPetya cyberattacks in 2017 spread around the world at an unprecedented rate due to their self-replicating features [23]. Given the growth of ransomware attacks and cybercriminals' ongoing efforts to improve their effectiveness, AI-enabled ransomware attacks with self-propagating capabilities may emerge in the future. Deep neural networks could be used to improve target selection based on specified attributes or to disable defences in target systems, making lateralization easier. Additionally, AI could exacerbate ransomware attacks through intelligent targeting and evasion. Intelligent targeting will find new vulnerabilities through various attack methods and apply the most effective ones to access the system.

Cyberwarfare. There have been several high-profile examples of AI-powered cyberattacks in recent years. One example is NotPetya, considered the most destructive malware ever to be deployed, which caused billions of dollars in damage to companies worldwide. NotPetya spread quickly and efficiently using an AI-powered algorithm that allowed it to infect computers without detection. AI-powered attacks have also been used to target critical infrastructure. For example, hackers used an AI-powered malware called BlackEnergy to attack power grids in Ukraine, causing widespread blackouts and disruption to the country's energy supply [17]. In another example, a UK energy firm was scammed out of £200,000 in 2019 when a hacker used AI to impersonate a CEO's voice in a phone call [4].

Thus, we have identified trends such as the use of AI in cybercrime, increased incidents of RaaS, and cyberwarfare during the years of 2019-2024. AI is increasingly being utilized in cybercrime, enhancing the capabilities of cybercriminals in various ways. Ransomware-as-a-Service represents a significant evolution in cybercrime, democratizing access to sophisticated attack tools. The Russian-Ukrainian conflict has the world on high alert and there have been several attacks associated with the Russian-Ukrainian conflict.

International instruments to counter cybercrime. As cybercrime and particularly AI-powered cybercrime has a strong transnational component, measures are needed to be taken at the international level, as well as at the national level, to counter illegal acts in cyberspace.

The Convention on Cybercrime (Budapest Convention) was adopted far in 2001. So, Chapter III of the Convention on Cybercrime provides a legal framework for international co-operation with general and specific measures [6]:

– International co-operation to combat cybercrime must be comprehensive. This principle allows for an uninterrupted exchange of information at the international level.

– The latter provision establishes the general principle that the rules of Chapter III do not override the provisions of international agreements on mutual legal assistance

and extradition, as well as mutual agreements between the parties or the relevant rules of domestic law relating to international cooperation [ibid].

The negotiations, which began in February 2022 under the Algerian presidency, concluded on 9 August 2024 in New York with the approval of the draft Convention [2]. The Russian Federation, which has been actively promoting the cybersecurity agenda since the beginning of 2019, was the initiator of the establishment of the relevant mechanism in accordance with the UN General Assembly resolution 74/247 as well as the inspiration and leader of the negotiations. During the negotiations, eight sessions were held, attended by representatives of law enforcement and political bodies of more than 160 UN member states. The document provides for the establishment of a 24-hour network of national contact centres aimed at assisting, suppressing and investigating illegal activities in cyberspace. The Convention is designed to create a legal basis for international co-operation in combating cybercrime. The document, developed and approved amidst a tense international situation, was submitted to the 79th session of the UN General Assembly for approval [ibid].

The Road of the United Nations. United Nations Office on Drugs and Crime (UNODC) is active in key areas of criminal justice related to the risks and opportunities arising from new technologies. These areas are dynamic and require adaptation to changing conditions and opportunities.

UNODC engages with national authorities, law enforcement agencies, the public and private sectors and civil society actors to effectively harness the potential of new technologies in justice and to analyse in depth their potential risks, including their impact on human rights.

The International Telecommunication Union (ITU) is a United Nations specialized agency responsible for the regulation of information and communication technologies. The ITU's mandate in the area of cybersecurity and cybercrime is based on decisions taken at formal meetings, including Plenipotentiary Conferences and world assemblies. In particular, Plenipotentiary Resolution 130 reinforced the ITU's role in this area by tasking the Secretary-General and Bureau Directors with supporting Member States, particularly developing countries, in developing effective legal measures to protect against cyber threats [15].

International coordination and cooperation through INTERPOL. Recent serious global cyberattacks and cross-border cybercrimes have demonstrated that few have been investigated and the perpetrators brought to justice. Since the 1980s, INTERPOL has served as the leading international police organisation for the development of global cybercrime capacity and training, as well as the coordination of investigations. Regional working groups have been established in Africa, the Americas, Eurasia (Europe and Asia/South Pacific), the Middle East and North Africa. INTERPOL aims to become a global centre for the detection and prevention of cybercrime through its Global Innovation Complex in Singapore, which houses the Digital Cybercrime Centre. The organisation also supports transnational investigations and provides operational assistance to police in 190 countries. INTERPOL has developed a system for the rapid exchange of cybercrime information through the I-24/7 global police network, which enables the collection, storage and analysis of cybercrime data. Coordinated law enforcement action at the international level is key in the fight against cybercrime, and the I-24/7 network provides the ability for police in one country to quickly call on

experts in other countries for assistance in real time. It is important that investigators can quickly seize digital evidence while it is still available and ensure effective co-operation between jurisdictions when cyberattacks affect multiple countries. Effective global investigations are only possible if law enforcement officials have access to information beyond their borders.

The Digital Crime Centre in Singapore has formed regional cybercrime units around the world and has established international partnerships with various public and private institutions, as well as with members of the private sector and academia. INTERPOL is aware that in the future, cyber experts will not only be employed by law enforcement agencies, but also by private companies and academic organisations.

Thus, the most prominent examples of strategic co-operation in the field of cybercrime interdiction and investigation are the partnerships within the relevant UN agencies and INTERPOL. Such institutions are modernising their techniques and tools to combat cybercrime in line with global cybercrime trends, including those related to the use of AI technologies. It is important to note that INTERPOL and UNICRI have agreed to continue to support the United Nations (UN) and INTERPOL member countries «in a coordinated effort, recognising the unique strengths of each organisation and their complementary areas of expertise» [12].

OUTCOMES. Governments across the globe are increasingly acknowledging the significance of AI-related cybersecurity and are implementing measures to regulate and monitor its advancement. The regulation of measures to combat such offences is evolving at both the national and international levels. A strategic partnership in the creation of comprehensive instruments to combat AI-powered cybercrime within the framework of the UN specialised agencies appears to be the most productive and universally applicable approach. Ongoing work includes further elaboration of normative legal acts to counter cybercrime in accordance with the development of new technologies and AI in particular.

References

1. 2022 ThreatLabz State of Ransomware Report // Zscaler, 2022. URL: https://info.zscaler.com/resources-industry-reports-2022-threatlabz-ransomware-report (accessed on 07.07.2024).

2. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (accessed on 06.07.2024).

3. Artificial intelligence in crime detection: how it’s useful // American Military University. URL: https://www.amu.apus.edu/area-of-study/information-technology/resources/artificial-intelligence-in-crime-detection (accessed on 06.08.2024).

4. A Voice Deepfake Was Used To Scam A CEO Out Of $243,000. URL: https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000 (accessed on 16.08.2024).

5. CBC News: The fight against 'deepfake' videos includes former U.S. ambassador to Russia Michael McFaul. URL: https://www.cbc.ca/radio/thecurrent/the-

current-for-july-20-2018-1.4754632/the-fight-against-deepfake-videos-includes-former-u-s-ambassador-to-russia-michael-mcfaul-1.4754674 (accessed on 16.08.2024).

6. Bokovnya A. Yu. et al. Motives and Objectives of Crime Commission Against Information Security // Ad Alta. 2020. Vol. 10, No. 2 S13. Pp. 7–9. EDN: SCSEBN

7. Cyber Dimensions of the Armed Conflict in Ukraine: Quarterly Analysis Report Q3 July to September 2023 // CyberPeace Institute. URL: https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf (accessed on 06.08.2024).

8. Cybersecurity trends in 2024. URL: https://www.bvp.com/atlas/cybersecurity-trends-in-2024 (accessed on 06.08.2024).

9. Cybercrime: the global challenge // International Telecommunications Union. URL: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/cybercrime.pdf (accessed on 15.08.2024).

10. European approach to artificial intelligence. URL: https://digitalstrategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (accessed on 15.08.2024).

11. IBM X-Force Threat Intelligence Index 2024. URL: https://www.ibm.com/reports/threat-intelligence (accessed on 10.08.2024).

12. INTERPOL and UNICRI release blueprint for responsible use of AI by law enforcement. URL: https://www.interpol.int/News-and-Events/News/2023/INTERPOL-and-UNICRI-release-blueprint-for-responsible-use-of-AI-by-law-enforcement (accessed on 09.08.2024).

13. ITU-T X.1205, Overview of cybersecurity. URL: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (accessed on 09.08.2024).

14. Lallie H. S., Shepherd L. A., Nurse J. R. C., Erola A., Epiphaniou G., Maple C., Bellekens X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic // Comput Secur. 2021. Jun., № 105. P. 102248. DOI: 10.1016/j.cose.2021.102248

15. RESOLUTION 130 (Rev. Guadalajara, 2010) Strengthening the role of ITU in building confidence and security in the use of information and communication technologies.

16. Significant Cyber Incidents. URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (accessed on 19.08.2024).

17. The Dark Side of AI: The Dangers of AI-Powered Cyber Attacks. URL: https://gibraltarsolutions.com/blog/the-dark-side-of-ai (accessed on 09.08.2024).

18 The fight against 'deepfake' videos includes former U.S. ambassador to Russia Michael McFaul. URL: https://www.cbc.ca/radio/thecurrent/the-current-for-july-20-2018-1.4754632/the-fight-against-deepfake-videos-includes-former-u-s-ambassador-to-russia-michael-mcfaul-1.4754674 (accessed on 19.08.2024).

19. The State of PHISHING 2024 Mid-Year Assessment // SplashNext. URL: https://slashnext.com/wp-content/uploads/2024/05/SlashNext-The-State-of-Phishing-24-Midyear-Report.pdf?utm_campaign=The (accessed on 19.06.2024).

20. ‘New deception tactics’. Employee costs company $25 million after scam call with deepfaked CFO. URL: https://www.hrgrapevine.com/us/content/article/2024-02-05-employee-pays-out-25-million-after-scam-call-with-deepfaked-cfo (accessed on 09.08.2024).

21. Smart policies for smart products: A policy maker's guide to enhancing the digital security of products, Directorate for Science, Technology and Innovation Policy Note // OECD, Paris. 2021. URL: https://www.oecd.org/digital/smart-policies-for-smart-products.pdf (accessed on 10.08.2024).

22. Proportion of incident response cases by region to which X-Force responded from 2021 through 2023. URL https://www.ibm.com/reports/threat-intelligence (accessed on 10.08.2024).

23. WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017 URL https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware (accessed on 10.08.2024)

А. А. Богданова,
студент,
Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)
А. А. Родин,
студент,
Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)

ПРАВОВЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ТРУДОВЫХ ОТНОШЕНИЯХ

Аннотация. По мере того как искусственный интеллект все шире применяется в различных сферах человеческой деятельности, вопросы юридического регулирования его внедрения в трудовые отношения приобретают особую значимость. В данном исследовании освещаются правовые сложности, связанные с использованием искусственного интеллекта в трудовой сфере.

Ключевые слова: искусственный интеллект, цифровая дискриминация, цифровые трудовые отношения, информационное общество, автоматизация, дистанционный формат работы, цифровизация, рекрутинг

LEGAL ASPECTS OF THE USE OF ARTIFICIAL INTELLIGENCE IN LABOR RELATIONS

Abstract. As artificial intelligence is increasingly used in various fields of human activity, the issues of legal regulation of its implementation in labor relations are becoming particularly important. This study highlights the legal complexities associated with the use of artificial intelligence in the workplace.

Keywords: artificial intelligence, digital discrimination, digital labor relations, information society, automation, remote work format, digitalization, recruiting

Введение. Двадцать первый век – это эра информационного общества, когда технологии искусственного интеллекта (далее – ИИ) становятся неотъемлемой частью различных сфер жизни, включая трудовые отношения. В экономическом

плане произошли революция, документооборот, наем работников, появление новых бизнес-сфер – все это заслуги развития информационных технологий.

Таким образом, целью данного исследования является анализ правовой действительности использования различных информационных технологий, выявление новых форм влияния ИИ на сферу трудовых отношений.

Основная часть. Информатизация охватывает все направления человеческой деятельности, что стало поводом видоизменения трудовых правоотношений и иных непосредственно связанных с ними отношений и их эволюционирования в цифровые правоотношения.

Первоначально необходимо разобраться, что же стало столь мощным фактором к правовой трансформации природы трудовых отношений и началом их становления в качестве цифровых.

Цифровизация – это последовательная и закономерная ступень развития человечества, обусловленная экономико-политической формацией общества. Ключевым моментом в модернизации природы трудовых правоотношений стала пандемия – COVID-19, которая предопределила мощную трансформацию трудовых отношений [20]. Пандемия COVID-19 обострила необходимость в автоматизации и оптимизации рабочих процессов, что побудило предприятия обратиться к цифровому разуму [10]. Переход на удаленный формат работы, необходимость повышенного мониторинга за производством, состоянием здоровья работников стали основными факторами внедрения ИИ в трудовые отношения. В период пандемии работодатели были вынуждены перевести работников на удаленный формат. Интересно, что на тот момент трудовое законодательство не знало понятия «дистанционная (удаленная) работа» в действующем смысле, не было столь подробной регламентации трудовых отношений дистанционного работника. Сейчас целая глава (49.1) Трудового кодекса Российской Федерации (ТК РФ) посвящена регламентации вопросов, связанных с удаленной работой. Государство и работодатели оперативно отреагировали на текущую ситуацию для защиты прав и интересов как работников, так и работодателей, с целью стабилизации экономических отношений. На федеральном уровне введены меры господдержки организаций и ИП в связи с коронавирусом [8], отдельные меры поддержки были разработаны для системообразующих организаций экономики России [9], для российских компаний, работающих в сфере информационных технологий, разрабатывающих и реализующих разработанные ими программы для ЭВМ, с 2021 г. действуют пониженные ставки страховых взносов ниже ранее установленных на 2017–2020 гг. наряду с другими мерами поддержки.

Российская трехсторонняя комиссия по регулированию социально-трудовых отношений рекомендовала незамедлительно перевести как можно больше работников на удаленный режим работы, что в целом было выполнено работодателями. В то же время Минтруд России подчеркнул, что перевод работника на дистанционную работу не является основанием для сокращения заработной платы, если объем выполняемых задач остается тем же, что также подтвердил Роструд [5].

Несмотря на меры государственной поддержки и внедрение ряда ограничений для сохранения баланса интересов работников и работодателей, ситуация на рынке труда усугубилась. Возникло множество проблем, отражающих сложности в согласовании интересов сторон трудовых отношений. Многие работодатели не

исполняли законодательные предписания, касающиеся соблюдения трудовых прав сотрудников. По статистике Минтруда, с апреля по декабрь 2020 года уволены 12 миллионов 162 тысячи 800 человек, 3 миллиона 144 тысячи россиян оказались в статусе безработных, а около 74 818 работников находились в отпусках без сохранения заработной платы.

Следует отметить, что увольнение работника, переведенного на дистанционный режим, возможно только по основаниям, прописанным в трудовом договоре, который был заключен заново при переводе. Однако многие увольнения происходили под формулировкой «отсутствие работы у данного работника», что фактически позволяло работодателям уклоняться от выполнения обязательств по ст. 22 ТК РФ – предоставления работы и оплаты ее отсутствия [2]. Таким образом, действия работодателей нарушали трудовые права работников, что негативно сказывалось на социально-экономических гарантиях. Эти показатели указывают на дестабилизацию на рынке труда.

В чем же причина столь масштабного увольнения работников и нарушения их трудовых прав и социальных гарантий? Причин несколько: во-первых, пандемия застала всех врасплох, ни работники, ни работодатели, ни государство не были готовы резко переходить на удаленный режим работы; во-вторых, отсутствовало должное законодательное оформление организации дистанционной работы, обеспечение безопасности и охраны здоровья, в-третьих, работодатели не имели четкого понимания, как осуществлять мониторинг эффективности работы сотрудников и поддерживать прежний уровень производительности; в-четвертых, отсутствовали необходимые программные решения и онлайн-платформы, способствующие налаживанию производственных процессов и упрощению поиска работы.

Пандемия COVID-19 стала катализатором для активного внедрения искусственного интеллекта в трудовые отношения и связанные с ними процессы. Она продемонстрировала уязвимости в организации дистанционной работы и дала возможность устранить недостатки как в законодательстве, так и в производственных процессах.

Искусственный интеллект стремительно внедряется в кадровые процессы, такие как рекрутинг, оценка производительности и управление человеческими ресурсами. Однако использование ИИ в этих сферах порождает ряд правовых вызовов, требующих внимания со стороны законодателей и работодателей.

Как верно отметил П. М. Морхат, не существует универсального определения искусственного интеллекта [4]. Предлагаем собственное понимание искусственного интеллекта. Искусственный интеллект – это система алгоритмов, способная осуществлять множество функций, в том числе анализ, моделирование, прогнозирование и другое, решать проблемы, как и человеческий мозг. Поэтому внедрение искусственного интеллекта в трудовые правоотношения – весьма закономерный процесс.

Прежде всего искусственный интеллект внедряется и активно используется при приеме на работу. Как замечено специалистами, развивается такая сфера, как рекрутинг – управление человеческими ресурсами.

С одной стороны, это весьма эффективно для сторон трудовых отношений, так как позволит сократить как человеческие, так и временные затраты на поиск подходящих предложений. Интересным было бы решение создать аналогичный

вариант и для работодателей с целью облегчить поиск подходящей работы работниками. Появится универсальная платформа, в которой будут содержаться данные о работодателях и организациях. Работник, регистрируясь на данной платформе, сможет подобрать подходящую для него вакансию посредством введения определенных данных. Эти данные и данные работодателей искусственный интеллект проанализирует и сгенерирует наиболее подходящие варианты. Но как у любого события, здесь есть и обратная сторона медали. Использование искусственного интеллекта при приеме на работу порождает сразу две проблемы: цифровую дискриминацию и защиту персональных данных.

Внедрение искусственного интеллекта поднимает на повестку дня еще одну проблему – безопасность персональных данных. Компании активно внедряют ИИ для автоматизации процессов, анализа больших объемов данных и повышения эффективности, однако это вызывает серьезные вопросы о защите личной информации работников. Искусственный интеллект, обучаясь на данных, может случайно раскрыть конфиденциальную информацию или же использовать ее ненадлежащим образом.

Кроме того, существует риск использования данных с нарушением прав работников. Важно, чтобы компании соблюдали принципы прозрачности и честности в использовании данных, а также обеспечивали возможность контроля за их обработкой.

Наконец, необходимо учитывать правовые аспекты. В разных странах существуют различные законы, регулирующие защиту персональных данных, такие как Общий регламент по защите данных (GDPR) в Европе. Организациям предстоит обеспечить соответствие этим требованиям, внедряя корректные меры защиты, такие как анонимизация данных или использование алгоритмов, которые могут минимизировать риск утечки информации. Это требует постоянного мониторинга и обновления методов защиты данных, что связано с дополнительными трудностями и затратами для бизнеса.

Конечно, кроме минусов внедрения ИИ, есть и плюсы. Искусственный интеллект можно использовать для мониторинга за производительностью работников, а также оценки состояния здоровья и безопасности работников [19]. К примеру, интересным представляется внедрение ИИ в работу в шахтах. Создание высокотехнологичной шахты, в которой управление будет осуществляться посредством искусственного интеллекта, что позволит осуществлять мониторинг состояния шахты, обеспечение сигнализацией и связью, определением точного места, где возможна авария. Интересным нам представляется проект «Умная шахта», разработанный ООО НПФ «ГРАНЧ», в которой представлена идея SBGPS – системы многофункциональной связи, наблюдения, оповещения и поиска людей, застигнутых аварией. Это очень важная разработка, которая поможет минимизировать риск аварий и гибели людей, что, в свою очередь, позволит обеспечить безопасность условий труда, а также права и гарантии шахтеров.

Данные примеры иллюстрируют положительные аспекты внедрения искусственного интеллекта. Во-первых, алгоритмы, заложенные в ИИ, позволят моделировать различные чрезвычайные ситуации, которые покажут уязвимые места.

В свою очередь работодатели и работники учтут это и ликвидируют, чем предотвратят происшествия. Во-вторых, ИИ могут проводить мониторинг состояния здоровья работников, в результате чего своевременно будут оказаны меры поддержки.

Перейдем к более интересному вопросу – ответственности за действия ИИ. Как мы знаем, искусственный интеллект – это система, представляющая совокупность алгоритмов, способных решать задачи аналогично человеческому мозгу. Но что делать, если вдруг произойдет сбой в системе? Вопрос ответственности за ошибки, допущенные ИИ, особенно в случае увольнения или отказа в приеме на работу, становится важным. Необходимо определить, кто будет нести ответственность: работодатель, разработчик программного обеспечения или сам ИИ?

Разумеется, привлечь к ответственности искусственный интеллект не представляется возможным ввиду того, что в современном понимании к ответственности можно привлечь лишь физическое или юридическое лицо. Искусственный интеллект таковыми не является, да и в принципе его правовой статус в доктрине еще не определен, поэтому привлекать к ответственности ИИ нецелесообразно. На данный момент системы искусственного интеллекта не обладают сознанием и не могут принимать решения в юридическом смысле, следовательно, они не могут быть ответственными за свои действия.

Привлечь кого-то одного к ответственности будет неправомерно и несправедливо, поэтому вопрос разделения ответственности между работодателем и разработчиком программного обеспечения, лежащего в основе деятельности искусственного интеллекта, остается открытым.

Предположим, что можно привлечь к ответственности работодателя за решения по кадровым вопросам, которые он принял на основе результатов, представленных цифровым разумом. Цифровой разум допустил ошибки при предоставлении результатов, что привело к неэффективному оцениванию кандидатов, как следствие, их не приняли на работу, что стало причиной цифровой дискриминации. Но при этом важно, чтобы со стороны работников не было злоупотребления правом при приеме на работу, что якобы их не приняли в результате сбоя ИИ или предвзятости алгоритмов. В этом случае компаниям, корпорациям необходимо разрабатывать собственные правила внутренней политики и практики, которые будут учитывать возможные предвзятости в действиях цифрового разума.

Вопрос в другом: если программное обеспечение при приеме на работу выдает ошибку, в результате кандидата не принимают на работу, то является ли это основанием для привлечения работодателя к ответственности за кадровое решение, принятое в результате сбоя цифрового разума или недостоверно предоставленной информации? Смело можно привлекать к ответственности разработчика ПО, так как он может и должен нести ответственность за успешность и этичное использование разработанных программ.

Таким образом, вопрос о том, кто будет нести ответственность за сбои ИИ, остается открытым. Возможным вариантом решения данного вопроса является идея разделения ответственности между работодателем и разработчиком программного обеспечения. Решение данной проблемы требует комплексного изучения данной тематики как со стороны трудового права, так и со стороны IT-специалистов, чтобы избежать юридических и этических последствий.

Внедрение искусственного интеллекта в сферу трудовых отношений создает новые перспективы, но вместе с тем приносит и множество проблем и вызовов. Рассмотрим основные моменты.

1. Угроза безработицы. Большинству компаний выгодно автоматизировать работу, что повышает их рентабельность, ведь не надо тратить ресурсы на переподготовку кадров для работы с новыми механизмами, ведь в искусственный интеллект загрузили нужные данные, настроили алгоритмы – и он работает по заданному шаблону.

2. Вопрос дискриминации. Механизмы работы ИИ часто строятся на исторических данных, которые могут содействовать поддержанию предвзятости. Например, если их источник содержал практику с дискриминацией.

3. Проблема безопасности и конфиденциальности данных. Цифровой разум создан для обработки большого количества данных. Сфера труда подразумевает сбор больших объемов данных о работниках. Может произойти утечка данных о работнике, поэтому работодатели должны внимательно относиться к сбору и обработке данных искусственным интеллектом. Необходимо комплексное правовое регламентирование данного процесса и взаимодействия с IT-специалистами.

4. Вопрос правовой регламентации использования искусственного интеллекта. Современное законодательство не поспевает за развитием общества, в связи с чем не определен статус искусственного интеллекта в доктрине, соответственно, и в трудовых отношениях. Многие аспекты использования ИИ не регламентированы, это порождает неопределенности и вызывает острую необходимость в разработке соответствующих правовых актов.

5. Увеличение стресса и давления на работников. Интеграция ИИ в рабочие процессы может создать дополнительное давление на сотрудников. Например, системы, отслеживающие производительность в реальном времени, могут приводить к стрессу и снижению морального духа, если работники будут чувствовать себя под вечным контролем.

6. Недостаток подготовленных кадров. С увеличением применения ИИ возрастает потребность в специалистах, способных управлять и выполнять техническую поддержку ИИ-систем. Сейчас рынок труда не готов предоставить достаточное количество таких профессионалов, что замедляет внедрение технологий.

В итоге, хотя ИИ приносит значительные преимущества в трудовые правоотношения, необходимо тщательно рассматривать все потенциальные проблемы, чтобы минимизировать негативные последствия. Это может потребовать сотрудничества работодателей, работников и регуляторов для создания сбалансированных и справедливых условий труда.

Законодательное развитие трудовых цифровых отношений в России представляет собой важный и актуальный процесс, связанный с изменениями в организации труда и внедрением новых технологий.

В США в 2022 году был создан The Blueprint for an AI Bill of Rights (Проект Закона о правах в области искусственного интеллекта). Проект закрепляет пять основных принципов, которые так или иначе применимы к трудовым отношениям:

– безопасность и эффективность систем;

– алгоритмическая безопасность от дискриминации;

– конфиденциальность данных;

– уведомление и объяснение целей использования ИИ-систем;

– человеческие альтернативы, рассмотрение и отказ от использования алгоритмов.

Этот проект не имеет полноценной юридической силы, но тем не менее принципы, которые он предлагает, являются базовыми. Реализация каждого из обозначенных принципов позволит в той или иной степени защитить права работников [25].

Поэтому вопрос о законодательной защите прав работников от внедрения новых автоматизированных систем с использованием искусственного интеллекта не терпит отлагательств.

В целом уже сегодня можно проследить новые тенденции, которые существенно повлияли на рынок труда. Конференцией ООН по торговле и развитию был опубликован доклад от 2017 года [24].

Если сопоставить предоставленные данные выше и современное состояние законодательства РФ, то можно сделать вывод, что еще не все сферы в достаточной мере урегулированы и, соответственно, нужен закон, регламентирующий данный вид деятельности.

Все виды работ в информационный сфере так или иначе предполагают дистанционный формат осуществления трудовой функции. Законодатель долгое время не мог решить вопрос о том, как именно должен быть нормативно закреплен дистанционный формат работы. Вопрос решился, была доработана гл. 49 ТК РФ – в 2013 году появилась гл. 49.1 ТК РФ «Особенности регулирования труда дистанционных работников». Практика показала, что данная глава имеет множество пробелов и вызвала неоднозначное отношение у правового сообщества. Вот что пишет профессор Н. Л. Лютов о данной главе ТК РФ: «Тем не менее далеко не все аспекты этой формы занятости можно назвать оптимально урегулированными законодательством. Часть из них чревата нарушением трудовых прав работников и несет в себе риски прекаризации этого типа занятости» [3]. С наступлением COVID-19 уже 1 января 2021 года вступил в силу Федеральный закон от 08.12.2020 № 407-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации в части регулирования дистанционной (удаленной) работы и временного перевода работника на дистанционную (удаленную) работу по инициативе работодателя в исключительных случаях» [16]. Большая часть пробелов была устранена, часть из них необходимо рассмотреть.

В соответствии с новыми изменениями в ст. 312.1 ТК РФ были приравнены понятия «удаленная работа» и «дистанционная работа». До поправок эти понятия были отделены друг от друга, имели различный правовой статус. Чтобы перевести работника на удаленную работу, нужно было всего-то издать соответствующий приказ и ознакомить с ним сотрудника. Для перевода работника на дистанционную работу было необходимо заключить с ним дополнительное соглашение к трудовому договору. Такая правовая неопределенность не имела права на жизнь в экстремальных правоприменительных условиях. Данное изменение в правовом регулировании позволило унифицировать порядок перевода работников, упростить, сделать прозрачным для правоприменителя.

Следующим шагом стала расширенная трактовка понятия «дистанционный работник». Ранее это были лица, которые заключили трудовой договор о дистанционной работе. Если понимать данный термин буквально, то это те работники, которые выполняют свою трудовую функцию только дистанционно, не комбинированно. Соответственно, данное понятие было расширено. Теперь это лицо, заключившее трудовой договор или дополнительное соглашение к трудовому договору, также предусматривалась возможность временного перевода работника на дистанционный формат по инициативе работодателя в случаях, указанных в ст. 312.9 ТК РФ.

Стоит отметить важное нововведение, которое отсутствовало в старой редакции. Была регламентирована гарантия по оплате труда дистанционных работников. Отныне в ст. 312.5 ТК РФ содержится следующее правило: «Выполнение работником трудовой функции дистанционно не может являться основанием для снижения ему заработной платы» [12]. Это важное законодательное положение пресекло нарушение работодателем прав работников на своевременную и в полном размере выплату справедливой заработной платы. Работодатели считали, что выполнение трудовой функции посредством дистанционного формата не имеет такой же нагрузки, как в офисе, и на основании этого снижали заработную плату.

Не было законодательно урегулировано взаимодействие дистанционного работника и работодателя вне осуществления трудовой функции. Непонятно, оплачивается ли это время. Ответ был дан в новой редакции ст. 312.4 в ее части 6. Норма устанавливала «время взаимодействия дистанционного работника с работодателем включается в рабочее время». Соответственно, это время теперь подлежало оплате, часть трудовых споров на этот счет было устранено. Но так или иначе законодатель не дает конкретики. Что понимается под взаимодействием? Какое взаимодействие должно включаться в рабочее время? Все эти вопросы вновь образовывают правовой вакуум, который со временем даст множество правовых коллизий и споров.

В общем и целом остается еще масса нерешенных вопросов, своей цели в полном объеме законодатель не достиг, дистанционный формат работы не был полностью урегулирован. К примеру, Е. А. Кашехлебова также «отмечает непроработанность вопроса об отнесении к рабочему времени взаимодействия дистанционного работника с работодателем» [1].

Анализ опыта Европейского союза в регулировании дистанционного труда показывает, что в 2002 году в ЕС было заключено рамочное соглашение о телеработе между Европейской комиссией и европейскими объединениями профсоюзов и работодателей [23]. Этот документ содержит базовые правила для дистанционной работы, сочетая экономические аспекты и права работников. В соглашении акцентируется внимание на гибкости условий труда и ответственности работодателей за защиту данных и обеспечение условий труда. Оно также гарантирует работникам право на добровольный доступ к обучению и карьерному росту наравне с офисными коллегами. Однако существует проблема низкой вовлеченности работников в процесс повышения квалификации.

В Европе наряду с «телеработой» существует форма «мобильной работы», основанная на информационно-коммуникационных технологиях (далее – ИКТ) –

ICT-based mobile work. Согласно исследованию Еврофонда 2015 года [22], мобильная работа включает трудовые отношения, выполняемые частично вне основного офиса с использованием ИКТ, в отличие от телеработы, где работник привязан к определенному месту. В России подобное разграничение наблюдается между дистанционной и надомной работой.

Федеральным законом от 22.11.2021 № 377 [17] внесены изменения в Трудовой кодекс, регламентирующие электронный документооборот в трудовых отношениях, который включает создание и хранение документов в электронном виде. Закон определяет платформы для документооборота, такие как «Работа в России», и позволяет работодателям создавать собственные информационные системы. Хотя это обеспечивает многофункциональность норм, отсутствует унификация, что может быть проблемой.

Заключение. С внедрением ИИ в сферу труда возникают и серьезные правовые вызовы, требующие внимательного рассмотрения и регулирования.

Во-первых, необходимо обратить внимание на вопросы защиты персональных данных работников, так как алгоритмы ИИ часто требуют обработки больших объемов информации о сотрудниках. Соблюдение прав на конфиденциальность и контроль над собственными данными являются залогом справедливого и этичного использования технологий.

Во-вторых, возникают сложности с определением ответственности за решения, принимаемые ИИ, особенно в случае возникновения трудовых споров или ущерба. Разработка четкого правового механизма, регламентирующего ответственность как работодателей, так и поставщиков технологий, имеет первостепенное значение.

В-третьих, внедрение ИИ может стать причиной изменения структуры рабочих мест, что требует внимания к вопросам трудовой безопасности, программ переподготовки и поддержки работников, которые могут оказаться под угрозой увольнения или перераспределения.

Список литературы

1. Кашехлебова Е. А. Понятие и особенности дистанционной работы как нестандартного вида занятости // Законы России: опыт, анализ, практика. 2021. № 4. С. 104–108.

2. Кофанова Е. Е., Лиликова О. С. Влияние пандемии коронавируса COVID-19 на отношения в сфере труда // Научные междисциплинарные исследования. 2021. С. 287–292.

3. Лютов Н. Л. Дистанционный труд: опыт Европейского Союза и проблемы правового регулирования в России // Lex Russica. 2018. № 10(143). С. 30–39.

4. Мохат П. М. К вопросу об определении понятия искусственного интеллекта // Теория и история права и государства. 2017. № 11(227). С. 25–31.

5. Письмо Роструда от 09.04.2020 № 0147-03-5 «О направлении ответов на наиболее часто поступающие вопросы на горячую линию Роструда, касающиеся соблюдения трудовых прав работников в условиях распространения коронавирусной инфекции».

6. Об утверждении государственной программы Российской Федерации «Информационное общество»: Постановление Правительства РФ от 15.04.2014 № 313 (ред. от 23.05.2024).

7. О внесении изменений в государственную программу Российской Федерации «Информационное общество» Постановлением Правительства РФ от 31.03.2020 № 386-20.

8. Об утверждении Правил предоставления из федерального бюджета субсидий субъектам малого и среднего предпринимательства и социально ориентированным некоммерческим организациям в условиях ухудшения ситуации в результате распространения новой коронавирусной инфекции: Постановление Правительства РФ от 7 сентября 2021 г. № 1513.

9. Об утверждении Порядка ведения реестра системообразующих организаций, в отношении которых принято решение о согласовании предоставления мер государственной поддержки, и мониторинга соблюдения условий их предоставления: приказ Минэкономразвития России от 13.05.2020 № 279.

10. Шутова А. А. Цифровой паспорт здоровья: этические и правовые проблемы // Вестник Казанского юридического института МВД России. 2021. Т. 12, № 2(44). С. 236–241. EDN: DPUAMG

11. Рыбаков М. С. Правовое регулирование труда в условиях цифровой реальности: основные тенденции развития законодательства // Молодой ученый. 2023. № 1(448). С. 188–194.

12. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 08.08.2024).

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

14. О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»): Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024).

15. Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ.

16. О внесении изменений в Трудовой кодекс Российской Федерации в части регулирования дистанционной (удаленной) работы и временного перевода работника на дистанционную (удаленную) работу по инициативе работодателя в исключительных случаях: Федеральный закон от 08.12.2020 № 407-ФЗ.

17. О внесении изменений в Трудовой кодекс Российской Федерации: Федеральный закон от 22.11.2021 № 377-ФЗ.

18. О стратегическом планировании в Российской Федерации: Федеральный закон от 28.06.2014 № 172-ФЗ (ред. от 13.07.2024).

19. О специальной оценке условий труда: Федеральный закон от 28.12.2013 № 426-ФЗ (ред. от 24.07.2023).

20. Правовое управление в кризисных ситуациях: монография / отв. ред. Ю. А. Тихомиров. М.: Проспект, 2025.

21. Смена технологических укладов и правовое развитие России: монография. М.: ИЗиСП: Норма: ИНФРА-М, 2024.

22. Eurofound. New forms of employment. Luxembourg: Publications Office of the European Union, 2015. 168 p.

URL: https://www.eurofound.europa.eu/sites/default/files/ef_publicatio /field_ef_document/ ef1461en.pdf

23. Framework Agreement on Telework, between the ETUC, UNICE/UEAPME and CEEP 2002.

24. Information economy report 2017: Digitalization, trade and development. United Nations Conference on trade and development. Sales No. E.17. II. D.8. October 2017. P. 62.

25. What the future of work will mean for jobs, skills, and wages. Report McKinsey Global Institute, November 2017. URL: https://www.mckinsey.com/global-themes/future-of-organizations-and-work/what-the-future-of-work-will-mean-for-jobs-skillsand-wages (дата обращения: 01.09.2024).

Е. Т. Борисенко,
студент,
Уральский государственный юридический университет
имени В. Ф. Яковлева

ОТВЕТСТВЕННОСТЬ ЗА РЕШЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАРУБЕЖНОГО ОПЫТА И ПЕРСПЕКТИВЫ ДЛЯ РОССИИ

Аннотация. В условиях стремительного развития и внедрения искусственного интеллекта (далее – ИИ) во все сферы жизни общества остро встает вопрос о юридической ответственности за решения, принятые алгоритмами. ИИ способен на действия, которые ранее были исключительной прерогативой человека, однако он не обладает правосубъектностью в традиционном понимании. Это создает сложную юридическую ситуацию, когда вред, причиненный решением ИИ, может остаться некомпенсированным. Особое внимание уделяется необходимости разработки новых правовых механизмов, адаптированных к специфике ИИ и обеспечивающих баланс между стимулированием инноваций и защитой прав и интересов человека.

Ключевые слова: цифровые технологии, искусственный интеллект, ответственность, правовое регулирование, автономные системы, Европейский союз, США

LIABILITY FOR ARTIFICIAL INTELLIGENCE DECISIONS: A COMPARATIVE ANALYSIS OF FOREIGN EXPERIENCE AND PROSPECTS FOR RUSSIA

Abstract. In the context of the rapid development and implementation of artificial intelligence (AI) across all spheres of society, the issue of legal responsibility for decisions made by algorithms becomes increasingly pressing. AI is capable of actions that were previously the exclusive prerogative of humans; however, it does not possess legal personality in the traditional sense. This creates a complex legal situation where harm caused by AI decisions may go uncompensated. Special attention is given to the need to develop new legal mechanisms that are adapted to the specifics

of AI and that ensure a balance between promoting innovation and protecting human rights and interests.

Keywords: digital technologies, artificial intelligence, liability, legal regulation, autonomous systems, European Union, United States

Введение. Стремительное развитие технологий искусственного интеллекта (далее – ИИ) и его активное внедрение в различные сферы человеческой деятельности предъявляют новые требования к системе права. Одной из наиболее актуальных проблем становится вопрос об ответственности за решения, принятые ИИ, которые могут причинить вред правам и интересам человека.

Основная часть. Исследователи отмечают: «Развитие технологий требует переосмысления многих юридических механизмов обеспечения безопасности применения искусственного интеллекта на основе баланса в части поддержания и стимулирования инновационных отраслей» [1. С. 683–708]. Это означает, что необходимо разрабатывать новые правовые механизмы, которые учитывали бы специфику ИИ и не позволяли уклониться от ответственности, ссылаясь на автономность системы.

Цель настоящей статьи – проанализировать существующую проблему ответственности ИИ, существующие подходы, опыт других стран, а также предложить рекомендации по совершенствованию российского правового регулирования в этой сфере.

Для начала следует определиться с центральным понятием данной работы – искусственным интеллектом. Наиболее подходящим мы считаем определение, данное в проекте Закона штата Калифорния SB 1047, который определяет «искусственный интеллект как созданную человеком или машинную систему, которая может варьироваться в уровне автономности и которая для достижения явных или неявных целей способна на основе полученных данных определять, какие действия необходимо выполнить для воздействия на физическую или виртуальную среду» [3].

Определение ответственности за решения, принятые искусственным интеллектом, представляет собой сложную задачу, обусловленную рядом факторов, которые коренным образом отличают ИИ от традиционных субъектов права – физических и юридических лиц. Эти факторы можно разделить на две основные группы: особенности самого ИИ и пробелы в существующем законодательстве.

Искусственный интеллект, в отличие от человека, не обладает рядом ключевых характеристик, которые традиционно лежат в основе юридической ответственности.

ИИ и роботы не являются самостоятельным субъектом права, не обладают правами и обязанностями, не могут нести юридическую ответственность за свои действия в том же смысле, что и человек или организация [6, 11].

Следующей проблемой выступает так называемый черный ящик. Процессы принятия решений ИИ, особенно в системах, основанных на глубоком обучении, могут быть непрозрачными и непонятными даже для самих разработчиков. Явление, известное как «черный ящик», создает серьезные трудности в доказывании вины и причинно-следственной связи между действием ИИ и наступившим вре-

дом. Если приводить в пример аварию беспилотного транспорта, который управляется ИИ с непрослеживаемыми внутренними процессами, то мы попросту не сможем объяснить «мотивацию» программы, мы будем лишь видеть результат, который привел к последствиям. Безусловно, ведутся исследования, как нам понять внутренние «размышления» ИИ, но пока что такого инструмента не существует.

И главной проблемой в вопросе ответственности стоит динамичность развития ИИ. Технологии ИИ постоянно развиваются, совершенствуются алгоритмы, появляются новые подходы к обучению ИИ [8–10, 12].

Важно учитывать, что применение единых правовых норм ко всем системам ИИ без учета их специфики нецелесообразно. Такой подход может необоснованно затруднить развитие перспективных технологий или, наоборот, создать угрозу правам и интересам человека из-за недостаточной правовой защиты.

Для решения этой проблемы предлагается использовать дифференцированный подход к регулированию ответственности, основанный на классификации систем ИИ по степени их потенциальной опасности [5. С. 19]. В качестве основных критериев классификации можно предложить рискованность и масштаб систем ИИ.

Первый критерий – рискованность – отражает степень возможного вреда, который система ИИ может причинить в случае сбоя или непредвиденных последствий. Здесь можно провести условную границу между высокорисковыми и низкорисковыми системами. Европейская комиссия в своем проекте Регламента об ИИ использует аналогичную логику, фокусируясь на регулировании именно высокорисковых систем, об этом пишут ученые в своей работе: «В этом отношении приложение ИИ следует считать высокорисковым, когда выполняются два совокупных критерия: (1) ИИ используется в секторе, где вероятно возникновение значительных рисков, таких как здравоохранение или транспорт. Эти сектора должны быть исчерпывающе перечислены в будущем правовом документе, и этот список должен регулярно пересматриваться и дополняться. (2) Способ использования приложения делает вероятным возникновение значительных рисков» [7; 4. С. 1–34].

Это, например, ИИ, используемый для персонализации рекомендаций в онлайн-магазинах или для автоматизации рутинных офисных задач. Для таких систем предлагается более мягкий подход к регулированию ответственности, возможно, достаточно будет общих норм гражданского права, исключающих строгую ответственность.

Однако следует учитывать, что развитие и масштабирование низкорисковых систем со временем может привести к появлению новых рисков, требующих пересмотра первоначальной оценки их опасности.

Второй критерий – масштаб системы ИИ – отражает ее сложность и мощность и влияет на оценку риска. Чем больше объем данных для обучения, сложнее алгоритмы и шире сфера применения, тем мощнее система ИИ и тем шире спектр потенциальных рисков. Законодательство штата Калифорния демонстрирует подход, основанный на оценке этого критерия, а именно он касается только моделей, обучение которых стоит более 100 миллионов долларов – этот порог заложен в определении «покрываемой модели», предусмотренном законопроектом, и не может быть изменен, кроме как в результате будущего законодательного акта [3].

Аналогичный подход может быть применен и в российском законодательстве.

Еще одной группой факторов, осложняющих определение ответственности за решения ИИ, являются пробелы в существующем законодательстве.

В большинстве стран, в том числе в России, отсутствует специальное законодательство, регулирующее разработку, применение и ответственность за действия ИИ. Это значит, что при решении споров, связанных с ИИ, приходится опираться на общие нормы гражданского, уголовного и административного права, которые не всегда адекватны специфике ИИ.

Таким образом, определение ответственности за решения, принятые ИИ, представляет собой сложную юридическую проблему, обусловленную как особенностями самого ИИ, так и несовершенством существующего законодательства. Решение этой проблемы требует комплексного подхода, включающего разработку новых правовых норм, адаптированных к специфике ИИ, и уточнения традиционных юридических концепций применительно к действиям ИИ.

Здесь наиболее показателен опыт Европейского союза и Соединенных Штатов Америки как регионов, активно внедряющих ИИ и предпринимающих шаги по его правовому регулированию.

Европейский союз выступает пионером в области правового регулирования ИИ, стремясь к выработке единого подхода на уровне всего союза. В 2021 году Европейская комиссия представила проект Регламента ЕС об ИИ (Artificial Intelligence Act). В основе этого документа лежит рискориентированный подход: вводятся специальные требования к разработчикам, поставщикам и пользователям систем ИИ в зависимости от уровня риска, присущего конкретной системе [2].

Проект регламента предусматривает запрет на использование ИИ в целях, противоречащих ценностям ЕС, например, для манипулирования людьми или социального скоринга. Особое внимание уделяется высокорисковым системам ИИ, применение которых может угрожать безопасности, здоровью или основным правам человека. Такие системы (например, в сфере здравоохранения, транспорта, правоохранительной деятельности) подлежат обязательной оценке соответствия перед выходом на рынок ЕС. Кроме того, предусматриваются механизмы надзора и контроля за рынком ИИ.

Однако проект Регламента ЕС об ИИ подвергся критике со стороны ряда представителей технологической индустрии и экспертов. Высказываются опасения, что регламент может создать избыточную административную нагрузку на компании и замедлить развитие технологий. Также выражаются сомнения в эффективности предлагаемых мер по обеспечению безопасности и защите прав человека.

В США регулирование ИИ находится на более ранней стадии. Федеральное законодательство в этой сфере отсутствует, и регулирование осуществляется в основном на уровне отдельных штатов. Одним из наиболее примечательных примеров такого регулирования является законопроект SB 1047 в штате Калифорния. Он предлагает ввести обязательные требования безопасности для компаний, разрабатывающих мощные модели ИИ.

В частности, законопроект предусматривает обязательное тестирование таких моделей на «критический вред», такой как кибератаки на критическую инфраструктуру или разработка оружия массового поражения. Также компании будут

обязаны гарантировать возможность отключения систем ИИ в случае необходимости и раскрывать информацию о своих мерах безопасности [3].

Анализ опыта ЕС и США показывает разные подходы к регулированию ИИ. В ЕС делается упор на предотвращение вреда, а в США – на стимулирование инноваций и саморегуляцию. Для России важно учитывать оба этих подхода при разработке собственной стратегии правового регулирования ИИ.

Заключение. Развитие технологий искусственного интеллекта ставит перед мировым сообществом новые вызовы, в том числе в сфере права. Вопрос об ответственности за решения, принятые ИИ, особенно актуален в условиях его растущей автономности и внедрения во все большее число сфер человеческой деятельности.

Как показал анализ международного опыта, единого подхода к регулированию ответственности за ИИ пока не существует. Разные страны и регионы выбирают свои стратегии, стремясь найти баланс между стимулированием инноваций и обеспечением защиты прав и интересов граждан.

При разработке собственного подхода к регулированию ответственности за ИИ необходимо внимательно изучить опыт других стран, учитывая как их достижения, так и проблемы, возникшие при практической реализации разных моделей регулирования.

Очевидно, что решение этой сложной проблемы требует взвешенного и комплексного подхода, который учитывал бы как специфику технологий ИИ, так и особенности национальной правовой системы.

Список литературы

1. 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. Вып. 58. С. 683–708.

2. European Commission Proposal for a Regulation of the European Parliament and of the Council laying down harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) 2021/0106 (COD) (‘Draft AI Act’). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (дата обращения: 01.09.2023).

3. SB 1047: Safe and Secure Innovation for Frontier Artificial Intelligence Models Act. URL: https://digitaldemocracy.calmatters.org

4. Schütte B., Majewski L., Havu K. Damages Liability for Harm Caused by Artificial Intelligence – EU Law in Flux. Helsinki: University of Helsinki, Faculty of Law, 2021. // Legal Studies Research Paper Series; Paper No 69. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3897839 (дата обращения: 01.09.2024)

5. Бегишев И. Р. Об обороте роботов, их составных частей (модулей) (инициативный проект федерального закона): Препринт № 1 за 2021 г. Казань: Познание, 2021. 28 с. EDN: FTFKAN

6. Бегишев И. Р. Криминологическая классификация роботов: риск-ориентированный подход // Правоприменение. 2021. Т. 5, № 1. С. 185–201. EDN: TBUVGY

7. Kirpichnikov D. V. et al. Bioprinting Medical Devices: Criminal Evaluation Issues / // AIP Conference Proceedings: VII International Conference “Safety Problems of Civil Engineering Critical Infrastructures” (SPCECI2021), Yekaterinburg, 2023. Vol. 2701. P. 020032. EDN: STBLEX

8. Бегишев И. Р., Хисамова З. И. Криминологические риски применения искусственного интеллекта // Всероссийский криминологический журнал. 2018. Т. 12, № 6. С. 767–775. EDN: YYSTVZ

9. Бегишев И. Р. Хисамова З. И. Искусственный интеллект и робототехника: глоссарий понятий. М.: Проспект, 2021. 64 с. EDN: HQELSK

10. Хисамова З. И., Бегишев И. Р. Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты // Всероссийский криминологический журнал. 2019. Т. 13, № 4. С. 564–574. EDN: QOFRXQ

11. Субъект права: стабильность и динамика правового статуса в условиях цифровизации: сборник научных трудов / под общ. ред. Д. А. Пашенцева, М. В. Залоило. М.: Инфотропик Медиа, 2021.

12. Черногор Н. Н., Емельянов А. С., Залоило М. В. Трансформация идейной основы юридической ответственности: между архаикой и постмодерном // Вопросы истории. 2021. № 11(2). С. 248–259.

А. Д. Бочкарева,
магистрант,
Казанский (Приволжский) федеральный университет

СИНЕРГИЯ ЦИФРОВОГО И ИНТЕЛЛЕКТУАЛЬНОГО ПРАВА: ВОЗМОЖНАЯ РЕЦЕПЦИЯ ЗАРУБЕЖНОГО ОПЫТА

Аннотация. В настоящей статье рассматриваются новейшие положения зарубежного законодательства, позиции судов иностранных государств, акты региональных правовых систем в части взаимодействия AI и IP с целью выявления наиболее важных и актуальных вопросов, подлежащих решению на уровне национального законодательства. Дается оценка возможности использования новелл зарубежного законодательства для совершенствования правового регулирования в Российской Федерации.

Ключевые слова: интеллектуальная собственность, искусственный интеллект, право, авторское право, синергия, результат интеллектуальной деятельности, нейросеть, дипфейк

SYNERGY OF DIGITAL AND INTELLECTUAL PROPERTY LAW: POSSIBLE RECEPTION OF FOREIGN EXPERIENCE

Abstract. This article considers the latest provisions of foreign legislation, positions of foreign courts, acts of regional legal systems in terms of interaction between AI and IP in order to identify the most important and relevant issues to be resolved at the level of national legislation. The assessment of the possibility of using novelties of foreign legislation to improve legal regulation in the Russian Federation is given.

Keywords: intellectual property, artificial intelligence, law, copyright, synergy, intellectual property result, neural network, dipfake

Введение. Наделение объектов интеллектуальной собственности и цифровых активов стоимостным эквивалентом, создание нетрадиционных объектов интеллектуальной собственности с использованием цифровых технологий, наделение объектов цифрового права творческим характером, новизной или иными признаками охраноспособности, машинное обучение с использованием объектов авторского права и ряд иных нюансов способствуют возникновению пласта вопросов о синергии данных правовых секторов.

Основная часть. Право Российской Федерации последние годы достаточно активно «впитывает» аспекты взаимодействия IP и AI, иными словами, института интеллектуальной собственности и технологий искусственного интеллекта. Блок цифрового права далеко не исчерпывается искусственным интеллектом (AI, ИИ), однако именно вопросы его проникновения в право интеллектуальной собственности (IP) в настоящее время вызывают ряд дискуссий, примером чему выступают и реальные кейсы, в том числе сборник рассказов «Пытаясь проснуться», написанный Павлом Пепперштейном и нейросетью ruGPT-3, появление дипфейков. Именно поэтому речь пойдет в первую очередь о «взаимном влиянии» IP и AI и о способах правовой обвязки результатов такого влияния.

В Проект выделены были положения, касающиеся проблематики определения автора изобретения программы, основанной на ИИ; правообладателя патента, связанного с ИИ-программой; в принципе предоставления правовой охраны изобретениями, созданными ИИ в автономном режиме; вопросы цифровой фабрикации. В пересмотренном проекте 2020 года ВОИС также отметил вопросы признания AI изобретателем, его указания в качестве изобретателя в заявке на выдачу патента, возможность замены квалифицированного профильного специалиста на AI-решение [5].

Представляется верным формировать практику разрешения вопросов путем тщательной информационной обработки опыта, сформировавшегося в иных юрисдикциях, для выбора наиболее применимого с целью его дальнейшей «отшлифовки» под правовую систему конкретной страны.

Опыт Европейского союза в части установки взаимодействия интеллектуальной собственности и искусственного интеллекта достаточно прогрессивен, что подтверждается весьма внушающим количеством правовых документов, нацеленных на правовое регулирование обозначенного явления на стыке двух блоков отношений. В Резолюции Европейского парламента о правах интеллектуальной собственности в связи с развитием технологий искусственного интеллекта (2020/2015(INI)) объекты, где уже разграничивались объекты, созданные человеком с помощью ИИ, и объекты, созданные ИИ автономно, в докладе Еврокомиссии 2020 года «Тренды и разработки в области ИИ. Директивы об авторских правах 2019/790 [4]. Положения упомянутого акта обязывают публично описывать контент, который использовался для обучения ИИ, и маркировать контент, сгенерированный ИИ. Представляется, что имплементация подобных положений в нашу правовую систему поспособствовала разрешению споров о допустимых границах

обучения искусственного интеллекта на объектах авторского права, а также четкому определению объема творческого вклада человека в создание результата интеллектуальной деятельности.

Великобритания дает свои ответы на вопросы, поставленные в Проекте ВОИС, в части определения авторства на произведения, сгенерированные ИИ. Так, Закон «Об авторском праве, промышленных образцах и патентах» от 1988 г. в ч. 3 ст. 9 указывает, что в отношении генерируемого компьютером произведения автором признается лицо, которым осуществляются необходимые для создания произведения мероприятия [2]. В качестве авторов могут рассматриваться, в зависимости от конкретного случая, разработчик системы ИИ, ее пользователь или иные лица. Позиция относительно принадлежности авторских и патентных прав на объекты, созданные ИИ в автономном режиме или при его использовании, подтверждается английскими судами: Верховный суд Великобритании в нашумевшем деле № 2021/0201 отказал Стивену Тайлеру в регистрации патента на изобретение, созданное нейросетью DABUS, которая была указана им в качестве соавтора [8].

На уровне правовой системы Великобритании принята позиция, согласно которой не подлежит патентованию и сама искусственная нейронная сеть (ИНС), в деле Comptroller-General of Patents, Designs and Trade Marks v Emotional Perception AI Ltd EWCA Civ 825 Английский апелляционный суд пришел к выводу, что обучение ИНС, как часть создания программы, не является техническим вкладом, что является обязательным для предоставления патентной охраны. Результаты работы ИНС, такие как улучшенные музыкальные рекомендации, были признаны нетехническими и субъективными, в связи с чем и непатентоспособными [9]. Это решение имеет значительные последствия для патентных заявок на системы генеративного ИИ, где обучение является важной частью разработки, которые подаются повсеместно и в других странах, согласно отчету ВОИС от 3 июля 2024 года о патентном ландшафте генеративного ИИ. Вопрос о рецепции данной позиции в правовую систему РФ представляется спорным в силу возможности дестимулирования патентной активности, что также имеет дискуссионную окраску. Подготовка консолидированного законодательного акта, регулирующего взаимодействие AI и IP в Великобритании, на настоящее время отложена, однако принятие данного акта окажет значительное влияние на английское право, не оставив без внимания и взаимодействие данных сфер на уровне других юрисдикций.

Необходимость определения вопроса о возможности наделения ИИ правосубъектностью в авторском праве летом 2024 года возникла и перед Федеральным судом Канады. В настоящее время Канада создала прецедент по наделению объектов, сгенерированных искусственным интеллектом, статусом правовой охраны в силу того, что оспариваемые права на фотографию Suryast были зарегистрированы в 2021 году в Канадском ведомстве. Согласно действующему в Канаде механизму, полномочия определения авторства лежат на судах. В связи с тем, что подобные кейсы не так часты для Канады, то определиться, какой ответ дается правовой системой страны на вопросы, поставленные в проекте ВОИС, представляется сложным. На настоящем этапе анализа можно отметить индивидуальность подхода в силу определения принадлежности права авторства судом, тактику case by case в части признания ИИ автором объекта интеллектуальной собственности ВОИС также рассматривал как возможную, которая, как представляется автору

статьи, при правильной ее «отшлифовке» допустима для правовой системы РФ, однако не без создания большого пласта работы для судебных органов.

Наиболее обширным является опыт США. Позиция судов США в части признания авторства исключительно за человеком в настоящее время также достаточно определена, однако в практике много иных вопросов, требующих разрешения. Что касается проблематики обучения генеративного ИИ на объектах авторского права, то суды США также начинают формировать собственное мнение по данному вопросу: так, 12 августа 2024 года судья Окружного суда Уильям Оррик вынес решение, позволяющее группе художников продолжить судебный иск против Stability AI, Midjourney и DeviantArt, обвиняющихся в использовании работ художников без их согласия для обучения модели ИИ, лежащей в основе генератора изображений Stable Diffusion, который сейчас конкурирует с художниками-людьми [6]. С родственной природой суду предстоит разрешить спор между OpenAI и NYT (The New York Times). NYT утверждает, что ChatGPT от OpenAI нарушил их авторские права, используя «практически дословные отрывки» из их статей без разрешения с целью обучения [7]. В Федеральном суде штата Массачусетс на рассмотрении иск к стартапам Suno и Udio, работающим в области создания музыки с использованием ИИ [10]. Компании оспаривают иски о нарушении авторских прав, заявляя, что их методы соответствуют доктрине «добросовестного использования» и способствуют инновациям и конкуренции в индустрии, сравнивая их с процессом обучения ребенка, в котором нет ничего противоправного. От дальнейшего разрешения указанных дел будет зависеть судьба сформировавшейся концепции «добросовестного использования», согласно которой использовать объекты авторских прав для обучения генеративного ИИ возможно в определенных пределах, такую же позицию обозначала Еврокомиссия в одной из Директив, ее положения указывали на неправомерность обучения на основе результатов интеллектуальной деятельности только в силу прямого запрета со стороны автора, правообладателя. Немаловажным является и то, что данные кейсы сформируют и позицию относительно места критерия добросовестной конкуренции среди авторов, правообладателей результатов интеллектуальной деятельности и субъектов, использующих их для обучения генеративного ИИ, в данной концепции, а также допустимости доказательств по данной категории дел.

В силу придания огласки проблематике распространения дипфейков и даже признания их объектами авторского права (Дело № А40-200471/23) автору представляется верным рассмотреть вариант имплементации в правовую систему положений проекта Акта о защите происхождения и целостности отредактированных и дипфейковых медиа (Content Origin Protection and Integrity from Edited and Deepfaked Media Act, COPIED Act). В данном Акте предлагается установить обязанность для компаний, занимающихся ИИ, встраивать данные о происхождении в созданный контент, а также запрет на удаление или изменение этой информации, что позволит создателям контента выявить несанкционированное использование их работ [1]. Имплементация положений данного акта позволит предоставить надежную правовую защиту создателям контента, таким как журналисты, художники и музыканты, позволяя им защищать свою интеллектуальную собственность и устанавливать условия использования.

Автор видит верной траекторию разработки положений национального законодательства, основанных на позиции «добросовестного использования» контента с целью обучения, устанавливающих защиту авторов от несанкционированного использования их трудов с помощью отлаженной системы информирования; надлежащим механизмом, подлежащим включению в законодательное регулирование, выступает и маркировка объектов, сгенерированных ИИ. На момент написания статьи не найдены примеры замены квалифицированного профильного специалиста на AI-решение, однако создание практики такого использования на уровне Российской Федерации представляется прогрессивным, так как определение возможности предоставления патентной охраны в настоящее время достаточно субъективно, а внесение элементов объективизации и минимизации уровня субъективности позволит укрепить доверие к институту и снизить количество возникающих споров.

Заключение. Таким образом, анализ опыта иных юрисдикций предоставляет огромный пласт правовой базы, использование которой в дальнейшем может поспособствовать формированию надлежащего источника регулирования.

Список литературы

1. Content Origin Protection and Integrity from Edited and Deepfaked Media Act, COPIED Act. URL: https://digitalpolicyalert.org/event/21426-introduced-content-origin-protection-and-integrity-from-edited-and-deepfaked-media-act-copied-act-including-user-rights (дата обращения: 07.09.2024).

2. Copyright, Designs and Patents Act 1988 (Chapter 48), United Kingdom. URL: https://www.wipo.int/meetings/ru/doc_details.jsp?doc_id=470053 (дата обращения: 07.09.2024).

3. Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence. URL: https://www.wipo.int/meetings/ru/doc_details.jsp?doc_id=470053 (дата обращения: 07.09.2024).

4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (дата обращения: 07.09.2024).

5. Revised Issues Paper on Intellectual Property Policy and Artificial Intelligence. URL: https://www.ompi.int/meetings/ru/doc_details.jsp?doc_id=499504 (дата обращения: 07.09.2024).

6. Case No. 23-cv-00201-WHO. URL: https://cand-ecf.sso.dcn/cgi-bin/DktRpt.pl?407208 (дата обращения: 07.09.2024).

7. The New York Times Company v. Microsoft Corp., et al., Case No. 1:23-cv-11195-SHS. URL: https://storage.courtlistener.com/recap/gov.uscourts.nysd.612697/gov.uscourts.nysd.612697.152.0.pdf (дата обращения: 07.09.2024).

8. Thaler (Appellant) v Comptroller-General of Patents, Designs and Trademarks (Respondent). URL: https://www.supremecourt.uk/watch/uksc-2021-0201/judgment.html (дата обращения: 07.09.2024).

9. Comptroller-General of Patents, Designs and Trade Marks v Emotional Perception AI Ltd EWCA Civ 825. https://www.judiciary.uk/judgments/comptroller-

general-of-patents-designs-and-trade-marks-v-emotional-perception-ai (дата обращения: 07.09.2024).
10. Case No. 24-04777. URL: https://www.riaa.com/wp-content/uploads/2024/06/Udio-Complaint-6.24.241.pdf (дата обращения: 07.09.2024).
11. Can AI be an author? Federal Court asked to decide in new copyright case. URL: https://www.ctvnews.ca/sci-tech/can-ai-be-an-author-federal-court-asked-to-decide-in-new-copyright-case-1.6962705 (дата обращения: 07.09.2024).

Ю. С. Варуша,
студент,
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВОТВОРЧЕСТВЕ И ПРАВОПРИМЕНЕНИИ

Аннотация. На протяжении истории существования человека информация была катализатором социальных изменений. Четвертая информационная революция 70-х гг. XX века внесла новые принципы хранения и обработки информации, развиваясь настолько стремительно, что крупные мировые державы не могли остаться в стороне и ступили на путь построения цифрового общества, внедряя цифровизацию во все сферы общественной жизни. Однако правовая сфера сталкивается с серьезными проблемами при адаптации к цифровизации, поскольку многие правовые концепции, связанные с цифровой эпохой, все еще находятся на ранних стадиях развития. Это обуславливает интерес многих исследователей к симбиозу права и цифровых технологий, особенно искусственного интеллекта и процессов правотворчества и правоприменения. Целью настоящей статьи стало изучение влияния искусственного интеллекта на правотворчество и правоприменение, а также перспективы его внедрения в сферу деятельности законодателей. Будучи инновационной, технология искусственного интеллекта открывает перед законодателями возможности комплексной модернизации зарождения законодательной инициативы и законотворчества, но, оставаясь несовершенной, она склонна нарушать юридическую технику и выдавать ложные ответы. Комплексный анализ внедрения искусственного интеллекта в правотворчество и правоприменение позволит определить наиболее реальные перспективы такого симбиоза.

Ключевые слова: искусственный интеллект, цифровизация, цифровое общество, правотворчество, правоприменение

USING ARTIFICIAL INTELLIGENCE IN LAWMAKING AND LAW ENFORCEMENT

Abstract. Throughout the history of human existence, information has been a catalyst for social change. The fourth information revolution of the 70s of the XX century introduced new principles of information storage and processing, developing so rapidly that the major world powers could not stand aside and embarked on the path

of building a digital society, introducing digitalization in all spheres of public life. However, the legal sphere faces serious problems in adapting to digitalization, since many legal concepts related to the digital age are still in the early stages of development. This causes the interest of many researchers in the symbiosis of law and digital technologies, especially artificial intelligence and the processes of law-making and law enforcement. The purpose of this article is to study the influence of artificial intelligence on law-making and law enforcement, as well as the prospects for its introduction into the sphere of activity of legislators. Being innovative, artificial intelligence technology opens up to legislators the possibility of a comprehensive modernization of the origin of legislative initiative and lawmaking, but remaining imperfect, it tends to violate legal technique and give false answers. A comprehensive analysis of the introduction of artificial intelligence into law-making and law enforcement will determine the most realistic prospects for such a symbiosis.

Keywords: artificial intelligence, digitalization, digital society, law-making, law enforcement

«Мы живем в информационную эпоху, и афоризм “Кто владеет информацией, тот владеет миром” отражает реальности современного мира», – заявил Владимир Путин на совещании послов и представителей РФ 30 июня 2016 года. С этим высказыванием сложно поспорить, ведь информация и появление новых способов ее распространения всегда были катализатором общественных изменений и прогресса. Четвертая информационная революция 70-х гг. XX века оказала на общество не менее значительное влияние, чем ее предшественницы, приведя в мир микропроцессоры и персональные компьютеры. Так появились новые системы хранения и поиска информации, положившие начало формированию информационного общества.

Под цифровым обществом понимается «современная стадия развития информационного общества, в которой важнейшее значение имеет не информация в целом, а прежде всего ее цифровой формат, методы оцифровки, кодирования и передачи информации» [1]. И хотя цифровое общество формируется в различных макрорегионах неравномерно, большинство развитых и развивающихся стран уже вступили на путь внедрения цифровизации в сферы общественной жизни. Согласно исследованию Европейской комиссии, 75 % опрошенных жителей Европейского союза считают, что новейшие цифровые технологии положительно влияют на экономику, 67 % – на качество их жизни [2]. И тем не менее исследователи отмечают и вызовы, перед которыми стоит современное общество в связи с внедрением цифровых технологий: развитие новейших форм социального неравенства, «усиление зависимости развивающихся стран от технологических лидеров» [1], нарушение приватности и прав человека.

Безусловно, серьезный вызов процесс цифровизации бросает правовой сфере, так как правовое осмысление многих продуктов цифровой эры находится на стадии формирования [22]. В связи с этим исследования, связанные с выявлением, интерпретацией и построением прогностических гипотез, касающихся влияния цифровизации на право, становятся актуальными в наши дни.

Автор настоящей работы ставит целью интерпретировать влияние одного из самых инновационных наследий цифровой эпохи – искусственного интеллекта

– на процессы правотворчества и правоприменения, а также определить потенциально возможные перспективы его внедрения в вышеуказанные процессы, применительно к российскому правовому полю.

Искусственный интеллект в правотворчестве. Цифровизация оказывает влияние прежде всего на содержание права [3], а способом изменения его содержания служит процесс правотворчества, в рамках которого квалифицированные органы государственной и муниципальной власти создают новые нормы права. Некоторые специалисты [4] убеждены, что процесс цифровизации окажет неминуемое влияние на правотворчество [24], ведь общество постоянно находится в поиске новых решений для модернизации процесса разработки новых правовых норм и коррекции действующих, а такие технологии, как искусственный интеллект, открывают возможности для более качественного законотворчества. Рассмотрим некоторые из возможностей.

При осуществлении своей деятельности субъекты законотворческого процесса сталкиваются с колоссальными объемами информации. Сам процесс законодательной инициативы обусловлен появлением соответствующего запроса внутри общества, данные о котором находятся не только в официальных статистических материалах, но и в неофициальных источниках. Искусственный интеллект способен оказать помощь при анализе и обобщении последних.

Перспективные методы, обозначенные в Национальной стратегии развития искусственного интеллекта на период до 2030 года [5], позволяют автоматизировать законотворческий процесс с помощью цифровых технологий в качестве инструмента для написания текстов нормативно-правовых актов. Чтобы подобное нововведение успешно функционировало, ИИ (здесь и далее – искусственный интеллект) потребуется база исходных данных, на основе которой будет происходить его обучение, преимущественно тексты действующих законов [6].

Таким образом, подобные новшества позволят законодателям автоматизировать процесс разработки законопроектов. Во-первых, ИИ сможет анализировать информационное поле на предмет наличия актуальных ниш для внедрения новых нормативно-правовых актов, а во-вторых, он позволит ускорить саму процедуру разработки нормы, позволяя законодателям освобождать ресурсы для более затратных областей их профессиональной деятельности.

Искусственный интеллект в правоприменении. В правоприменении органы, реализующие действие нормативно-правовых актов, сталкиваются с некоторыми вызовами. Это обусловлено тем, что в эпоху цифровизации права законодатель уделяет значительное внимание вопросу защиты прав человека, поэтому потенциальные нарушения становятся основным вопросом при исследовании возможностей применения ИИ в праве. Рассмотрим некоторые из потенциальных проблем.

ИИ на сегодняшнем этапе своего развития способен анализировать лишь те информационные ресурсы и материалы, которые в него загрузил человек. Эта технология уже «обучается» автоматической классификации, но при этом пока не может самостоятельно получать общие принципы и логику понятий, иными словами, понять суть вещей, именно поэтому значимой проблемой в использовании технологий ИИ в правоприменении становится нарушение юридической техники. Оно, как отмечает Ю. Балатаева, заключается в наличии различных технико-юридических дефектов, которые будут существенным образом осложнять процесс

обучения искусственного интеллекта. Наиболее распространенными в российском праве являются такие технико-юридические дефекты, как пробелы и коллизии [7, 17]. Даже в традиционной практике пробелы в праве и коллизии усложняют процедуры правоприменения и порождают споры, разрешить которые уполномочен только суд. Отсюда вытекает закономерный вывод, что ИИ неспособен самостоятельно заполнить пробелы в правовой базе, что, в свою очередь, приведет к путанице и выдаче неверных ответов со стороны ИИ.

В действующих нормативных правовых актах специалисты отмечают и немало языковых дефектов, среди которых использование сложной терминологии, которая усложняет правоприменение. По мнению А. Головиной, «практика, в том числе и судебная, показывает, что многие правовые нормы благодаря своей сложности оставляют большой простор для различных толкований, нередко полярно противоположных» [8]. Алгоритмы же микропроцессоров основаны на идее правил и логики и, хотя современный ИИ «выходит за пределы аналогового порядка, базирующегося на связывании анализируемых элементов, он сталкивается со сложными проблемами, которые возникают в результате взаимодействия с большим количеством переменных, а переменные не отрегулировать правилами» [9].

ИИ постоянно комбинирует эти переменные и приходит к наиболее вероятному решению. Однако практически невозможно понять, почему система приняла именно это решение, а не иное. Таким образом, ответы ИИ есть результат агрегирования многих показателей, что гораздо ближе к аналогии, нежели к логике и правилам.

Развитие технологий активно модернизирует различные сферы юридической деятельности. Опыт отечественных и зарубежных коллег показывает, что к настоящему времени сформировалось несколько перспективных отраслей для внедрения ИИ:

1. Судопроизводство.
2. Видеонаблюдение.
3. Деятельность правоохранительных органов.
4. Антикоррупционная экспертиза.
5. Бюджетное регулирование.

Судопроизводство. В 2023 году председатель Совета судей России Виктор Момотов анонсировал скорый запуск суперсервиса «Правосудие-онлайн». Благодаря этому сервису граждане смогут через портал госуслуг переходить в онлайн-заседания и участвовать в судебных процессах через свой телефон. «Сервис сделает доступным онлайн-документооборот: через него можно будет ознакомиться с любыми документами по делу и направить заявления, которые будут генерироваться с помощью встроенных шаблонов» [10].

Деятельность органов судебной власти в цифровой среде обеспечивают и другие специализированные информационные системы: ГАС «Правосудие», АИС «Банк решений арбитражных судов», ИС «Картотека арбитражных дел», которые способствуют автоматизации судебного делопроизводства и введению элементов электронного судопроизводства. С 2017 года в этих системах зарегистрировано более 2 млн личных кабинетов и подано порядка 20 млн электронных обращений.

На сегодняшний день в России идет процесс дискуссий по вопросу применения ИИ в судебной сфере.

Так, 26 декабря 2023 года в Совете Федерации состоялся семинар-совещание «Цифровизация деятельности органов судебной власти в Российской Федерации». В ходе семинара поднимался вопрос применения ИИ в суде зарубежными коллегами. Среди основных задач, в решении которых за рубежом используются цифровые технологии, являются организация виртуальных заседаний (Колумбия, Сингапур, Китай), судебная аналитика и судебное прогнозирование (Великобритания, США), помощь в вынесении решения (США, Китай) и рассмотрение коммерческих споров (WeChat в Китае).

По словам сенатора Ирины Рукавишниковой, «цифровизация системы правосудия во многом оптимизировала работу в части направления извещений участникам процесса, направления копий судебных актов в форме электронных документов, также она оказывает влияние на снижение коррупционных рисков в управленческой деятельности» [11].

Вопрос применения искусственного интеллекта был поднят и в Верховном суде РФ. Так 21 мая 2024 года на совете Верховного суда РФ были озвучены предложения по применению искусственного интеллекта в расследовании уголовных дел. По словам Председателя ВС РФ Ирины Подносовой, Верховный суд проанализировал судебные дела по ст. 228 УК РФ и сроки, которые назначали по ним судьи. На основе них подготовлены предложения, в том числе по изменению в УК РФ, которые повысят эффективность государственной политики в борьбе с наркопреступностью. ВС также проанализировал уголовные дела, где так или иначе есть ссылки на результаты следственной деятельности с использованием искусственного интеллекта, и подготовил свои предложения, которые не позволят использовать искусственный интеллект во вред праву, а наоборот, для восстановления справедливости. В ближайшее время Верховный Суд представит свои предложения в деталях.

И тем не менее в отечественной и зарубежной правовой практике зафиксированы случаи неправомерного использования искусственного интеллекта в рамках судебного процесса.

В начале 2023 года ученого Александра Цветкова обвинили в совершении серии убийств, которые произошли 20 лет назад. Фоторобот предполагаемого преступника сгенерировал искусственный интеллект, и он совпал с изображением ученого 20-летней давности на 55 %. Несмотря на то, что следствию сразу же были представлены доказательства наличия у А. Цветкова алиби, мужчина провел под арестом десять месяцев.

Это не единственный в мире случай, когда были совершены недопустимые ошибки со стороны ИИ. Так, 20 октября 2023 года в Калифорнии (США) 61-летний мужчина был обвинен в ограблении магазина на основании данных системы распознавания лиц, установленной в этом магазине, которая идентифицировала его как виновника ограбления [12]. Несмотря на то, что в момент ограбления магазина мужчина жил в другом штате, он был арестован и заключен под стражу. Через несколько часов, после проверки алиби, его выпустили, но за это время мужчина подвергся насилию со стороны сотрудников правоохранительных органов. Впоследствии мужчина подал в суд на сеть магазинов Macy's и материнскую компанию торговой точки Sunglass Hut, за ограбление которой он был арестован, из-за использования магазинами системы распознавания лиц, которая ошибочно

идентифицировала его как виновника вооруженного ограбления и привела к судебному преследованию.

Данные примеры свидетельствуют о необходимости контроля новых технологий в судопроизводстве со стороны квалифицированных специалистов.

Видеонаблюдение. На сегодняшний день в России установлено свыше 13 миллион камер видеонаблюдения, пишут на портале rbc.ru. «Большая часть камер в России (58,7 %) установлена коммерческими организациями с целью обеспечения безопасности, предотвращения краж и преступлений. Еще 32,8 % камер установили за бюджетные средства. Они работают на территории школ, детсадов, медицинских учреждений, дорогах и госучреждениях» [13].

В последние годы растет популярность использования камер видеонаблюдения при выявлении лиц, нарушающих правила дорожного движения на дорогах общего пользования. За 2023 год в России было возбуждено свыше 240 миллионов административных дел, связанных с нарушением правил дорожного движения, о чем сообщил на своем портале Научный центр БДД МВД России [14]. Большинство нарушений (92 %) было выявлено в ходе автоматической фиксации, что составляет 221 миллион правонарушений. Это на 20,3 % превышает показатели 2022 года, хотя число камер видеонаблюдения увеличилось лишь на 9,8 %. Данные показатели свидетельствуют о повышении качества видеосъемки и расширении их функционала, который все в большем объеме основывается на использовании искусственного интеллекта.

Применимы камеры видеонаблюдения с ИИ и в сфере контроля деятельности управляющих компаний. Так, в 2023 году на территории Московской области специальные технические средства «Автоматизированные комплексы с использованием интеллектуальной нейронной сети видеофиксации нарушений с предустановленным ПО» зафиксировали нарушения в сфере ЖКХ при помощи фото- и видеосъемки, среди которых невывезенный мусор, отсутствие уборки снега/противогололедных средств и т. д. После фиксации информацию обработал искусственный интеллект, затем она поступила в ГУ содержания территорий Московской области, на основании чего должностные лица учреждения составили протоколы. Управляющая компания заявила, что данные камер с нейронной сетью не являются надлежащим доказательством, так как у разработчика используемой системы нет декларации о соответствии комплекса требованиям законодательства, свидетельств о поверке такой системы и решения должностных лиц о вводе таких камер в эксплуатацию. Однако в рамках дела № А41-17948/23 Арбитражный апелляционный суд признал эти доводы несостоятельными [15]. Такие системы с использованием нейронной сети не являются средством измерения, а лишь фиксируют нарушения. Поэтому для установления факта нарушения достаточно паспорта устройства, данных о сертификации и о поверке таких комплексов.

Свое применение камеры видеонаблюдения с встроенным ИИ нашли и при фиксации лиц, находящихся в уголовном розыске; нарушающих масочный режим во время пандемии коронавирусной инфекции COVID-19 [11]; совершающих подозрительные действия возле полок с товарами, на кассах и складах; совершающих несанкционированное проникновение на охраняемые территории. Благодаря высокотехнологичным чипам с искусственным интеллектом и алгоритмами тща-

тельного обучения камеры с ИИ активно анализируют изображения во время прямой трансляции, выявляют отклонения и незамедлительно передают информацию оператору или в правоохранительные органы. Подобные технологии все еще находятся на стадии разработки, однако в России уже существуют производители современных камер видеонаблюдения с ИИ.

Деятельность правоохранительных органов. Весной 2024 года сотрудники Новосибирского государственного университета разработали беспилотный летательный аппарат-полицейский, который ориентируется в пространстве без GPS. Дроны будут оснащены системой интеллектуальной навигации. Каждый дрон будет способен летать на расстояние до 30 км и поддерживать активность до 1,5 часов. В планах разработчиков – «обучить» дрон принимать решения с помощью искусственного интеллекта для патрулирования улиц. Однако с учетом того, что специальное регулирование этой сферы еще не сформировано, вероятно появление проблем применения таких дронов и вопросов, касающихся неприкосновенности частной жизни, личной тайны, последствий ошибок и сбоев ИИ-систем.

Новейшие технологии затронули и Прокуратуру России. 24 апреля 2024 года Генеральный прокурор России Игорь Краснов подписал план по внедрению и использованию искусственного интеллекта, нейронных сетей в работе прокуратуры. Нейросети будут использоваться для аналитической работы, прогнозирования роста преступности в отдельных регионах, анализа законопроектов и других документов. Генпрокурор РФ заверил, что речь о замене человека искусственным интеллектом не идет, решение будет принимать человек, но возможности искусственного интеллекта «будут максимально использоваться».

Антикоррупционная экспертиза. Особое внимание правоведы по всему миру уделяют применению ИИ [18] в сфере антикоррупционной экспертизы [23].

В 2010 году в Китае аналитик Джон Киндерваг разработал проект Zero Trust, целью которого является выявление коррупционеров. Получив доступ к 150 базам данных государственного значения, в которых содержится информация о работе и социальной жизни чиновников, искусственный интеллект обработал эти данные и выявил несоответствия, которые могут указывать на нарушение закона чиновниками, среди которых подозрительные банковские транзакции. Так, ИИ зафиксировал нарушения среди 9000 государственных служащих.

По мнению ведущего научного сотрудника Центра технологий государственного управления РАНХиГС при Президенте РФ Алексея Ефремова, «привлечение технологии искусственного интеллекта к проведению антикоррупционной экспертизы позволит повысить ее объективность и выявить ряд коррупциогенных факторов, которые на сегодняшний день не учитываются.

Ключевые возможности данной технологии:

Минимизация субъективизма лиц, проводящих антикоррупционную экспертизу.

Выявление иных типичных коррупциогенных факторов, не подлежащих выявлению на сегодняшний день.

Выявление нетипичных факторов, которые поддерживают коррупционные факторы.

Выявление связи коррупциогенных факторов и коррупционных практик и рынков.

По мнению Алексея Ефремова, внедрение технологии ИИ необходимо осуществить в два этапа, когда «будет проверять только нормативно-правовые акты и их проекты, подлежащие антикоррупционной экспертизе» и когда «такая экспертиза должна затронуть все правовые акты, включая индивидуальные».

Бюджетное регулирование. На Петербургском международном экономическом форуме – 2024 пресс-служба Сбербанка сообщила, что на базе нейросети GigaChat совместно с Министерствам финансов РФ разрабатывается ИИ-агент для оптимизации бюджетного процесса. ИИ-агент будет интегрирован в систему «Электронный бюджет», он возьмет на себя рутинные процессы вычислений, анализа и обработки запросов. Эксперты Минфина будут самостоятельно адаптировать решение на основе искусственного интеллекта и применять навыки работы с большими языковыми моделями при изменении структуры и статей бюджета госпрограмм. Пилотное внедрение запланировано в ближайшем бюджетном цикле.

«Искусственный интеллект станет хорошим подспорьем для финансистов – он возьмет на себя рутинные процессы вычислений и анализа. Однако не стоит забывать, что бюджетный процесс – это решения, связанные в том числе с политикой, с пониманием нужд реальных людей, предприятий, а не цифр на экране. Поэтому последнее слово всегда будет за человеком», – прокомментировал запуск новой технологии министр финансов Антон Силуанов.

«Искусственный интеллект все активнее используется в нашей жизни, в медицине [19, 20], образовании, в бизнес-процессах в любых отраслях экономики. Но и в госуправлении перспективы применения AI колоссальны. Новый AI-агент, которого мы разрабатываем в партнерстве с Минфином на базе GigaChat, окажет огромное содействие бюджетному процессу. Эта передовая разработка в перспективе может внести большой вклад в управление бюджетом и другими ключевыми процессами в госуправлении» [21], – заявил президент, председатель правления Сбербанка Герман Греф.

Заключение. Информация всегда была катализатором социальных изменений и прогресса, а появление новых способов распространения и хранения информации оказало существенное влияние на общество. Россия, вступая в информационное общество, признает значимость цифровизации и внедрения цифровых технологий в различные сферы общественной жизни, в том числе и в правовое поле.

Правовая сфера сталкивается с серьезной проблемой адаптации к процессу цифровизации, поскольку многие правовые концепции, связанные с цифровой эпохой, все еще находятся на ранних стадиях развития. Целью настоящей статьи стало изучение влияния искусственного интеллекта на правотворчество и правоприменение, а также перспективы его внедрения в сферу деятельности законодателей.

Искусственный интеллект способен анализировать крупные пласты информации, поэтому его применение в статистической аналитике позволило бы значительно автоматизировать процесс появления законодательной инициативы. Мониторинг законодательства и судебной практики может, в свою очередь, помочь законодателям определять пробелы в праве и правовые коллизии с целью их дальнейшего совершенствования. Однако применение цифровых технологий в праве

должно осуществляться под пристальным контролем со стороны человека. Усовершенствование механизма ИИ в симбиозе с квалифицированной экспертизой специалистов позволит усовершенствовать законотворческий процесс в России уже в ближайшее время.

Список литературы

1. Смирнов А. В. Цифровое общество: теоретическая модель и российская действительность // Мониторинг общественного мнения: экономические и социальные перемены. 2021. № 1. С. 129–153.

2. Attitudes Towards the Impact of Digitisation and Automation on Daily Life. Special Eurobarometer 460. Report. European Union, 2017.

3. Хабриева Т. Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. № 9. С. 8–20.

4. Самородов В. Ю. Цифровизация в современной культуре правотворчества: тренд на обновление и позитивная тенденция правовой жизни // Актуальные проблемы государства и права. 2020. Т. 4, № 14. С. 166.

5. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации».

6. Язык правотворчества в условиях цифровизации общественных отношений: сборник научных трудов / под общ. ред. Д. А. Пашенцева, М. В. Залоило. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: ИНФРА-М, 2019.

7. Балалаева Ю. С. Изменения правотворческого процесса в условиях развития и внедрения технологий искусственного интеллекта: проблемы и перспективы // Юридическая техника. 2023. № 17. С. 618–622.

8. Язык правотворчества в условиях цифровизации общественных отношений: сборник научных трудов / под общ. ред. Д. А. Пашенцева, М. В. Залоило. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: ИНФРА-М, 2019. С. 101.

9. Талапина Э. В. Искусственный интеллект и правовые экспертизы в государственном управлении // Вестник Санкт-Петербургского университета. Право. 2021. № 4. С. 865–881.

10. Суперсервис «Правосудие онлайн» заработает с 2024 года // ТАСС. URL: tass.ru (дата обращения: 01.05.2024).

11. Рукавишникова рассказала, как цифровизация помогает правосудию // Парламентская газета. URL: pnp.ru (дата обращения: 01.05.2024).

12. Facial recognition used after Sunglass Hut robbery led to man’s wrongful jailing, says suit. Facial recognition // The Guardian (дата обращения: 01.05.2024).

13. Эксперты назвали Россию третьей в мире по числу камер видеонаблюдения // РБК. URL: rbc.ru (дата обращения: 01.05.2024).

14. Научным центром БДД МВД России подготовлен информационно-аналитический обзор «Правоприменительная деятельность в области безопасности дорожного движения в 2023 году» // [сайт] (Дата обращения 01.05.2024).

15. Решения арбитражных судов. URL: arbitr.ru (дата обращения: 01.05.2024).

16. В Новосибирске разработали БПЛА-полицейский, ориентирующийся в пространстве без GPS. URL: turbopages.org (дата обращения: 01.05.2024).

17. Бегишев И. Р. Криминологическая классификация роботов: риск-ориентированный подход // Правоприменение. 2021. Т. 5, № 1. С. 185–201. EDN: TBUVGY

18. Бегишев И. Р., Хисамова З. И. Искусственный интеллект и робототехника: глоссарий понятий. М.: Проспект, 2021. 64 с. EDN: HQELSK

19. Kirpichnikov D. V. et al. Bioprinting Medical Devices: Criminal Evaluation Issues // AIP Conference Proceedings: VII International Conference “Safety Problems of Civil Engineering Critical Infrastructures” (SPCECI2021), Yekaterinburg, 2023. Vol. 2701. P. 020032. EDN: STBLEX

20. Шутова А. А. Цифровой паспорт здоровья: этические и правовые проблемы // Вестник Казанского юридического института МВД России. 2021. Т. 12, № 2(44). С. 236–241. EDN: DPUAMG

21. «Сбер» совместно с Министерством финансов РФ разработал первого AI-агента в госуправлении для оптимизации бюджетного процесса. Новости Национального портала искусственного интеллекта РФ. URL: https://ai.gov.ru/ (дата обращения: 01.05.2024).

22. Концепция цифрового государства и цифровой правовой среды: монография. М.: ИЗиСП: Норма: ИНФРА-М, 2024.

23. Противодействие коррупции и процессы цифровизации: научно-практическое пособие. М.: Инфотропик Медиа, 2023.

24. Залоило М. В. Современные юридические технологии в правотворчестве: научно-практическое пособие / под ред. Д. А. Пашенцева. М.: ИЗиСП: Норма: ИНФРА-М, 2024. 184 с.

А. С. Васильева,
магистрант,
Московский государственный университет имени М. В. Ломоносова

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

Аннотация. Целью статьи является демонстрация целесообразности разработки законодательства о защите персональных данных работников при их обработке искусственным интеллектом. Искусственный интеллект активно используется для осуществления работодательской власти. Однако отсутствует законодательное регулирование, позволяющее защитить персональные данные работника. Следовательно, требуется разработать процедуру предоставления согласия работника на обработку его персональных данных искусственным интеллектом и порядок оспаривания решений искусственного интеллекта.

Ключевые слова: искусственный интеллект, цифровые технологии, персональные данные, защита работника

ARTIFICIAL INTELLIGENCE AND PROTECTION OF PERSONAL DATA OF EMPLOYEES

Abstract. The purpose of the article is to demonstrate the expediency of legislation developing on the protection of personal data of employees during their processing by artificial intelligence. Artificial intelligence is actively used to exercise employer power. However, there is no legislative regulation to protect the employee's personal data. Therefore, it is necessary to develop a procedure for granting an employee's consent to the processing of his personal data by artificial intelligence and a procedure for challenging artificial intelligence decisions.

Keywords: artificial intelligence, digital technologies, personal data, employee protection

Введение. Работодатель, как писал Л. С. Таль, обладает «хозяйской властью», которая проявляется в трех различных формах:

1) диспозитивной – работодатель дает приказания работникам в рамках их трудовой функции;

2) дисциплинарной – работодатель привлекает работника к ответственности за неисполнение или ненадлежащие исполнение трудовой функции;

3) нормативной – работодатель издает локальные нормативные акты организации [4. С. 172–183].

Основная часть. Для реализации данных полномочий работодатель использует работодательский контроль – следит за тем, как работник исполняет свою трудовую функцию.

В настоящие время все данные формы проявления работодательской власти активно опосредуются цифровыми технологиями.

Так, искусственный интеллект [6, 7] активно применяется на этапе трудоустройства работников.

Искусственный интеллект используется для мониторинга работника со стороны работодателя. В период выполнения трудовой функции работодателю важно фиксировать начало и окончание рабочего дня работника, проверять, выполняет ли работник свою трудовую функцию и т. д. [5. С. 357–360].

Применение искусственного интеллекта распространяется и на случаи наложения дисциплинарных взысканий на работников.

В 2022 году компания MAC при сокращении численности штата решила применять искусственный интеллект для выбора работников, с которыми будет расторгнут трудовой договор. Отбор заключался в прохождении видеоинтервью, записи которых анализировались искусственным интеллектом. Оценивались технические навыки, выражение лица работника и его общая вовлеченность в рабочий процесс. Представители компании MAC заявляли, что видеоинтервью было лишь одним из этапов оценивания кандидатов на увольнение и после его анализа искусственным интеллектом следовала проверка видеоинтервью человеком [7].

Повсеместное внедрение цифровых технологий порождает проблемы, связанные с использованием персональных данных. Все они подразделяются на про-

блемы с предоставлением согласия на использование персональных данных и связанная с непосредственной обработкой персональных данных искусственным интеллектом.

Остро стоят проблемы, связанные с получением согласия работника на использование искусственного интеллекта при обработке его персональных данных. Согласно ч. 1 ст. 16 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением наличия письменного согласия субъекта персональных данных [1]. В данном нормативном правовом акте отмечается использование автоматизированных систем. Не каждая автоматизированная система является искусственным интеллектом. Особенность искусственного интеллекта, что он может на основе ранее заложенных алгоритмов создавать новые, поэтому разработчики не могут заранее знать, как обучится данное программное обеспечение и как будет работать в дальнейшем.

Обработка искусственным интеллектом персональных данных несет более высокие риски, чем автоматизированная система, поэтому требует особой процедуры предоставления согласия работника на использование искусственного интеллекта в обработке его персональных данных.

Также требуется уточнить порядок оспаривания решений, принимаемых искусственным интеллектом.

Так, в процессе обработки персональных данных возникает проблема дискриминации соискателей и работников при оценивании их искусственным интеллектом. В случае с компанией MAC было неясно насколько качественно составлена программа для оценки видеоинтервью работников и как учитывались при оценке кандидатов, имеющих разные национальности, особенности их мимики, речи и т. д. В случае с компанией Amazon было неясно, не учитываются ли каким-либо образом факторы места рождения, пола, возраста, семейного статуса и другие, оценка которых могут повлечь дискриминацию. Как отмечает А. Ю. Марченко, отличие искусственного интеллекта от другого программного обеспечения – возможность к самообучению, поэтому даже разработчик не всегда может сказать, как искусственный интеллект компонует и учитывает информацию, приведенную в резюме, данная непрозрачность может вести к дискриминации [3. С. 46].

Проблемы могут возникнуть при использовании искусственного интеллекта как программы для мониторинга работника. Искусственный интеллект полезен, так как позволяет избегать субъективизма при оценке качества и объема работ. В то же время он способен к самообучению. Искусственный интеллект в рамках мониторинга может работать:

– для фиксации наличия работника в поле зрения камеры – он считывает биометрию работника;

– фиксирования изображения на экране; при этом если работник в рамках выполнения трудовой функции использует персональные данные иных работников, то искусственный интеллект может фиксировать и запоминать персональные данные и использовать их в дальнейшем для аналитики.

Искусственный интеллект удобен для установления работодательского контроля над работником, в то же время из-за самообучаемости искусственного интеллекта он может неправомерно использовать персональные данные работников.

В связи с эти необходимо разработать систему защиты персональных данных.

В настоящие время право на оспаривание решения выводится с помощью расширительного толкования из ч. 3 ст. 22 Регламента № 2016/679 Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)» [2]. Однако его требуется уточнить и раскрыть процедуру оспаривания в российских нормативных правовых актах.

Заключение. Таким образом, внедрение искусственного интеллекта оказывает значительное влияние на возможность защиты персональных данных работников. Особенность искусственного интеллекта в том, что он способен к самообучению, при его использовании изменяется первоначальный код, поэтому даже разработчикам становится неясна логика дальнейшего функционирования программы.

Самообучение искусственного интеллекта представляет особую опасность при работе с персональными данными. Их обладатель не может прогнозировать, как и для чего искусственный интеллект будет использовать персональные данные.

Несмотря на большое количество рисков, которые несет искусственный интеллект, он активно используется работодателем при осуществлении работодательской власти.

Для снижения рисков использования искусственного интеллекта целесообразно:

Уточнить в законодательстве процедуру предоставления работником согласия на обработку его персональных данных искусственным интеллектом.

Разработать процедуру оспаривания решений, принимаемых искусственным интеллектом.

Список литературы

1. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ // Российская газета. 2006, 29 июля.

2. О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных) (принят в г. Брюсселе 27.04.2016: Регламент № 2016/679 Европейского парламента и Совета Европейского союза // Official Journal of the European Union. N L 119. 04.05.2016. P. 1.

3. Марченко А. Ю. Правовой анализ новейшего законодательства ЕС о применении технологий искусственного интеллекта: дис. ... канд. юрид. наук. М., 2022. С. 46.

4. Таль Л. С. Трудовой договор: цивилистическое исследование. Часть 2. Внутренний правопорядок хозяйственных предприятий. Ярославль: типография Губернского правления. 1918. С. 172–183.

5. Традиции и новации в системе современного российского права: материалы Международного конгресса молодых ученых, 5–6 апреля 2024 г., Москва: в 3 т. Т 2. М.: Издательский центр Университета имени О. Е. Кутафина (МГЮА), 2024. С. 357–360.

6. Бегишев И. Р., Хисамова З. И. Искусственный интеллект и робототехника: глоссарий понятий. М.: Проспект, 2021. 64 с. EDN: HQELS.

7. Бегишев И. Р. Криминологическая классификация роботов: риск-ориентированный подход // Правоприменение. 2021. Т. 5, № 1. С. 185–201. EDN: TBUVGY

К. А. Васильева,
студент,
Казанский инновационный университет имени В. Г. Тимирясова,
Набережночелнинский филиал

СОСТОЯНИЕ И ПЕРСПЕКТИВЫ ЗАЩИТЫ ПРАВ НА ЦИФРОВЫЕ АКТИВЫ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье рассматриваются правовые аспекты и вызовы, связанные с развитием метавселенной и появлением новых форм цифровых активов, таких как невзаимозаменяемые токены (NFT) и аватары. Акцентируется внимание на иммерсивности метавселенной и ее децентрализованной структуре, подчеркивая необходимость адаптации российского законодательства к современным реалиям цифровой экономики. В работе анализируются существующие нормативно-правовые акты Российской Федерации с целью выявления пробелов в регулировании прав на цифровые активы. Указывается на важность признания правового статуса цифровых активов и разработки специализированных норм для их защиты. Предлагаются дополнения к действующему законодательству, направленные на введение определений для NFT, метавселенной и аватаров.

Ключевые слова: метавселенная, цифровые активы, невзаимозаменяемые токены, интеллектуальная собственность, правовое регулирование, авторское право, цифровые технологии, токенизация, виртуальные объекты, цифровая идентификация, аватар

STATUS AND PROSPECTS OF DIGITAL ASSET RIGHTS PROTECTION IN THE RUSSIAN FEDERATION

Abstract. The article explores the legal aspects and challenges associated with the development of the metaverse and the emergence of new forms of digital assets, such as non-fungible tokens (NFTs) and avatars. The author focuses on the immersive nature of the metaverse and its decentralized structure, highlighting the need to adapt Russian legislation to the current realities of the digital economy. The study analyzes existing regulatory acts of the Russian Federation to identify gaps in the regulation of digital asset rights. It emphasizes the importance of recognizing the legal status of digital assets and developing specialized norms for their protection. The article proposes amendments to the current legislation aimed at introducing definitions for NFTs, the metaverse, and avatars.

Keywords: metaverse, digital assets, non-fungible tokens, intellectual property, legal regulation, copyright, digital technologies, tokenization, virtual objects, digital identification, avatar

Введение. Концепция метавселенной стремительно развивается, интегрируя в себя элементы виртуальной и дополненной реальности, что приводит к созданию новых форм цифровых активов. Принципиальной особенностью метавселенной является так называемая иммерсивность – это способ восприятия, создающий эффект погружения в искусственно созданную среду. Из анализа литературы по информационным технологиям следует, что самым важным признаком метавселенной является то, что она создается на платформе, т. е. это одноранговая, децентрализованная сеть [1. С. 48].

Основная часть. Появление метавселенной, представляющей собой взаимосвязанное пространство виртуальной реальности, повлекло за собой значительные преобразования в области цифровых взаимодействий. Внедрение такой цифровой платформы позволило открыть новые перспективы в сфере развлечений, коммерции и социального взаимодействия. С увеличением распространенности и значимости этой иммерсивной цифровой среды ключевые технологии стремительно вносят изменения в традиционные подходы к пониманию интеллектуальной собственности. С учетом повсеместного внедрения цифровых технологий возникает необходимость переосмыслить существующие правовые механизмы и адаптировать их до уровня, способного адекватно реагировать на вызовы, возникающие в контексте развивающихся цифровых экосистем [8. С. 358].

Возможность токенизации различных видов объектов с помощью решений на основе блокчейна в последнее время привлекла большое внимание [6. С. 9]. В результате чего особого внимания требует утверждение о том, что существующее законодательство РФ по интеллектуальной собственности и цифровым правам, включая Федеральный закон «О персональных данных», Гражданский кодекс РФ и Федеральный закон «Об информации, информационных технологиях и защите информации», в определенной степени может применяться к цифровым активам. Однако специфика метавселенной требует более детального подхода к регулированию.

Одним из основных вызовов для современной правовой системы Российской Федерации является признание прав на цифровые активы, созданные в виртуальных мирах. На данный момент в российском законодательстве отсутствует закрепление правового статуса невзаимозаменяемого токена. Данное упущение в дальнейшем может послужить источником правовых споров и противоречий [2. С. 102].

Сейчас, с точки зрения традиционного авторского права, определить создание NFT как нарушение прав интеллектуальной собственности затруднительно, поскольку эта технология не всегда попадает под привычные правовые рамки. Кроме того, такая позиция непосредственно связана с самой сущностью NFT, который изначально не является предметом искусства. Как правило, NFT представляет собой лишь строку чисел, сгенерированных на основе произведения, в связи с чем такой файл не может рассматриваться в качестве варианта воспроизведения или формы адаптации этого произведения [5. С. 1378].

Обострение этого вопроса связано также с тем, что метавселенная создает новые формы нарушений прав на цифровые активы, такие как несанкционированное копирование, использование и распространение виртуальных объектов. Существующие механизмы правоприменения часто оказываются неэффективными в условиях виртуальной среды. Развивая тематику, учтем, что виртуальные миры не знают границ, что создает дополнительные сложности для определения юрисдикции и применимого права. Это особенно актуально в условиях, когда различные пользователи могут находиться в разных странах с различными правовыми системами.

В связи с чем для адекватной защиты прав на цифровые активы необходимо обновление существующего законодательства. В частности, требуется введение соответствующих правовых дефиниций в законодательные акты, а также разработка специальных норм, регулирующих права и обязанности участников виртуальных миров.

Основной причиной появления понятий «метавселенная», «аватар» и NFT является коммерческий интерес, побуждающий бизнес предлагать рынку новые продукты. Поскольку эти инновации подпадают под правовое регулирование, важно найти эквивалентные термины в российской юридической терминологии. Мы полагаем, что такой подход к усовершенствованию существующей правовой основы регулирования данной сферы поможет избежать ошибок при выборе нормативных правовых актов для регулирования таких отношений. В условиях необходимости приведения действующего законодательства Российской Федерации в соответствие с реалиями цифровых активов требуется правовой подход к определению и интерпретации каждого из этих понятий.

Метавселенная в контексте российского права может рассматриваться как виртуальное пространство, аналогичное информационной системе, обладающей специфическими особенностями. С юридической точки зрения, наиболее близкими понятиями, которые могут быть применены для описания этой цифровой среды, являются «информационные системы», «интерактивные цифровые среды» и «интерактивные сервисы». Однако для корректного правового регулирования этих инновационных технологий необходимо учитывать не только их общие черты с указанными категориями, но и специфические аспекты, такие как обработка и защита персональных данных, охрана интеллектуальной собственности, а также особенности регулирования электронной коммерции. По нашему мнению, внедрение понятия «метавселенная» в Федеральный закон «Об информации, информационных технологиях и защите информации» требует комплексного подхода в дополнение к существующим правовым нормам.

В правовом контексте аватар может быть интерпретирован как форма цифрового представления личности, выступая в качестве идентификатора пользователя в виртуальной среде. Продолжая мысль, акцентируем внимание на главенствующей роли норм права, касающихся защиты персональных данных, поскольку аватары часто включают информацию, позволяющую идентифицировать пользователя. Важно отметить, что существует необходимость учитывать правовые аспекты, связанные с конфиденциальностью и безопасностью, так как использование аватаров может нести потенциальные риски неправомерного доступа и использования личной информации.

С юридической точки зрения, термин «аватар» целесообразно сопоставить с такими понятиями, как «профиль пользователя», «цифровая идентификация» или «средство аутентификации». Эти термины отражают функции аватара как инструмента для подтверждения и отображения личности в цифровом пространстве. Исходя из вышесказанного, можно сделать вывод, что существующие законы о защите персональных данных могут служить отправной точкой для разработки более конкретных правовых норм, регулирующих использование аватаров, особенно в свете их роли в обеспечении безопасности и приватности цифровой личности.

Следует отметить, что термин NFT может быть также рассмотрен в рамках Закона «Об информации, информационных технологиях и о защите информации» как цифровой актив, обладающий уникальными свойствами и связанный с объектами интеллектуальной собственности или цифровыми правами. В правовом поле NFT способен выступать в качестве цифрового аналога имущественного права, что позволяет ему вписываться в понятие «цифровые активы» или «цифровые финансовые активы», подлежащие регулированию в контексте финансовых инструментов. Кроме того, NFT может быть определен как электронный сертификат, удостоверяющий подлинность и право владения конкретным цифровым объектом, будь то произведение искусства, медиафайл или иной контент. В этом контексте применимы термины, связанные с «цифровыми правами», «электронными сертификатами» и «цифровыми активами».

На основе вышеизложенной информации предложим соответствующее дополнение ст. 2 Федерального закона «Об информации, информационных технологиях и защите информации» и изложим ее в следующей редакции:

15.1) невзаимозаменяемый токен (NFT) – уникальный цифровой объект, закрепленный на распределенном реестре (блокчейне), удостоверяющий исключительное право собственности на связанный с ним цифровой или физический актив. NFT характеризуется неделимостью и невзаимозаменяемостью, используется в правоотношениях, связанных с цифровыми активами, и подлежит правовому регулированию в сферах интеллектуальной собственности, цифровой идентификации, гражданского оборота и защиты прав владельцев в соответствии с настоящим Федеральным законом и иными нормативными правовыми актами Российской Федерации;

15.2) метавселенная – децентрализованная виртуальная цифровая среда, созданная с использованием информационных систем, блокчейн-технологий и интерактивных сервисов, позволяющая пользователям взаимодействовать через аватары и владеть цифровыми активами, включая невзаимозаменяемые токены (NFT). Метавселенная подлежит правовому регулированию в части защиты персональных данных, интеллектуальной собственности, прав пользователей и электронной коммерции в соответствии с настоящим Федеральным законом и иными нормативными правовыми актами Российской Федерации;

15.3) аватар – цифровое представление пользователя в виртуальной среде или информационной системе, используемое для идентификации, взаимодействия и участия в действиях, происходящих в этих цифровых пространствах, включая метавселенные. Аватар может обладать различными характеристиками, определяемыми пользователем, и является объектом правового регулирования в части защиты персональных данных, виртуальной идентификации и взаимодействия в

соответствии с настоящим Федеральным законом и иными нормативными правовыми актами Российской Федерации.

Дополнения к статье 2 Федерального закона «Об информации, информационных технологиях и защите информации», включающие определения невзаимозаменяемых токенов (NFT), метавселенной и аватаров, направлены на решение ряда конкретных правовых и практических проблем, возникающих в современной цифровой среде. По нашему мнению, введение определения для NFT занимает одну из ключевых позиций в построении нормативно-правовой базы, которая впоследствии может быть непосредственно применена для защиты прав собственников уникальных цифровых активов, которые не поддаются привычным методам регулирования. Более того, в условиях отсутствия четкого правового статуса такие активы могут стать объектом преступного посягательства, спорных сделок или иных мошеннических действий, а также правовых споров, в том числе в контексте интеллектуальной собственности и трансграничного оборота. Определение NFT в законе позволит однозначно квалифицировать правоотношения с участием этих активов и обеспечить защиту интересов пользователей и инвесторов.

В продолжение научного анализа отметим, что определение метавселенной как понятия необходимо установить законом для определения правил и норм взаимодействия в децентрализованных виртуальных средах, где пересекаются цифровые активы, услуги и пользовательский контент. Метавселенная создает уникальные правовые вызовы, такие как регулирование прав собственности на виртуальные объекты, соблюдение авторских прав и защита данных в среде, где общепризнанные подходы не работают из-за отсутствия централизованного контроля и юрисдикционных границ. Особенно важно для предотвращения правовых конфликтов и защиты интересов пользователей в таких многообразных и динамичных цифровых пространствах.

Говоря о правовом регулировании понятия аватара как цифрового представления пользователя, мы приходим к выводу о том, что такое нововведение поможет сформировать правовые рамки для регулирования цифровой идентификации и взаимодействия в виртуальных средах. В цифровом пространстве аватары выступают посредниками в действиях пользователей, что поднимает вопросы, связанные с идентификацией, защитой личных данных и ответственностью за действия, совершаемые в виртуальной среде. Следует упомянуть, что введение правового статуса аватара создаст основы для регулирования таких действий, обеспечивая защиту как самих пользователей, так и третьих лиц, с которыми они взаимодействуют в виртуальных мирах.

Несмотря на то, что в блокчейн-среде нет четкой связи между NFT и авторским правом, цифровые художники могут оказаться в затруднительном положении, если Закон об авторском праве на данном этапе не способен обеспечить таким художникам средств правовой защиты [7. С. 82].

Таким образом, предложенные дополнения способствуют не только упорядочиванию правовых аспектов, но и формированию более безопасной и контролируемой цифровой экосистемы, что, в свою очередь, привлечет инвестиции и будет развивать инновации в российской цифровой экономике.

На основании проведенного анализа можно заключить, что современное законодательство о метавселенных находится на начальном этапе своего развития, поскольку в большинстве развитых юрисдикций метавселенная рассматривается лишь

как технология будущего. В этой связи особое значение приобретает осведомленность пользователей о правовых аспектах взаимодействия с цифровыми активами, и, следовательно, для успешной защиты своих прав они должны быть информированы о существующих рисках и доступных правовых механизмах защиты.

Для обеспечения эффективной защиты прав на цифровые активы в условиях метавселенной, безусловно, требуется комплексное обновление российского законодательства. В частности, необходимо дополнить правовые акты определениями, касающимися цифровых активов, признать их правовой статус, а также разработать специализированные нормы, регулирующие различные аспекты их использования.

Заключение. Таким образом, только такой всесторонний и продуманный подход позволит создать надежную правовую основу для защиты цифровых активов и успешного развития метавселенной в России. Важно, чтобы изменения в законодательстве шли в ногу с развитием технологий, учитывая их динамичность и сложность. Авторы предлагают весьма интересные концепции внесения изменений в действующее законодательство [4. С. 7–32]. Признание правового статуса цифровых активов, внедрение новых правовых норм и развитие институтов, ответственных за разрешение споров, будет способствовать формированию устойчивой правовой среды. В итоге это создаст условия для защиты прав пользователей и бизнеса, укрепит доверие к цифровым технологиям и поспособствует активному развитию метавселенной [3. С. 200], что, без сомнения, окажет положительное влияние на развитие цифровой экономики страны в целом.

Список литературы

1. Мансуров Г. З. Правовой режим аватаров NFT в метавселенной // Вестник Уральского юридического института МВД России. 2023. № 4. С. 47–51.

2. Синицына А. Д. NFT как новый объект гражданского права в Российской Федерации // ПРЭД. 2023. № 3. С. 99–105.

3. Ситников М. С. Финансово-правовое развитие общественных отношений с использованием цифровых валют в метавселенных // Journal of Digital Technologies and Law. 2024. № 1. С. 200–219.

4. Филипова И. А. Создание метавселенной: последствия для экономики, социума и права // Journal of Digital Technologies and Law. 2023. № 1. С. 7–32.

5. Guadamuz A. The treachery of images: non-fungible tokens and copyright // Journal of Intellectual Property Law & Practice. 2021, December. URL: https://doi.org/10.1093/jiplp/jpab152 (дата обращения: 06.08.2024).

6. Kaisto J., Juutilainen T., Kauranen J. Non-Fungible Tokens, Tokenization, and Ownership // Computer Law & Security Review. 2024. Vol. 54. URL: https://doi.org/10.1016/j.clsr.2024.105996 (дата обращения: 07.08.2024).

7. Siriwardane H., Wirtz M., Loudermilk K. The Rise of NFTs: Transforming Intellectual Property Rights in the Digital Age // The Journal of World Intellectual Property. 2024. Vol. 27, № 3.

8. Wyczik J. The rise of the metaverse: tethering effect and intellectual property of crypto tokens // Journal of Intellectual Property Law & Practice. 2024. № 4.

А. А. Виноградова,
студент,
Казанский инновационный университет имени В. Г. Тимирясова

ТРЕШ-СТРИМ С ТОЧКИ ЗРЕНИЯ УГОЛОВНОГО ПРАВА

Аннотация. В качестве цели исследования, поставленной в работе, выступает изучение такого явления, как треш-стримы, с точки зрения уголовного права. Количество треш-стримеров с каждым годом увеличивается все больше, а контент, выкладываемый на площадках в сети Интернет, становится только страшнее (все чаще появляются ролики аморального и противоправного характера), в связи с этим вырастает необходимость научного изучения данной тенденции для разработки способов предотвращения проявления этого девиантного поведения, а также проведения анализа уже имеющихся способов, в том числе и законодательных.

Ключевые слова: треш-стрим, стримеры, публичная демонстрация, преступления, уголовное право, уголовное законодательство, девиантное поведение

THRASH STREAM FROM A CRIMINAL LAW PERSPECTIVE

Abstract. The aim of the research set in the paper is to study such phenomenon as thrash-streamers from the point of view of criminal law. The number of thrash streamers is increasing faster and faster every year, and the content posted on sites on the Internet is only getting scarier (more often there are clips of immoral and illegal nature), in this regard there is a need for scientific study of this trend to develop ways to prevent the manifestation of this deviant behavior, as well as the analysis of existing ways, including legislative.

Keywords: thrash stream, streamers, public demonstration, crimes, criminal law, criminal legislation, deviant behavior.

Введение. Треш-стрим – это онлайн-трансляция, в ходе которой зрители наблюдают за тем, как стример (ведущий) совершает в отношении себя или других людей действия, классифицирующиеся как опасные, противоправные, аморальные, оскорбительные или причиняющие физический и (или) моральный вред [4].

Основная часть. Проанализировав основные направления снимаемого контента, предложена следующая классификация треш-стримов:

1) алко- и наркостримы – онлайн-трансляция злоупотребления алкогольными напитками и (или) наркотическими веществами;

2) секс-стримы – трансляция девиантного сексуального поведения;

3) треш-стримы насильственного характера – вещание различных видов насильственных действий (физическое, моральное). Можно разделить на два подвида:

– суицидальные (самоповреждающие);

– направленные на третьих лиц (соведущего, зрителей и т. д.);

4) асоциальные треш-стримы – прямые эфиры, транслирующие асоциальное поведение (драки, истерики, конфликтные ситуации и др.).

Изучение данного явления с точки зрения уголовного права и разработка способов их предотвращения необходимы, поскольку были неоднократные случаи

демонстрации преступных деяний. Это и обуславливает актуальность выбранной темы исследования.

В качестве примера можно привести материалы судебной практики по наиболее ярким и освещенным СМИ делам. В качестве одного из таких выступает дело по стримеру М. В. Королеву. 13 декабря 2023 года Навлинский районный суд Брянской области вынес приговор жителю Приморского края, признанному виновным в совершении преступления, предусмотренного пунктами «а», «г» ч. 2 ст. 117 УК РФ. Королев Михаил с целью получения материального дохода от добровольных пожертвований зрителей («донатов») в прямом эфире на своем канале, действуя умышленно, причинял потерпевшей физическую боль и психические страдания путем систематического нанесения побоев и иных насильственных действий, демонстрируя беспомощность и унижая человеческое достоинство потерпевшей. Приговором суда виновному назначено наказание в виде 3 лет лишения свободы с отбыванием наказания в исправительной колонии общего режима [2].

В качестве еще одного примера можно привести дело Reeflay (блогера Станислава Решетняка). Блогер в прямом эфире совершил непредумышленное убийство своей подруги Валентины Григорьевой. Это вызвало общественное волнение не только в России, но и за рубежом. Блогер в момент совершения преступления находился в алкогольном опьянении, в ходе ссоры нанес множество телесных повреждений, которые стали причиной образования черепно-мозговой травмы. Смерть Валентины Григорьевой наступила на месте происшествия. Вину подсудимый признал. По приговору Раменского городского суда Московской области Решетняк признан виновным по ч. 4 ст. 111 УК РФ и приговорен к 6 годам колонии строгого режима [3].

Этот список судебных дел не является исчерпывающим, что доказывает вышеуказанное утверждение по поводу того, что демонстрация преступлений при проведении прямых эфиров на различных площадках сети Интернет начала увеличиваться. На стримах могут транслироваться преступления не только против жизни и здоровья, но и против свободы, чести и достоинства личности, против собственности, против общественной безопасности и т. д. Однако опасность подобных стримов состоит не только в совершении противоправного деяния самим блогером, но и в пропаганде этого девиантного поведения. В связи с этим необходима разработка специальных методов и средств по предотвращению этой тенденции [5].

Одним из решений данной проблемы является вступление в законную силу изменений в УК РФ от 8 августа 2024 г., согласно которым совершение преступлений с публичной демонстрацией, в том числе в СМИ или сети Интернет, в ряде норм признано обстоятельством, отягчающим наказание [1]. То есть раньше проведение во время преступления стрима признавалось только лишь доказательством совершения данного преступления, а сейчас будет влиять и на выбранную судом меру наказания.

Предупреждение совершения аналогичных преступлений будет достигаться за счет:

– назначения справедливого наказания;

– обнародования фактов выявления и осуждения таких лиц.

Эффективность принятия данных изменений пока невозможно оценить по причине короткого срока действия данных норм во времени.

В случаях негативной статистики для снижения количества треш-стримов предлагается по таким делам привлекать к уголовной ответственности не только самих блогеров, но и владельцев площадок для онлайн-трансляций в случаях отсутствия мониторинга выкладываемого контента (в виде штрафа). Кроме этого, предлагается законодательно закрепить понятие «треш-стрим», поскольку это позволит определить конкретные действия, которые будут подпадать под нормы уголовного законодательства. Данные изменения позволят судам при рассмотрении дела правильно оценить опасность прямого эфира в конкретном деле.

Вопрос ответственности зрителей треш-стримов на данный момент является открытым, поскольку их нельзя рассмотреть ни в качестве подстрекателей, ни в качестве пособников.

Заключение. Таким образом, в настоящее время уже реализуются некоторые способы решения проблемы распространения такого явления, как треш-стримы, однако проработка имеющихся законодательных норм и дальнейшее развитие профилактических способов не должны прекращаться, поскольку эта проблема может породить ряд других.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 г. (ред. от 08.08.2024 г.) // Собрание законодательства РФ. 1996. 17 июня. № 25. Ст. 2954; 2024. № 33 (Часть 1). Ст. 4914.

2. Архив Навлинского районного суда Брянской области. // Официальный сайт Навлинского районного суда Брянской области. URL: https://navlinsky--brj.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=204828985&delo_id=1540006&new=0&text_number=1 (дата обращения: 04.09.2024).

3. Архив Раменского городской суд Московской области // Официальный сайт Раменского городской суд Московской области. URL: https://ramenskoe--mo.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=280356041&delo_id=1540006&new=&text_number=1 (дата обращения: 02.09.2024).

4. Алексеева Т. Треш-стрим с точки зрения уголовного права // Аналитический центр уголовного права и криминологии. URL: https://crimexpert.ru/2021/10/27/треш-стрим-с-точки-зрения-уголовного-п (дата обращения: 03.09.2024).

5. Закон о запрете треш-стримов: за какой контент будут наказывать и что грозит блогерам // Тинькофф-журнал. URL: https://journal.tinkoff.ru/news (дата обращения: 04.09.2024).

Д. А. Власенко,
магистрант,
Санкт-Петербургский государственный университет

ПРОБЛЕМНЫЕ АСПЕКТЫ РЕГУЛИРОВАНИЯ ВИРТУАЛЬНОГО ИМУЩЕСТВА

Аннотация. Виртуальное имущество является одной из наиболее обсуждаемых тем в цифровом праве по причине его инвестиционной привлекательности и большого количества проблемных вопросов. Среди них можно выделить, например, отсутствие универсального определения, различие правовой природы виртуальных объектов в мире, оправданность вмешательства государства в регулирование отношений, связанных с виртуальными объектами, и трудности при определении личности нарушителя. Решение каждой из проблем разнится от государства к государству, что создает препятствия при разрешении споров в каждой юрисдикции. В данном исследовании в качестве компромисса предлагается избрание регулирования виртуального имущества с помощью договорного права с обеспечением слабой стороны таких отношений минимальным набором прав во избежание формирования монополии.

Ключевые слова: виртуальное имущество, виртуальные объекты, криптовалюта, игровая индустрия, видеоигры, пользовательское соглашение, право собственности

PROBLEMATIC ASPECTS OF REGULATION OF VIRTUAL PROPERTY

Abstract. Virtual property is one of the most discussed topics in digital law due to its investment attractiveness and a large number of problematic issues. These include, for example, the lack of a universal definition, the different legal nature of virtual property in the world, the justification for state intervention in the regulation of relations concerning virtual property, and difficulties in determining the identity of the infringer. The solution to each of the problems varies from state to state, which creates obstacles in resolving disputes in each jurisdiction. This study proposes as a compromise to regulate virtual property through contract law, providing the weaker party to such relationships with a minimum set of rights to avoid monopoly formation.

Keywords: virtual property, virtual objects, cryptocurrency, gaming industry, video games, user agreement, property right

Введение. Виртуальное имущество является одной из самых активно обсуждаемых тем в цифровом праве, особенно в рамках правового регулирования игровой индустрии. Способствует такому ажиотажу и инвестиционная привлекательность таких объектов. Согласно прогнозу мирового поставщика данных о рынке игр и аналитической информации Newzoo объем только лишь игрового рынка в 2024 году составит 189,3 миллиардов долларов США [20]. До сих пор остается неопределенность в отношении того, какова природа виртуального имущества, стоит ли распространять на него нормы вещного права и права собствен-

ности, насколько оправданы вмешательство государства и использование легальных механизмов в «виртуальном мире», как установить нарушителя права на виртуальный объект.

Среди первых зарубежных исследователей, обнаруживших проблемы, кроющиеся в определении, что является виртуальной собственностью, были такие ученые, как Г. Ластовка, Д. Хантер, Э. Кастронова, Дж. Фэрфилд [1. С. 96–97]. Последний, в частности, попытался объяснить суть виртуального имущества как конкурирующий, постоянный и взаимосвязанный код, который имитирует характеристики реального мира [18. С. 1053]. В России законодательно закрепленного определения виртуального имущества на данный момент не существует, что понимается исследователями как одна из проблем, требующих скорого решения. Доктор юридических наук М. А. Рожкова предлагает относить к виртуальному имуществу нематериальные объекты, обладающие экономической ценностью, которые притом могут быть использованы только в виртуальном пространстве [10]. Определения, предлагаемые М. А. Рожковой и Дж. Фэрфилдом, являются довольно широкими и могут подразумевать объемный перечень виртуальных объектов без четко очерченных границ отнесения их к таким объектам.

Основная часть. Чаще всего к виртуальному имуществу относят игровое имущество, криптовалюту, виртуальные токены, доменные имена, виртуальное имущество в социальных сетях и др. Поскольку список таких объектов не исчерпывающий, а мир в эпоху цифровизации меняется все быстрее, что приводит к появлению и развитию новых виртуальных объектов, законодательное регулирование оказывается не всегда достаточным для разрешения того или иного спора. Например, в деле № А41-4212/20 Арбитражный суд Московской области отказал истцу в удовлетворении иска о взыскании неосновательного обогащения в связи с тем, что обеспечительный платеж был осуществлен посредством перевода криптовалюты. Суд указал, что в РФ нет нормативных правовых актов, которые бы регулировали рынок «виртуальной валюты», а потому все подобные операции осуществляются на свой риск [8]. Аналогичный результат последовал в деле № А40-164942/2019, в котором суды трех инстанций сошлись во мнении, что операции с использованием криптовалюты не защищены законодательством РФ. Так как истец требовал возмещения в долларах, суды также пояснили, что из-за сугубо цифрового возникновения криптовалюты эквивалентный возврат в натуре не может быть осуществлен [7]. Интересен тот факт, что суды отметили отсутствие возможности возврата данной виртуальной валюты по причине отсутствия такого способа защиты права среди тех, что перечислены в ст. 12 ГК РФ. Этот аргумент является спорным, поскольку список способов защиты не является исчерпывающим и в случае законодательного регулирования оборота криптовалют не будет являться препятствием для предъявления подобных исков в будущем. Лишь в августе 2024 года Президентом Российской Федерации В. В. Путиным был подписан Закон о легализации майнинга криптовалют, хотя в России майнеры начали осуществлять свою деятельность еще в начале 2010-х гг. Теперь, согласно Федеральному закону от 8 августа 2024 г. № 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», установлены порядок и условия ведения деятельности лицами, осуществляющими майнинг цифровых валют [14].

Не стоит говорить о нерасторопности лишь отечественных законодателей. В американском штате Арканзас, например, в 2023 году был предложен законопроект, приравнивающий майнинговые компании к дата-центрам, что позволит взыскивать с таких компаний налоги и комиссии, которые уплачиваются дата-центрами в штате, и вести свою деятельность, не перегружая местную энергетическую инфраструктуру. Помимо обязанностей, законопроект направлен на защиту майнеров, а потому был положительно встречен как политиками, так и непосредственно экспертами в области криптовалют. Напротив, штат Техас стремится снизить количество желающих заниматься добычей криптовалюты, приняв ряд ограничений, что объясняется потребностью снизить давление на местную электросеть [3]. Таким образом, на примере криптовалют видно, что законодательство часто оказывается неготовым к регулированию принципиально новых виртуальных объектов, вследствие чего в течение десятка лет воцаряется хаос как в законодательстве, так и в правоприменительной практике.

В связи с вышесказанным возникает вопрос: а так ли необходимо правовое регулирование виртуального имущества? Кандидат юридических наук А. И. Савельев, акцентируя внимание преимущественно на «игровом имуществе» как разновидности виртуального имущества, выделил три существующих на сегодня подхода квалификации отношений, возникающих в связи с оборотом и неправомерным завладением виртуальными объектами [11, С. 131]. Рассмотрим каждый из них подробнее.

Во-первых, государство может вовсе не вмешиваться в игровые процессы. Данный подход соотносится с позицией Йохана Хейзинги, голландского историка и автора книги Homo Ludens, который полагал, что участие в игре должно быть отделимо от реальности, оно подобно вхождению в «магический круг», где искусственно созданные правила воспринимаются людьми как реальные [19. С. 8]. Российские суды также придерживаются схожей позиции при рассмотрении споров, связанных с аккаунтами пользователей популярных онлайн-игр. При этом нормативное обоснование в отказе истцам в судебной защите судьи находили в ст. 1062–1063 ГК РФ. В частности, иск о возмещении ущерба в связи с блокировкой аккаунтов истца в игре Lineage 2, предъявленный к ООО «Иннова Системс», не был удовлетворен со ссылкой на п. 1 ст. 1062 ГК РФ [9]. Однако здесь интересен тот факт, что судом было отмечено нарушение истцом правил игры, что являлось причиной блокировки. Аналогичные этому решения судов нередко осуждаются юристами в сфере цифрового права как пример некорректного изложения правовой нормы [1. С. 31], а вследствие этого ее неверного толкования, ведь под «пари» и «играми» по смыслу ст. 1062–1063 ГК РФ подразумеваются вовсе не видеоигры (или компьютерные игры, как устоявшееся определение, используемое в отношении любых виртуальных игр), где нет как такового проигравшего и выигравшего [11. С. 132]. Более того, как отмечал А. Г. Федотов в своем исследовании, игры и пари априори являются сделками, заключенными под влиянием заблуждения [15. С. 41]. Отсутствие этих двух статей привело бы к попыткам признать их незаключенными или недействительными. Видеоигры изначально не предполагают наличие заблуждения в отношениях между сторонами, игрок понимает, что получит определенный виртуальный объект, если заплатит установленную сумму иг-

ровой валюты или реальных денег. То есть фактически данный подход основывается вовсе не на концепции «магического круга», а на ошибочном применении норм о пари и играх к отношениям, ими не являющимся. С другой стороны, при должном обосновании он имеет место существовать как способ разгрузить суды и оставить подобные споры на саморегулирование в пределах игры.

Во-вторых, на виртуальные объекты можно распространить нормы о вещах и праве собственности, что уже активно используется в Восточной Азии. В 2011 году в Тайване, например, Министерство юстиции издало постановление, где за объектами виртуальной собственности закреплялся статус собственности в правовом смысле, т. е. они признавались отчуждаемыми и передаваемыми, а за нарушение прав на них следовала уголовная ответственность [18. С. 1086]. Сторонники данного подхода ставят виртуальные объекты между объектами интеллектуальной собственности и традиционными объектами права собственности, так как, с одной стороны, они не имеют под собой творческого начала, а с другой – у них отсутствует материальное выражение, поскольку существуют они лишь как код, воспроизводимый электронно-вычислительной машиной [17. С. 80]. В качестве обоснования данной позиции нередко в пример приводятся высказывания английского философа Джона Локка, который допускал, чтобы вещи принадлежали тому, кто затратил на них свой труд, хотя до этого все обладали на них правом собственности [4. С. 26]. То есть человек, затрачивая свой труд и время на приобретение виртуального объекта, хоть тот фактически существует только в виртуальном пространстве и представляет собой лишь набор пикселей, все же должен получать права на этот объект, чтобы защитить себя от посягательств, которые могли бы повлечь кражу, уничтожение этого объекта. В США, несмотря на предложение распространить на виртуальное имущество нормы общего права о праве собственности, вопрос остался неразрешенным, ведь индустрия высокобюджетных игр не заинтересована в предоставлении хоть каких-либо прав игрокам. Это также объясняет стремление игровых компаний перевести пользователей на формат подписок на сервисы вместо предоставления им физических копий игр [6], которые сейчас в основном продаются как коллекционный товар и, если мы говорим о компьютерных версиях, представляют собой код, который все еще требует подключения к тому или иному сервису. Например, для получения доступа к игре Baldur`s Gate III требуется регистрация на платформе разработчиков [16], а эксклюзивные виртуальные объекты (уникальную одежду для персонажа) можно было получить только после регистрации на стриминговой платформе Twitch. Таким образом, поддержке данного подхода часто противостоит бизнес, интересы которого в странах с развитой экономикой ставятся выше интересов конечных пользователей. Однако, как в случае с криптовалютой, в США существует вероятность установления минимальных мер по защите прав потребителей в области виртуального имущества на уровне штатов. В России пока нельзя говорить о массовой поддержке такого подхода, тем более для его применения могут потребоваться значительные изменения в российском законодательстве, какие в свое время понадобились для выработки особого режима исключительных прав [11. С. 142].

В-третьих, виртуальные объекты возможно регулировать посредством договорного права. Если проанализировать мировую практику, то это, пожалуй,

наиболее распространенный подход, который встречается, например, при заключении click-wrap соглашений. Виртуальные объекты с точки зрения договора могут рассматриваться как лицензионный платеж, за который лицензиат получает право использования некоторого виртуального имущества. По сути, подобный подход представляет собой монополию лицензиара, который волен указывать в таком договоре всевозможные условия, не всегда направленные на обеспечение прав пользователей. Например, в Соглашении подписчика цифровой платформы распространения компьютерных игр Steam прямо указано на лицензионный характер использования сервиса и различных услуг, а коллективные иски прямо им запрещены [12], что подтверждает высказанное выше суждение о монополии в рамках установления правил. Более того, подобные пользовательские соглашения часто не определяют правовой статус виртуальных объектов, поэтому их регулирование лицензиаром может варьироваться от случая к случаю. На уже упомянутой платформе Steam у пользователей есть право вернуть деньги за покупку игры, если в нее было наиграно менее 2 часов, однако в некоторых случаях это ограничение снимали. Например, якутская студия Fntastic добилась ажиотажа вокруг игры посредством привлекательных трейлеров и иной рекламы, собрала деньги с предзаказов, а после выхода самой игры, которая оказалась значительно хуже ожиданий игроков, закрылась и заявила, что возвращать деньги никому не будет, а сервера игры будут вскоре закрыты. В такую вопиющую ситуацию пришлось вмешаться самой платформе Steam, где была выпущена игра, поддержка которой заверила обманутых пользователей, что деньги им будут возвращены, даже если ими было наиграно более двух часов [2]. Следовательно, нельзя однозначно определить данный подход как неудачный, однако, на мой взгляд, он требует закрепления на национальном уровне минимального набора прав граждан во избежание чрезмерного ущемления прав лицензиатов, которые в большинстве таких соглашений повлиять на их содержание никак не могут.

Исходя из вышесказанного, у каждого из трех подходов есть как преимущества, так и недостатки, которые не позволяют на сегодня сформировать универсальный подход квалификации отношений, связанных с виртуальным имуществом. Необходимым компромиссом является переход российского государства, в частности отечественных судов, с невмешательства в регулирование виртуального имущества на регулирование таких отношений с помощью договорного права. Притом влияние государства не должно быть больше того, что необходимо для защиты минимальных прав и интересов слабой стороны (потребителя, пользователя, игрока). Рассмотренный выше зарубежный опыт показывает способность таких отношений подлежать саморегулированию, чрезвычайное вмешательство государства, напротив, может негативно сказываться на ведении бизнеса и на самом игровом опыте, который, как отмечал Й. Хейзинга, не должен пересекаться с реальностью [19. С. 8]. Тем более существует много положительных примеров, когда посягательства на виртуальное имущество решались в пределах виртуального пространства. Например, разработчики игры Impressive Space создали отдельную категорию обсуждений в социальной сети «ВКонтакте», где игроки могли пожаловаться на посягательства на их виртуальное имущество, после чего аккаунт нарушителя блокировался, а украденные виртуальные объекты возвращались их «собственнику» [5].

Здесь кроется последняя выделенная нами проблема, которая заключается в поиске субъекта правонарушения. Если в случае с игровой индустрией и социальными сетями препятствий к применению санкций к нарушителю не так много, особенно если нарушитель находится в той же юрисдикции, что и потерпевший, то в случае с криптовалютой и виртуальными токенами не все так просто. Особенность взаимодействий продавца и покупателя при обороте таких виртуальных объектов не дает с точностью установить личность и местонахождение человека. Можно ли признавать сделку по приобретению криптовалюты действительной, если неустановленная личность является несовершеннолетним или недееспособным? С проблемой определения субъекта правонарушения также столкнулись ряд художников, рисунки которых преобразовывались в токены и продавались за реальные деньги без их на то ведома. Британскому художнику комиксов Лиам Шарп и некоторым другим лицам, работающим в творческой сфере, приходилось закрывать свои галереи и профили, так как их работы выставляли на продажу в виде NFT-коллекций. Безусловно, существует возможность подачи иска в защиту своих авторских прав, однако, по словам потерпевших, практически невозможно угнаться за вновь создаваемыми виртуальными объектами, основой которых является чье-то нарушенное право [13]. Нередко сделки с NFT отождествляют с отмыванием денег в связи с отсутствием налогов и каких-либо ограничений для осуществления подобных операций. Обеспечение государством минимальных прав и необходимых ограничений позволило бы сократить количество нарушений и защитить участников таких отношений. Такие законодательные изменения должны быть небольшими и скорыми, направленными на первичное регулирование новых виртуальных объектов, поскольку крупномасштабные реформы в законодательстве требуют порой слишком много времени, которого недостаточно для следования за быстро меняющимся виртуальным пространством.

Заключение. Подводя итог, можно сделать вывод, что в настоящий момент не существует универсального определения понятия «виртуальное имущество». Не прекращаются попытки исследователей сформулировать особенности и содержание данного термина, но нередко они сталкиваются с критикой из-за своей абстрактности или по причине чрезмерного уклона в техническую часть этого понятия. Решение данной проблемы законодателями сделало бы шаг навстречу выработке новых правовых норм, направленных на регулирование виртуальных объектов. В ином случае виртуальное имущество в России часто остается вне правового контроля, что становится причиной отсутствия защиты потерпевших при посягательстве на их виртуальные объекты.

В отличие от невмешательства Российского государства в такие отношения в других странах распространено применение норм вещного права и права собственности к виртуальным объектам или регулирование отношений между сторонами на основе договорного права. Несмотря на возможное установление монополии одной из сторон в случае с последним подходом, регулирование посредством договора видится наиболее удачным как для бизнеса, так и для государства. Так, государство будет вмешиваться в оборот виртуальных предметов в минимальных пределах, не препятствуя ведению экономической деятельности и не нагружая собственную судебную систему бесчисленными делами по взаимодействию с виртуальными объектами.

В таком случае государству будет достаточно обеспечить слабую сторону таких отношений минимальным набором прав, которые позволят не допустить полного бесправия пользователя, чье виртуальное имущество могут отобрать или ликвидировать без веской на то причины. Говоря даже о минимальном вмешательстве государства, мы можем поднять проблему определения личности нарушителя.

Не всегда возможно установить субъекта правонарушения, если сам оборот виртуальных объектов предполагает анонимность. Пока что не существует однозначного ответа на вопрос, готовы ли стороны таких отношений раскрывать свои личности, чтобы в случае посягательства на их права была бы возможность обратиться за защитой в органы государственной власти. То есть некоторые виртуальные объекты могут ограничивать государственное вмешательство, исходя из своих особенностей.

По итогам исследования можно заключить, что виртуальное имущество недостаточно урегулировано во многих государствах мира, что усугубляется неопределенностью субъектов отношений, связанных с оборотом виртуальных объектов, и отсутствием терминологического базиса. Следовательно, необходима быстрая выработка минимальных прав и обязанностей для сторон таких отношений, ведь значительные по объему законодательные реформы требуют больших временных затрат, непозволительных с точки зрения быстро меняющегося виртуального пространства.

Список литературы

1. Видеоигры, гейминг, киберспорт: правовые вопросы = Video games, gaming, cybersports: legal issues: коллективная монография / под науч. ред. М. А. Рожковой, Р. Л. Лукьянова. М.: Развитие правовых систем, 2023. 240 с.

2. Всем игрокам The Day Before начали возвращать деньги // Сайт новостного отдела VK Play Media. 2023, 14 декабря. URL: https://media.vkplay.ru/news/2023-12-14/vsem-igrokam-the-day-before-nachali-vozvrashat-dengi-v-steam (дата обращения: 10.08.2024).

3. В США майнинговые компании приравняли к дата-центрам. Что это значит и к чему приведет? // 2bitcoins.ru. 2023, 11 апреля. URL: https://2bitcoins.ru/majningovye-kompanii-v-ssha (дата обращения: 10.08.2024).

4. Локк Д. The Second Treatise of Government. Второй трактат о правлении. М.: Юрайт, 2024. 148 с. (Читаем в оригинале). URL: https://urait.ru/bcode/540472 (дата обращения: 10.08.2024).

5. Обсуждение «Книга жалоб» сообщества Impressive Space // Сайт ВКонтакте. URL: https://media.vkplay.ru/news/2023-12-14/vsem-igrokam-the-day-before-nachali-vozvrashat-dengi-v-steam (дата обращения: 10.08.2024).

6. Почему все игровые издатели хотят подсадить вас на подписку // Shazoo.ru. 2019, 21 июня. URL: https://shazoo.ru/2019/06/21/81009/pochemu-vse-igrovye-izdateli-hotyat-podsadit-vas-na-podpisku (дата обращения: 10.08.2024).

7. Решение Арбитражного суда города Москвы от 29.11.2019 по делу № А40-164942/2019 // Банк решений арбитражных судов «Электронное правосудие». URL: https://kad.arbitr.ru/Card/db741b81-cf91-4880-99b3-140e4b4e15c1 (дата обращения: 10.08.2024).

8. Решение Арбитражного суда Московской области от 31.08.2020 по делу № А41-4212/20 // Банк решений арбитражных судов «Электронное правосудие». URL: https://kad.arbitr.ru/Card/063d733a-50e2-4357-94b2-038b79263ca0 (дата обращения: 10.08.2024).

9. Решение мирового суда судебного участка № 352 Басманного района г. Москвы от 01.02.2011 по делу № 02-0001/362/2011 // Портал единого информационного пространства мировых судей г. Москвы. URL: https://mos-sud.ru/362/cases/civil/details/7a56af32-be74-4c0b-ab29-83d77bddaeeb?caseNumber=02-0001/362/2011 (дата обращения: 10.08.2024).

10. 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 (дата обращения: 10.08.2024).

11. Савельев А. И. Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх // Вестник гражданского права. 2014. № 1. С. 127–150.

12. Соглашение подписчика Steam (с изм. от 02.12.2022) // Сайт цифровой платформы распространения компьютерных игр Steam. URL: https://store.steampowered.com/subscriber_agreement/russian (дата обращения: 10.08.2024).

13. Темная сторона NFT: как от модной технологии страдают художники // Медиаплатформа DTF. 2021, 29 декабря. URL: https://dtf.ru/gameindustry/1011214-temnaya-storona-nft-kak-ot-modnoi-tehnologii-stradayut-hudozhniki (дата обращения: 10.08.2024).

14. Федеральный закон от 08.08.2024 № 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/document/0001202408080016 (дата обращения: 10.08.2024).

15. Федотов А. Г. Игры и пари в гражданском праве // Вестник гражданского права. 2011. № 2. С. 25–74.

16. Collector's edition of Baldur's Gate 3 [Electronic resource] // Baldur's Gate 3 Pre-order site. 2023, Dec. URL: https://ce.baldursgate3.game (access date: 10.08.2024).

17. Duranske B. T. Virtual Law: Navigating the Legal Landscape of Virtual Worlds. Chicago: ABA Publishing, 2008. P. 461.

18. Fairfield J. Virtual Property // Boston University Law Review. 2005. Vol. 85. P. 1047.

19. Huizinga J. Homo Ludens : a study of the play element in culture. London: Routledge & Kegan Paul, 1949. P. 219.

20. Newzoo: Global games market expected to grow to $187bn in 2024 [Electronic resource] // GamesIndustry.biz. 2024, Jan. 23. URL: https://www.gamesindustry.biz/newzoo-global-games-market-expected-to-grow-to-189bn-in-2024 (access date: 10.08.2024).

В. Д. Гаврилова,
студент,
Волгоградский государственный университет

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ПРАВОВОГО СТАТУСА ЦИФРОВОГО ГРАЖДАНИНА В РОССИИ И ЗА РУБЕЖОМ: НОРМАТИВНЫЕ И ПРАВОПРИМЕНИТЕЛЬНЫЕ АСПЕКТЫ

Аннотация. В статье утверждается, что термины «цифровое гражданство» и «цифровой гражданин» являются показателями уровня новой социоправовой реальности и отражением необходимости правового регулирования цифровой среды, в которой живет современный человек, юридизации цифрового гражданства. Сформулирован понятийно-категориальный аппарат цифрового гражданства. Проанализирована практика ЕАЭС, показывающая проблемы, с которыми сталкиваются цифровые граждане при ошибках цифровизации. Проведено сравнение порталов электронных правительств РФ, ОАЭ, Мальты, показано, как цифровой гражданин взаимодействует с органами власти и как государства принимают меры к повышению цифрового образования граждан и их правовой культуры.

Ключевые слова: цифровое гражданство, цифровой гражданин, цифровая культура, цифровая идентичность, цифровое образование

Исследование выполнено за счет гранта Российского научного фонда № 24-28-01342 «Правовая культура цифровых граждан».

FEATURES OF THE IMPLEMENTATION OF THE LEGAL STATUS OF A DIGITAL CITIZEN IN RUSSIA AND ABROAD: REGULATORY AND LAW ENFORCEMENT ASPECTS

Abstract. The author believes that the terms "digital citizenship" and "digital citizen" are indicators of the level of a new socio-legal reality and reflect the need for legal regulation of the digital environment in which a modern person lives, the legitimization of digital citizenship. The conceptual and categorical apparatus of digital citizenship is formulated. The practice of the EAEU is analyzed, showing the problems faced by digital citizens with digitalization errors. The comparison of the portals of the electronic governments of the Russian Federation, the UAE, and Malta is carried out, it is shown how a digital citizen interacts with authorities and how states take measures to improve the digital education of citizens and their legal culture.

Keywords: digital citizenship, digital citizen, digital culture, digital identity, digital education

The research was carried out at the expense of a grant from the Russian Science Foundation No. 24-28-01342 "Legal culture of digital citizens".

Введение. Сегодня гражданин использует продукты электронного и цифрового правительства и правосудия, реализуя новые формы осуществления прав

(например, голосовать дистанционно), новые права и свободы (выход, идентичность, отключение) и учитывая имеющиеся гарантии (система безопасности и конфиденциальности). Формируется целостное цифровое пространство, требующее детального законодательного регулирования [14].

В этой связи термины «цифровое гражданство» и «цифровой гражданин» являются показателями уровня новой социоправовой реальности и отражением необходимости правового регулирования цифровой среды, в которой живет современный человек, юридизации цифрового гражданства. Думается, это не просто модная фраза, коррелирующая с умением использовать продукты цифровизации, а феномен, требующий основательного анализа, этап к изучению правовой культуры такого гражданина.

Степень разработанности исследования нельзя признать минимально имеющейся или достаточной. Отметим, что существуют лишь исследования на смежные темы (цифровой профиль, цифровое государство, цифровой интеллект) и некоторые междисциплинарные темы (цифровые права согласно ст. 141.1 ГК РФ, цифровой административно-правовой статус в рамках взаимодействия с органами исполнительной власти). Вместе с тем отсутствует соответствующий понятийно-категориальный аппарат: «цифровое гражданство», «цифровой гражданин», «гендерное цифровое гражданство», «правовой статус цифрового гражданина», «принцип равенства цифровых граждан», «правовая культура цифрового гражданина», «гражданственность цифрового гражданина». Кроме того, требуется обоснование юридизации цифрового гражданства.

Объектом исследования являются общественные отношения, связанные с формированием, развитием и научной концептуализацией такого феномена, как цифровое гражданство.

Предмет исследования – проблема правового статуса цифрового гражданина.

В этой связи цель исследования – изучить особенности реализации правового статуса цифрового гражданина в России и за рубежом.

Для достижения данной цели были поставлены следующие задачи:

– обосновать необходимость юридизации цифрового гражданства;

– разработать и сформулировать понятийный ряд института цифрового гражданства;

– выявить элементы цифрового гражданства и установить виды связей между ними;

– рассмотреть понятие «правовая культура цифрового гражданина» в связи с выявленными закономерностями.

Выполнение данных задач позволит достичь цели исследования и составить эмпирическую и методологическую базу для изучения правовой культуры цифрового гражданина как показателя уровня новой реальности и необходимости правового регулирования цифровой среды, юридизации цифрового гражданства.

Это определяет новизну исследования: формулирование ключевых понятий данной актуальной тематики и системный подход к их определению, стремление преодолеть междисциплинарную рассогласованность научных взглядов на цифровое гражданство и различную его отраслевую правовую интерпретацию.

Эмпирическую базу исследования составляют законодательные акты, затрагивающие вопросы использования цифровых технологий в конкретных сферах жизни общества, в частности, электронной демократии и электронном голосовании, электронном бизнесе, электронном правительстве, электронном правосудии.

В ходе проведенного исследования используются такие методы познания, как анализ и синтез, аналогия, дедукция и индукция, описание и обобщение, моделирование, конкретно-социологический, формально-юридический метод и сравнительно-правовой методы.

Статья состоит из введения, основной части, заключения и списка использованной литературы.

Основная часть. Примечательно, что проведение закупок для государственных нужд в цифровом формате вызвало ряд споров, связанных с обеспечением заявок (дело ЕАЭС № СЕ-2-2/1-22-БК, Решение от 22.11.2022) и ограничением прав предпринимателей. Из Особого мнения судьи Т. Н. Нештаевой по делу ЕАЭС № СЕ-2-2/1-22-БК следует, что отказ от проведенной цифровизации на уровне национального права ведет к нарушению прав цифрового гражданина. В другом деле ошибки во введенном цифровом коде привели к нарушению прав предпринимателей при таможенном декларировании товаров – например, переплата денежной суммы за товар, который из-за ошибки был отнесен к другой группе (Решение ЕАЭС от 14 апреля 2021 г. № СЕ-1-2/2-21-КС).

Приведенные судебные дела отражают специфичные отношения, возникающие в связи с цифровизацией бизнеса и правового статуса личности. Решения суда были вынесены по формальным признакам без учета действительных интересов цифровых граждан-предпринимателей, которые рассчитывают на отсутствие ошибок цифровизации.

В научной литературе справедливо указывается, что любой продукт цифровизации, например электронное и цифровое правительство, – это не просто вертикальное общение гражданина и государства, а возможность учета потребностей населения и его развития [4. С. 11]. Добавим, что это актуально и в трудовых отношениях, где у работника – цифрового гражданина – появляется право на отключение после завершения дистанционной работы. Это может быть законным правом на отдых, «протестом» на требования работодателя «задержаться» в Сети или выходом работником в отпуск за свой счет.

Считаем, что выделенные элементы и признаки цифрового гражданства, правового статуса такого гражданина присутствуют в отечественной и зарубежной практике. Органы публичной власти прилагают достаточно усилий для совершенствования алгоритмов цифрового гражданина: лицо должно понимать, как пользоваться продуктами цифровизации, что и где найти, куда отправить значимые для жизни документы и прочее. Разумеется, это заметно на примере упомянутого портала РФ «Госуслуги», содержащего ДЭГ, разъяснения относительно того, как создать ИП, возможность оплатить штраф, записаться к врачу и т. д.

В контексте исследования представляется полезным сравнить отечественную и зарубежную практику электронного и цифрового правительства с точки зрения взаимодействия с гражданами и понятности платформы.

Примечательна система электронного правительства с элементами правосудия, существующая в ОАЭ (https://u.ae). В данном случае цифровой гражданин

может получать разъяснения и взаимодействовать со всеми ведомствами через один сайт. Все услуги характеризуются как круглосуточные и «проактивные», которые чаще представлены как автоматические: например, в разделе юстиции разъясняется, что информация о штрафах в приговоре автоматически попадает в соответствующую службу [11]. На наш взгляд, платформа имеет хороший потенциал для развития цифрового образования, при этом лишь небольшое внимание уделяется алгоритмизации действий цифрового гражданина (сервер отвечает на вопрос «почему так?», а не «что делать?»).

Граждане ОАЭ могут принять «электронное участие» в опросах, имеющих значение для государственной политики, написать обращение и иным образом проявить свою гражданскую позицию. Это делается согласно разработанной ОАЭ Стратегии в области государственных услуг, Политике единой цифровой платформы и Политике цифровых клиентов и цифровых государственных услуг [9].

Сходством платформ РФ и ОАЭ является разветвление информации в рамках одного сайта и налаженное взаимодействие власти и населения. Вместе с тем портал РФ содержит наиболее понятные для цифрового гражданина разъяснения, ответ на вопрос «что делать» и базу для развития цифровых компетенций (ДЭГ и др.)

Отметим, что не все государства придерживаются принципа «все услуги в одном месте». Так, например, в Республике Мальта отсутствует единый портал электронного правительства, у каждого учреждения есть сайт, где граждане решают вопросы, находящиеся в компетенции соответствующего органа. Думается, здесь особо актуальны вопросы цифрового гражданства, поскольку государственные и муниципальные услуги переведены в электронный и цифровой вид. После 2008 г. в Мальте происходит активный сбор биометрических данных, а паспорта и иные значимые для граждан Мальты документы выдаются в электронном виде, с 2019 г. – в виде поликарбонатной карты с качественным чипом, идентификационные данные выгравированы лазером (снижение риска подделки). Граждане и резиденты Мальты должны посещать паспортный стол лично и вживую принимать от Malta post документы, взаимодействовать с сотрудниками органов ЗАГС [10], однако уклон на цифровизацию государства не вызывает сомнений.

Выделим следующие структуры Мальты, имеющие сайты, и продемонстрируем, как цифровые граждане взаимодействуют с государством.

Во-первых, Управление идентификацией граждан и реализации миграционных процессов (Identità, https://identita.gov.mt). Соответствующий сайт позволяет цифровому гражданину забронировать онлайн время для посещений органов, которые изготавливают документы, а также является прозрачной и понятной базой для цифрового образования, развития цифровых компетенций. Законодательство Мальты требует менять паспорт с большой периодичностью, что актуализирует значимость сайта.

Так, цифровые граждане могут ознакомиться с «полезной информацией» (подобно приведенной выше информации о картах Мальты) и ответами на «часто задаваемые вопросы» о паспортном столе, публичных реестрах и других подразделениях (например, что делать, если пара решила пожениться). Функционирование сайта способствует совершенствованию процедуры получения цифровым гражданином электронного паспорта, документов о проживании (как постоянный

или временный вид на жительство в РФ) и визы, а также актов гражданского состояния.

Во-вторых, Агентство по делам сообщества Мальты (https://komunita.gov.mt/en). На сайте данного Агентства, как и на сайте описанного выше Управления, содержится ряд разъяснений по вопросам приобретения гражданства Мальты и отказа от него, получения свидетельства о гражданстве. Вместе с тем сайт сам по себе не является площадкой для связи с представителями органов власти (это осуществляется через мобильный номер или электронную почту) [3].

В-третьих, Агентство местных систем правоприменения (LESA, https://les.gov.mt). На наш взгляд, данный ресурс делает акцент не на разъяснениях, а на взаимодействии. Так, граждане 1) оплачивают выписанные полицией и общественными инспекторами штрафы; 2) взаимодействуют с комиссарами по правосудию в рамках местных трибуналов; 3) следят за расписанием судебных заседаний и уведомляют органы об уважительности своей неявки; 4) обращаются в Агентство с петициями.

Следует признать интересным разделение функций учреждений Мальты на разных сетевых платформах. Вместе с тем из представленных порталов реальное взаимодействие цифрового гражданина через цифровую платформу осуществляется лишь на портале Агентства местного правоприменения.

Рассматривая модели взаимодействия цифрового гражданина и государства, отметим, что расположение лаконичной и точной информации является удачным как на одной платформе (РФ, ОАЭ, Исландия, Корея и др.), так и на нескольких (Мальта и др.). Заметен вклад государств в цифровое образование, преодоление цифрового разрыва и правовую культуру цифрового гражданина.

В этой связи примечательна характеристика 4-балльной шкалы цифровых граждан среди студентов университета Султана Кабуса в Омане. Это было сделано в период пандемии COVID-2019 [12, 13] на основании выполнения последними 26 сценарных заданий. В ходе такого эксперимента определялись следующие уровни: 1) цифровая идентичность; 2) цифровая гражданская активность; 3) цифровая этика; 4) цифровая грамотность; 5) цифровая безопасность; 6) глобальная цифровая коммуникация. В итоге было установлен более высокий уровень развития цифровых навыков у женщин по сравнению с мужчинами [7. С. 290].

Разумеется, изложенные аспекты затрагивают правовую культуру цифрового гражданина и в целом описывают ее содержание. Однако видится необходимым рассмотреть это явление в более широких масштабах, выделяя параметры. Данный вывод логичен и ввиду описанного выше эксперимента, в котором элементы правовой культуры цифрового гражданина анализировались по 4-балльной шкале.

Кроме того, данный вопрос коррелирует с цифровой идентичностью гражданина, тем, как он показывает себя в цифровом мире с учетом обладания определенными персональными данными (логин, пароль и т. д.).

Насколько гибким цифровым мышлением обладает ребенок, который с детства вовлечен родителями в создание контента в социальных сетях, особенно с целью получения денежных сумм от донатов и рекламы? По мнению Франциско

Хосэ Аранда Серна, при подобном шерентинге родители переносят свою цифровую идентичность на ребенка, искажая его собственную и нарушая его цифровую конфиденциальность [6. С. 405]. Примечательно, что подобные ситуации получили в РФ широкий общественный резонанс [2]. Думается, цифровая идентичность отражает и степень самостоятельности гражданина.

Заключение. Соблюдение цифрового равенства и преодоление цифрового разрыва возможно путем постановки государством равных исходных условий и учета гендерных аспектов цифрового гражданства при составлении методик (например, в странах третьего мира).

Современные отечественные и зарубежные порталы электронного и цифрового правительства и правосудия имеют разную форму, однако способствуют построению конструктивного диалога и реализации статуса цифрового гражданина, развитию его правовой культуры (особенно в контексте разъяснений, цифрового образования) и, соответственно, цифровой гражданственности.

Вместе с тем проблемными являются ситуации, связанные с неопределенностью отдельных цифровых систем (отражено в приведенных судебных делах ЕАЭС) и последующим нарушением прав цифрового гражданина, а также вопросы цифровой идентичности несовершеннолетних – элемента правовой культуры.

Перспективой исследования является дополнение концепции правовой культуры цифрового гражданина, продолжение исследования статуса цифрового гражданина в цифровом пространстве (например, фандрайзинг), а также изучение обозначенной проблемы цифровой конфиденциальности.

Список литературы

1. Костина Н. Б., Чижов А. А. К вопросу о разграничении понятий «цифровой раскол», «цифровое неравенство» и «цифровой разрыв» // Уфимский гуманитарный научный форум. 2022. № 1(9). С. 56–63.

2. «Скамят деньги на ребенке»: за что Инстасамка критикует Кукояк и почему в сети встают на ее сторону. 25.06.2024. URL: https://postnews.ru/a/29278 (дата обращения: 08.09.2024).

3. Связаться с нами. Агентство по делам сообщества Мальты. URL: https://komunita.gov.mt/en/contact-us (дата обращения: 08.09.2024).

4. Судоргин О. А. Концепция и перспективы развития электронного правительства во Франции // Политика и общество. 2019. № 3. С. 9–13.

5. Ташбаев А. М., Маликов А. А., Жакшылык К. Г. Цифровые навыки и компетенции для цифровой экономики: модели, структура и виды цифровых навыков // Финансовая экономика. 2020. № 2. С. 430–435.

6. Aranda Serna F. J. Social and Legal Risks of Sharenting when Forming a Child's Digital Identity in Social Networks // Journal of Digital Technologies and Law. 2024. Т. 2, № 2. Pp. 394–407.

7. Alsaadi M., Alharassi N., Alsalmi J. & Alkindi S. The Practices of Digital Citizenship Among Undergraduates at Sultan Qaboos University in Oman During COVID-19 // Future Trends in Education Post COVID-19. SHJEDU 2022 / Al Naimiy, H.M.K., Bettayeb, M., Elmehdi, H.M., Shehadi, I. (Eds.). Springer, Singapore. Pp. 281–294. DOI: https://doi.org/10.1007/978-981-99-1927-7_22

8. Bokov Y. A., Abezin D. A. Digital Citizenship: Implementation in the Modern World // Competitive Russia: Foresight Model of Economic and Legal Development in the Digital Age. CRFMELD 2019. Lecture Notes in Networks and Systems / A. Inshakova, E. Inshakova (Eds.). 2020. Vol. 110. Springer, Cham. Pp. 442–448.

9. Bokovnya A. Yu. et al. Motives and Objectives of Crime Commission Against Information Security // Ad Alta. 2020. Vol. 10, № 2 S13. Pp. 7–9. EDN: SCSEBN

10. Passport Office. Useful Information. URL: https://identita.gov.mt/passport-office-sec-page-useful-info (дата обращения: 08.09.2024).

11. Proactive Services. Ministry of Justice. URL: https://www.moj.gov.ae/en/services/proactive-services.aspx (дата обращения: 08.09.2024).

12. Криминологический анализ преступности и виктимизации несовершеннолетних в современной Японии / Р. А. Сабитов, А. В. Майоров, В. В. Денисович, О. Н. Дунаева // Пробелы в российском законодательстве. 2022. Т. 15, № 7. С. 170–177. EDN: UKEWYO

13. Шутова А. А. Цифровой паспорт здоровья: этические и правовые проблемы // Вестник Казанского юридического института МВД России. 2021. Т. 12, № 2(44). С. 236–241. EDN: DPUAMG

14. Право как созидатель новой социальной реальности: монография / отв. ред. Ю. А. Тихомиров. М.: Проспект, 2024.

У. П. Генсицкая,
студент,
Московская государственная юридическая академия
имени О. Е. Кутафина (МГЮА)

РОЛЬ FAMILYTECH В СОВРЕМЕННЫХ СЕМЕЙНЫХ ВЗАИМООТНОШЕНИЯХ: ОБРАЗОВАНИЕ, РАЗВЛЕЧЕНИЕ И ПСИХОЛОГИЯ

Аннотация. В статье рассматривается влияние цифровых технологий на семейные и межличностные отношения в условиях стремительного развития технологий. Рассматриваются направления FamilyTech, включающие интеллектуальные помощники, социальные сети, мобильные игры и виртуальную реальность, которые решают образовательные, развлекательные и психологические задачи. Обсуждаются преимущества и недостатки IT-технологий, включая их влияние на семейные коммуникации и образовательные процессы. Особое внимание уделяется роли родительского контроля в обеспечении безопасности и качества потребляемого контента детьми, а также геймификации образовательного процесса для дошкольников. Анализируются влияние технологий на баланс между работой и личной жизнью, дистанционное образование и возможности для людей с ограниченными способностями.

Ключевые слова: FamilyTech, цифровые технологии, виртуальная реальность, родительский контроль, геймификация, образование, межличностные отношения, дистанционное обучение, интеллектуальные помощники

THE ROLE OF FAMILYTECH IN MODERN FAMILY RELATIONSHIPS: EDUCATION, ENTERTAINMENT AND PSYCHOLOGY

Abstract. This article explores the impact of digital technologies on family and interpersonal relationships in the context of rapid technological advancement. It examines FamilyTech directions, including intelligent assistants, social networks, mobile games, and virtual reality, which address educational, entertainment, and psychological needs. The advantages and disadvantages of IT technologies are discussed, including their effects on family communication and educational processes. Special attention is given to the role of parental control in ensuring the safety and quality of content consumed by children, as well as the gamification of the educational process for preschoolers. The article also analyzes the impact of technology on balancing work and personal life, remote education, and opportunities for people with disabilities.

Keywords: FamilyTech, digital technologies, virtual reality, parental control, gamification, education, interpersonal relationships, remote education, intelligent assistants.

Введение. В век развития технологий на помощь детям и родителям по совершенно различным вопросам приходят цифровые сервисы, которые обеспечивают решение образовательных, развлекательных и психологических задач.

В мировой повестке FamilyTech ряд направлений сочетают в себе функции, начиная от развлечений и заканчивая поддержанием рабочих/учебных задач. Такими инструментами выступают интеллектуальные помощники, социальные сети, мобильные игры и ранее упомянутые технологии виртуальной реальности [2, 5]. Все эти атрибуты помогают моделировать социальные ситуации, дабы избежать ошибок в построении межличностных отношений и/или, наоборот, набраться опыта.

Основная часть. Легкий доступ к социальным сетям, интернет-ресурсам и приложениям помогает потреблять большой пласт информации, многие люди разных профессий делятся своими знаниями и навыками путем написания статей, ведения блогов и создания познавательных видеороликов. Многие психологи, бебиситтеры, воспитатели, разработчики социальных программ рассказывают о своих наблюдениях в различных жизненных сферах, используя короткие ролики длиной около 15 секунд или через образовательные платформы, которые помогают запоминать информацию. Благодаря этому можно получить совет или задать свой вопрос по темам воспитания детей, построения отношений, учета рисков и возможностей при заключении брачных отношений, и это только начало списка.

Помимо образовательного контента, конечно, чаще Интернет используют для развлечений. В период с февраля по май 2022 года была проведена статистика Касперского «Что ищут дети в Интернете, отчет 2022 года». Популярностью среди детей пользуются сайты категории «Аудио и видео» (43,6 %) [2. С. 60–62]. Большой популярностью пользуются видео блогеров, музыкальные треки на стриминговых платформах и фильмы и сериалы.

Нужно приложить минимум усилий, всего лишь навести курсор, кликнуть по кнопке, и результат появится на экране.

Главная задача родителей – отследить момент, когда их ребенок поймет разницу между миром реальным и виртуальным, чтобы технический прогресс не поглотил юный разум. Дать понять ребенку, что в реальности, чтобы чего-то добиться или получить, нужно приложить усилия [3].

Группой колумбийских ученых на 7-й Международной конференции по транскультурному образованию было сформулировано позитивное и негативное влияние IT-технологий на семейные взаимоотношения [1]. В категорию положительных вошли: онлайн-коммуникация с людьми, улучшение коммуникации и понимания благодаря фото- и видеосообщениям, широкий и быстрый доступ к знаниям, а также оптимизация времени. В группу негативных факторов вошли: чрезмерная погруженность в виртуальный мир, вследствие этого приобретение цифровой зависимости, ухудшение психических и физических качеств человека [1].

В ноябре 2023 года Институт статистических исследований и экономики знаний НИУ ВШЭ опубликовал отчет, посвященный так называемым семейным цифровым технологиям (FamilyTech) [1]. Наиболее значимы тенденции поиска баланса между работой/учебой и личной жизнью, а также поддерживающими его гибкой формой занятости, техникой для дистанционного образования и глобальнее – EdTech (образовательные технологии) [2].

Наиболее популярными стали видеоконференции, которые позволяют продолжать свою привычную трудовую функцию, оставаясь в любой точке мира. События минувшей пандемии COVID-19 [4] заставили нас с большим рвением окунуться в мир технологий и повысить продажи приложений для работы/обучения онлайн. Адаптация к дистанционному обучению пошла на пользу многим образовательным учреждениям, которые и по сей день используют различные инструменты, работающие на базе машинного обучения, виртуальной реальности.

В социальной сфере это поспособствовало открытию большинства возможностей для людей с ограниченными способностями или тех, кто не могут посещать занятия очно.

Основным потребителем продукции цифровизации являются скорее дети, чем их родители. Из-за этого, в частности, главной задачей родителей выступает отслеживание качественного потребляемого контента – для этого была создана функция «родительский контроль». В нее входят ограничение экранного времени, посещения сайтов с определенным контентом, настройки поиска и защита цифровых данных.

FamilyTech в Российской Федерации направлен на защиту института семьи через функции родительского контроля и систем умного дома. Умные колонки и встроенные виртуальные ассистенты пользуются спросом у людей всех возрастных групп, от самых маленьких до самых возрастных. Это происходит благодаря их растущей доступности и унификации цифровых технологий для дома.

Для детей дошкольного возраста на первое место рейтинга выходит геймификация образовательного процесса, а именно использование технологий вертикальной реальности, активно способствующих обучению детей, которые еще не научились читать и писать, так как имеют функции распознавания речи, и с поддержкой персонализированных рекомендаций.

Заключение. Таким образом, мы уже неотъемлемо связаны между собой. Технологии в сферах жизнедеятельности стали занимать одну из ключевых ролей

в семейных и иных межличностных отношениях. Наш культурный код преобразовывается ежесекундно благодаря пользователям IT-технологий, социальные роли и модели познаются людьми вокруг намного быстрее и способствуют нормативному развитию общества. Законодательство развивается вместе с информационными технологиями, чтобы выстраивать защиту интересов граждан [1].

Список литературы

1. Влияние Интернета на семью. URL: https:// skovoronok.ru/people/the-impact-of-the-internet-on-the-family.html (дата обращения: 02.09.2024).

2. Отчет Института статистических исследований и экономики знаний НИУ ВШЭ, посвященный семейным цифровым технологиям (FamilyTech). URL: https://issek.hse.ru/mirror/pubs/share/871577477.pdf (дата обращения: 02.09.2024).

3. Сержитдинова М. Л. Влияние цифровизации общества на семейные отношения // Молодой ученый. 2023. № 36(483). С. 60–62.

4. Шутова А. А. Цифровой паспорт здоровья: этические и правовые проблемы // Вестник Казанского юридического института МВД России. 2021. Т. 12, № 2(44). С. 236–241. EDN: DPUAMG

5. Залоило М. В., Власова Н. В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2014. № 5. С. 140–145.

Р. Э. Гильманов,
магистрант,
Казанский инновационный университет имени В. Г. Тимирясова
Э. Е. Азаров,
студент,
Казанский инновационный университет имени В. Г. Тимирясова

СМИ КАК ИНСТРУМЕНТ ВЛИЯНИЯ НА ОБЩЕСТВЕННОЕ МНЕНИЕ И ОТВЕТСТВЕННОСТЬ ЗА ЕГО ИСПОЛЬЗОВАНИЕ

Аннотация. С появлением мобильных средств, а в последующем их активным распространением среди граждан произошел рывок, преодолевший информационный барьер и закрытость информационного поля, доступ к которому ранее был усложнен по ряду признаков. В настоящее время мы можем с легкостью получить и изучить довольно обширный перечень информации, представленный как в средствах массовой информации, которые излагают чье-либо мнение по конкретной ситуации, так и предлагающий проанализировать узконаправленные темы, которые в большинстве своем отражают один из ключевых инструментов управления общественным мнением. В интернет-СМИ присутствуют как позиции, так и отношения, которые не всегда формируются в угоду общих интересов внутри страны, а зачастую могут отражать интересы третьих лиц, в том числе и иностранных. Данная научная работа посвящена анализу средств массовой информации через призму некоего инструмента в оказании влияния на общественное мнение.

Ключевые слова: информационные технологии, СМИ, общественное мнение, сеть Интернет, влияние информации на общество

THE MEDIA AS AN INSTRUMENT OF INFLUENCE ON PUBLIC OPINION AND RESPONSIBILITY FOR ITS USE

Abstract. With the advent of mobile devices, and their subsequent active distribution among citizens, there was a "breakthrough" that overcame the information barrier and the closeness of the information field, access to which had previously been complicated by a number of signs. Currently, we can easily obtain and study a fairly extensive list of information presented both in the media, which express someone's opinion on a particular situation, and offering to analyze narrowly focused topics, which, for the most part, reflect one of the key tools for managing public opinion. Online media contains both positions and attitudes, which are not always formed for the sake of common interests within the country, and can often reflect the interests of third parties, including foreign ones. This scientific work is devoted to the analysis of the mass media through the prism of a certain tool in influencing public opinion.

Keywords: information technology; mass media; public opinion; Internet; the impact of information on society

Введение. Последнее десятилетие принято называть веком цифровой информации. Дни, когда информация доносилась посредством газетной печати, радио, информационных трансляций, оказались позади благодаря развитию технологий, в частности, повсеместному наличию и использованию индивидуальных мобильных средств. С появлением мобильных средств, а в последующем их активным распространением среди граждан именно рывок, преодолевший имевшийся ранее информационный барьер [1. С. 83] и закрытость информационного поля, доступ к которому ранее был усложнен, можно определить как территориальное отношение информации к конкретному месту или субъекту, закрытость информации, неосвещенность некоторых проблем в силу незаинтересованности средств массовой информации. Особую проблему деятельность СМИ приобретает в связи со специальной военной операцией [2. С. 163], когда неверно поданная информация может стать источником паники среди населения.

В настоящее время мы легко можем получить и изучить довольно обширный перечень информации, представленной в различных средствах массовой информации, которые излагают свое или чье-либо мнение по отдельным ситуациям, различающимся как по временному интервалу, так и высказывающимся в отношении узконаправленных тем, которые, таким образом, в большинстве своем отражают один из ключевых инструментариев управления общественным мнением, позиции, так и отношения, которое не всегда формируются в угоду общих интересов внутри страны. Заметим, что конкретные средства массовой информации могут отражать интересы конкретных лиц, общественных или политических деятелей либо распространять иное мнение, противоречащее интересам определенного общества или государства.

Основная часть. Наличие в информационном пространстве обширного перечня средств массовой информации дает определенную надежду на достоверность доносимой информации. Для дальнейшего рассмотрения мы обратимся к открытому информационному ресурсу «МЕДИАЛОГИЯ», на просторах которого опубликован «Топ-10 российских СМИ» по состоянию на июль 2024 года.

Мы можем увидеть ряд категорий, которые можно отнести к наиболее изучаемым, просматриваемым, а равно читаемым гражданами Российской Федерации [3]. Как видно из данного рейтинга, наибольшую популярность среди средств массовой информации по-прежнему занимают мастодонты печатных изданий, которые уже успели сменить способ распространения требуемой информации с привычной печати на бумажных носителях на информационно-телекоммуникационную сеть Интернет: среди таковых выделены электронные газеты «Известия», «Коммерсантъ», «Российская газета», «Ведомости».

Необходимо учитывать, что обширность или известность изданий, в том числе медиаресурсов, отнюдь не свидетельствует о достоверном донесении основных информационных посылов либо пристально освещаемых событий, которые могут в ряде случаев изменять заинтересованность общества с одной недавно обсуждаемой темы на диаметрально противоположную тематику. Как пример можно проиллюстрировать ситуацию с задержанием правоохранительными органами Франции 7 сентября 2024 г. Павла Дурова – основателя и генерального директора мессенджера Telegram. Данное событие на протяжении всего периода задержания Павла Валерьевича вышеуказанные информационные издания активно освещали, формируя то или иное настроение внутри читающей данные источники части общества, а различного рода предположения, высказываемые относительно данного задержания, можно определить как резонансные и даже скандальные. Полагаем, что описанные действия французских властей сложно назвать законными в настоящее время, так как они нарушают один из принципов уголовной ответственности – принцип индивидуально-определенной ответственности, а также принципы законности и равенства перед законом [4. С. 344].

Однако эмоциональные информационные вбросы, которые можно сравнивать с фейк-новостями, можно охарактеризовать как попытки установить определенное психическое отношение к описываемой ситуации внутри общественного сознания. Мы понимаем желание каждого из участников, а равно лиц, осуществляющих работу в конкурирующих СМИ, отразить посредством публикаций, заявлений, цитируемых позиций определенное первенство в управлении общественным мнением и явное желание сформировать в обществе определенное отношение к данному событию, а также попытку привлечь большее количество заинтересованных читателей для дальнейшего освещения следующих информационных событий. Однако в ряде случаев СМИ, особенно электронные ресурсы, используют незаконные и даже аморальные способы предоставления информации [5. С. 95], зачастую искажая ее или освещая в неверном свете.

Вышеизложенный пример может проиллюстрировать, как негативное высказывание по отношению к определенному информационному поводу может оказать негативное влияние и на экономическую сферу, в частности на внутренний климат пользовательского сообщества мессенджера Telegram.

Вместе с тем необходимо понимать, что имеются случаи, когда определенная опубликованная фейковая информации [6. С. 38] оказывала негативное влияние на общественную жизнь как внутри конкретного административного образования внутри государства, либо даже на всей территории страны. В качестве иллюстрируемого примера приведем ситуацию с появлением подложного аккаунта врио губернатора Курской области Алексея Смирнова, который был использован

для рассылки фейковой информации о начале эвакуации в данном регионе [7]. Данное действие можно квалифицировать в соответствии со ст. 207.1 Уголовного кодекса Российской Федерации, так как данное противоправное действие было направлено на создание информационного повода, в соответствии с информацией, которая свидетельствовала об обстоятельствах, представляющих угрозу жизни и безопасности граждан Курской области. Данный информационный посыл был охарактеризован как возможный катализатор, который мог привести к всеобщей панике и ряду негативных эмоций и прямых действий, предпринятых для следования данному сообщению. Соответственно, публичные издания в ряде случаев также выступают в качестве источника фейковой информации [8].

Заключение. Исходя из ранее изложенного, мы видим острую проблему в необходимости контроля информации, распространяемой в информационно-телекоммуникационной сети Интернет, если она касается каждого из членов общества. Понимая, что на данный момент простота распространения информации, в том числе и ложной, не соответствующей действительности, продиктована желанием завоевания первенства в иерархии СМИ, для создания возможностей для роста числа подписчиков и читателей определенных изданий, а равно их цитируемости и читаемости, может приводить к явной дезинформации или добросовестному заблуждению среди читателей, тем самым формируя неправильное, а иногда и негативное навязанное мнение. Мы видим необходимость создания и расширения содержания методических инструкций, которые могут быть использованы в учебных заведениях для просвещения граждан в сфере содержания информации, а ее использования в рамках конкретной ситуации, без придания им какого-либо субъективного окраса. Также необходимо разрабатывать технологии по выявлению подложной, ошибочной или же иной информации, распространение которой может повлечь негативные последствия или стать фактором формирования негативного отношения к определенному событию или факту, освещаемому в средствах массовой информации.

Список литературы

1. Нечаева Е. В., Латыпова Э. Ю., Гильманов Э. М. Посягательство на цифровую информацию: современное состояние проблемы // Человек: преступление и наказание. 2019. Т. 27, № 1. С. 80–86.

2. Латыпова Э. Ю., Гончарова Н. Н. О военном времени как квалифицирующем признаке преступлений против военной службы // Уголовное право: стратегии развития в XXI веке. 2024. № 3. С. 162–172.

3. Рейтинги российских СМИ // МЕДИАЛОГИЯ. URL: https://www.mlg.ru/ratings/media

4. Латыпова Э. Ю. Принцип равенства и принцип гуманизма и их особенности в уголовном праве // Конституция Российской Федерации и развитие правовой системы государства: общетеоретические и отраслевые аспекты: материалы Международной научно-практической конференции. Казань: Отечество, 2019. 416 с.

5. Латыпова Э. Ю., Гильманов Э. М., Абдуллина А. Е., Гильманов Р. Э. Влияние нравственно-моральных норм на содержание уголовно-правовых норм в Уголовном кодексе России // Вестник экономики, права и социологии. 2022. № 1. С. 93–99.

6. 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. 2. Казань: Изд-во «Познание» Казанского инновационного университета, 2022. С. 37–40.

7. Власти Курской области предупредили о фейках про эвакуацию // РБК. URL: https://www.rbc.ru/rbcfreenews/66b8ca049a794790d82e7b88

8. Латыпова Э. Ю., Гильманов Р. Э., Воронцов И. А. О классификации видов фейковой информации применительно к уголовной ответственности за публичное распространение заведомо ложной информации // Актуальные проблемы правового, экономического и социально-психологического знания: теория и практика: материалы VI Международной научно-практической конференции. Донецк: Цифровая типография, 2022. С. 147–154.

А. Д. Григорова,
студент,
Российский государственный университет правосудия,
Северо-Кавказский филиал

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ЗАЩИТА ИМУЩЕСТВЕННЫХ ПРАВ ГРАЖДАН ПРИ ОСУЩЕСТВЛЕНИИ ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ И ПРОЦЕССУАЛЬНЫХ ДЕЙСТВИЙ

Аннотация. Цель исследования состоит в разработке действенного механизма защиты прав лиц в уголовном судопроизводстве, которые сталкиваются с повреждением/утратой их имущества в результате обыска или выемки в жилом помещении через информационную цифровую среду. Отдельно рассматривается проблема нарушения прав супругов подозреваемых/обвиняемых при наложении ареста на совместное имущество. Выявлены возможности обращения в суд и иные правоохранительные органы посредством электронного делопроизводства. Рассматриваются варианты решения этой проблемы за счет дистанционного сокращенного производства.

Ключевые слова: обыск, выемка, имущество, цифровые технологии, имущество, прокурор, суд

DIGITAL TECHNOLOGIES AND PROTECTION OF PROPERTY RIGHTS OF CITIZENS IN THE IMPLEMENTATION OF CERTAIN INVESTIGATIVE AND PROCEDURAL ACTIONS

Abstract. The purpose of the study is to develop an effective mechanism for protecting the rights of persons in criminal proceedings who face damage/loss of their property as a result of a search or seizure in a residential premises through a digital information environment. The problem of violation of the rights of spouses of suspects/accused when seizing joint property is considered separately. The possibilities of applying to the court and other law enforcement agencies through

electronic record keeping have been identified. Options for solving this problem through remote reduced production are being considered.

Keywords: search, seizure, property, digital technologies, property, prosecutor, court

Введение. В современной юридической практике нередко возникают случаи ограничения имущественных прав граждан, вовлеченных в уголовный процесс, не имеющих самостоятельного правового статуса в уголовном судопроизводстве. Чаще всего речь идет о неправомерном наложении ареста на совместное имущество супругов, а также о порче имущества в жилище, в котором производился обыск или выемка, когда страдают интересы собственника [1]. Но у него должна быть возможность своевременной защиты своих имущественных прав.

Основная часть. Цифровые технологии во многом помогают в этом. Поэтому существует необходимость на сайтах мировых судей и районных судов и прокуратуры сделать вкладку «Обращения граждан в связи с проведением следственных и иных процессуальных действий».

Чтобы исключить перегрузку правоохранительных органов по этому направлению работы, допустимо внедрить систему искусственного интеллекта [3].

Обыск в жилище – это принудительное обследование индивидуального жилого дома с входящими в него жилыми и нежилыми помещениями, жилого помещения независимо от формы собственности, входящего в жилищный фонд и используемого для постоянного или временного проживания, а равно иного помещения или строения, не входящего в жилищный фонд, но используемого для временного проживания. Из определения выделяется характеризующий признак данного следственного действия – принудительность, в свою очередь п. 6 ст. 182 УПК РФ гласит: «При производстве обыска могут вскрываться любые помещения, если владелец отказывается добровольно их открыть. При этом не должно допускаться не вызываемое необходимостью повреждение имущества» [2].

Как показывает практика, в ходе совершения определенных процессуальных или следственных действий иногда существенно для собственника повреждается внешняя и внутренняя отделка помещения, происходит порча мебели и оборудования. При выявлении такого ущерба, помимо предложенной выше формы обращений в суд и иные правоохранительные органы, было бы разумно разработать механизм сокращенного дистанционного судебного производства по его компенсации с перечислением денег в цифровых рублях [4. С. 28].

К большому сожалению, в нашей стране еще не в достаточной степени налажено взаимодействие по такого рода вопросам между судами, органами предварительного расследования, ФССП и другими государственными органами и организациями. Именно поэтому добиться компенсации имущественного ущерба в уголовном процессе можно только спустя длительное время. Все исправить смогла бы специальная цифровая платформа, представляющая возможность с различным правом доступа отдельным должностным лицам беспрепятственно получать необходимые сведения.

Подрывает доверие к суду и правоохранительным органам и имеющаяся возможность наложения без уведомления супруга подозреваемого/обвиняемого ареста на совместно нажитое имущество в порядке ст. 115 УПК РФ.

В этом случае также эффективным видится использование искусственного интеллекта [5], который позволит своевременно выявлять наличие режима общей совместной собственности.

Супруг подозреваемого/обвиняемого или собственник жилища, где производится обыск, никак не причастен к совершенному преступлению, однако претерпевает существенное умаление своих имущественных прав.

Заключение. Подводя итоги вышесказанному, полагаем, что законодателю необходимо закрепить в п. 6 ст. 165 УПК РФ то, что «должностное лицо, осуществляющее полномочия в рамках проведения обыска и выемки в жилище на законных основаниях, несет ответственность за причинение существенного имущественного ущерба гражданину. Под существенным имущественным ущербом понимаются действия, влекущие за собой невозможность проживания в жилище. При этом расходы возмещаются за счет федерального бюджета с возможностью сокращенного дистанционного производства».

Предлагаем также внести изменение в ст. 115 УПК РФ:

«…п. 8.1. При наложении ареста на совместно нажитое имущество супругов, один из которых является подозреваемым/обвиняемым, а другой – нет, происходит обязательное уведомление обоих собственников, с возможностью выделения супружеской доли лицу, не причинившему ущерб в результате совершения преступления, в том числе дистанционно посредством цифровых технологий…»

Список литературы

1. Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993, с изменениями 01.07.2020) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_28399/?ysclid=lpcd6x6st0482435474 (дата обращения: 28.08.2024).

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34481/?ysclid=lpcddk2alp204727859 (дата обращения: 28.08.2024).

3. Цифровизация правоприменения: поиск новых решений: монография. М.: Инфотропик Медиа, 2022.

4. Ситник А. А. Цифровой рубль как объект финансово-правового регулирования // Актуальные проблемы российского права. 2023. № 8. С. 20–36.

5. Бегишев И. Р., Хисамова З. И. Искусственный интеллект и робототехника: глоссарий понятий. М.: Проспект, 2021. 64 с.

Д. Э. Демин,
магистр,
Сибирский федеральный университет

РОЛЬ СОЦИАЛЬНЫХ СЕТЕЙ В ПРОФИЛАКТИКЕ ПРЕСТУПНОСТИ

Аннотация. В статье рассматривается взаимодействие процессов цифровизации общества и права в рамках профилактики преступности посредством социальных сетей. Представляется анализ мониторинга преступности, в котором задействованы инструменты пользовательских сетей. Исследуются способы цифровой профилактики преступности, а также их значение в снижении уровня преступности. Предлагается такой способ предупреждения преступности, как правовое консультирование пользователей интернет-сообществ официальными представителями органов государственной и муниципальной власти в социальных сетях.

Ключевые слова: преступность, социальная сеть, интернет-сообщество, цифровизация права, мониторинг преступности, профилактика преступности, предупреждение преступности, правовое консультирование

THE ROLE OF SOCIAL MEDIA IN CRIME PREVENTION

Abstract. The article examines the interaction of the processes of digitalization of society and law within the framework of crime prevention through social media. An analysis of crime monitoring using user network tools is presented. Methods of digital crime prevention are explored, as well as their importance in reducing crime. A method of crime prevention is proposed, such as legal advice to users of Internet communities by official representatives of state and municipal authorities on social media.

Keywords: crime, social media, online community, digitalization of law, crime monitoring, crime prevention, crime prevention, legal consulting

Введение. На протяжении тысячи лет преступные деяния приносят несоизмеримый вред общественным отношениям. Совокупность данных деяний образует преступность. Преступность – это социальное явление, заключающееся в решении частью населения своих проблем с виновным нарушением уголовного запрета [1. С. 17]. В ходе развития общества преступность приобретала разные формы и государство вырабатывало ряд мер по ее мониторингу, предупреждению и пресечению в соответствии с теми ресурсами и технологиями, которыми оно обладало в определенный момент времени. Так, в последнее время наибольшей популярностью в обществе пользуется такой продукт цифровизации, как социальные сети [12].

Социальные сети – интернет-сервисы, которые преследуют цель создания удобной платформы для взаимодействия людей [2. С. 247]. В наши дни наиболее популярной социальной сетью в России, согласно данным ВЦИОМ, является «ВКонтакте» [3]. Социальные сети выступают в качестве инструмента социального контроля, выполняя следующие функции: оценку со стороны пользователей приемлемости деяния или события для общества путем обсуждения в группах

и диалогах; предупреждение негативных событий посредством обмена информацией между пользователями; устранение экстремистской информации с помощью удаления записей с цифровой платформы, так называемый бан.

Появление и развитие социальных сетей являются только одной из сторон цифровизации общественной жизни, другой стороной выступает процесс цифровизации права, выражающийся в расширяющемся использовании современных технологий в правовом регулировании общественных отношений [4. С. 25]. Данный процесс имеет логичное объяснение: в связи с информатизацией общественных процессов и сложной эпидемиологической обстановкой в странах мира происходит повышение активности социальной жизни в киберпространстве. Это приводит к перенесению явлений реального мира в мир виртуальный. В этом случае социальные сети становятся полем для получения криминологической информации и осуществления профилактики преступности.

Получение криминологической информации выражается в исследовании тематических запросов целевых групп в виртуальном пространстве, проведении онлайн-опросов, анализе реакции интернет-сообществ на события реальной жизни. На основе полученных данных осуществляется мониторинг преступности: выявляются ее тенденции и детерминанты.

Так, Комитет по информатизации и связи г. Санкт-Петербурга при участии Комитета по вопросам законности, правопорядка и безопасности провел мониторинг проявления религиозного и национального экстремизма в своем городе [5], в частности, мониторинг публикаций в социальных сетях на тему «Межнациональные и межконфессиональные конфликты в Санкт-Петербурге в период с января по сентябрь 2020 года» [5. С. 26–28]. Проанализировав количество публикаций, активность пользователей в обсуждении данных тем и характер комментариев, исследователи выяснили, что основными темами публикаций стали межнациональные конфликты, выражающиеся в противоправных деяниях представителей одной национальности в отношении представителей другой (побои, драка, изнасилование), данные темы широко обсуждались пользователями социальных сетей, и большинство комментариев носило негативный или нейтральный характер. Можно сделать вывод, что проблема преступности между представителями разных наций остается актуальной, но, судя по характеру преступлений, главной причиной враждебность наций по отношению к другим не выступает. Общество активно обсуждает и осуждает неправомерные действия иностранцев на территории Санкт-Петербурга, что непосредственно способствует развитию негативного отношения петербуржцев к представителям других наций. Такое явление может выступать детерминантом возможной преступности.

На основе полученной криминологической информации из социальных сетей и других источников осуществляется профилактика преступности. Она заключается в правовом просвещении и консультировании пользователей сети. Для рассмотрения правового просвещения нам необходимо посетить сообщества социальной сети «ВКонтакте»: так, в сообществе «Министерство внутренних дел Российской Федерации» в рубрике «Правовая справка» регулярно появляются записи, носящие информативный характер и объясняющие, как правомерно поступить в разных жизненных ситуациях. Например, памятка о безопасной покупке лекар-

ственных препаратов, биологически активных или пищевых добавок в зарубежных интернет-магазинах [6]; памятка об основных схемах «дистанционного» мошенничества и борьбе с ними [7]; памятка о сущности и последствиях взяточничества для участников преступления [8]. Сообщество «Новости ФССП России» информирует пользователей о способах противодействия коррупции [9].

Для предотвращения преступлений, вызванных незнанием законодательства, сообщество «Государственная Дума» регулярно информирует граждан о внесенных на рассмотрение законопроектах и законах, вступающих в силу в скором времени. Так, внесение законопроекта о повышении наказания для педофилов-рецидивистов [10]; принятие во втором чтении поправки в УК РФ об ужесточении наказания за реабилитацию фашизма и публичное оскорбление ветеранов ВОВ [11]. Такая профилактическая работа со стороны государства является значимой для общества, так как пользователи социальных сетей, которые со временем проводят все больше времени в виртуальном мире, знакомятся с образцами правомерного поведения в удобной для них форме; кроме того, распространение такой информации является наиболее легкой и менее материально затратной процедурой со стороны государства, если брать в сравнение проведение профилактических работ в реальном мире.

Для более полного изучения правовых вопросов, по нашему мнению, необходимо ввести консультирование пользователей сети официальными представителями государственных структур в социальных сетях. Такое решение способствует повышению конструктивного взаимодействия государства и общества, поможет оперативно разрешить правовую проблему и предоставить квалифицированную помощь для предотвращения правонарушений.

В современном цифровом обществе приоритетным направлением профилактики преступности должна выступать работа государственных органов с гражданами через социальные сети, так как для этого созданы все условия и роль социальных сетей в жизни человека с каждым днем возрастает. Рассмотрев примеры способов мониторинга и профилактики преступности через социальные сети, можно утверждать, что социальные сети выступают источником информации об обществе, следовательно, и характеристиках преступности. Виртуальное пространство, являясь носителем полезных правовых сообщений – памяток, используется во благо сохранения правопорядка, а взаимодействие органов государственной власти и граждан через социальные сети как итог способствует повышению правовой культуры общества и снижению криминогенной обстановки.

Список литературы

1. Преступность, ее виды и проблемы борьбы / под общ. ред. А. И. Долговой. М., 2011. 371 с.

2. Малинина Т. Б., Смертина Д. А. Феномен социальной сети в информационном обществе // Наука и бизнес: пути развития. 2019. № 2. С. 246–250.

3. ВЦИОМ Новости. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/kiberbulling-masshtab-problemy-v-rossii (дата обращения: 25.08.2024).

4. Карцихия А. А. Цифровая трансформация права // Мониторинг правоприменения. 2019. № 1. С. 25–29.

5. Результаты мониторинга проявлений религиозного и национального экстремизма в Санкт-Петербурге в период с января по сентябрь 2020 года / Комитет по информатизации и связи администрации Санкт-Петербурга. СПб., 2020. 60 с.

6. Памятка МВД РФ о безопасной покупке лекарственных веществ // Официальное сообщество МВД России во «ВКонтакте». URL: https://vk.com/mvd?w=wall-26323016_38164 (дата обращения: 25.08.2024).

7. Памятка МВД РФ о противодействии мошенничеству // Официальное сообщество МВД России во «ВКонтакте». URL: https://vk.com/mvd?w=wall-26323016_37919 (дата обращения: 25.08.2024).

8. Памятка МВД РФ о противодействии коррупции // Официальное сообщество МВД России во «ВКонтакте». URL: https://vk.com/mvd?w=wall-26323016_37107 (дата обращения: 25.08.2024).

9. Памятка ФССП РФ о противодействии коррупции // Официальное сообщество ФССП России во «ВКонтакте». URL: https://vk.com/news_fssprus_ru?w=wall-59564564_6696 (дата обращения: 25.08.2024).

10. Наказание в отношении педофилов может быть ужесточено // Официальное сообщество Государственной Думы Федерального собрания РФ во «ВКонтакте». URL: https://vk.com/duma?w=wall-138347372_1092819 (дата обращения: 25.08.2024).

11. Может быть усилена ответственность за публичное оскорбление ветеранов // Официальное сообщество Государственной Думы Федерального собрания РФ во «ВКонтакте». URL: https://vk.com/duma?w=wall-138347372_1008592 (дата обращения: 25.08.2024)

12. Залоило М. В., Власова Н. В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2014. № 5. С. 140–145.

Р. Р. Дзетль,
студент,
Российский государственный университет правосудия

ВИДЫ КИБЕРПРЕСТУПЛЕНИЙ И МЕТОДЫ ИХ СОВЕРШЕНИЯ

Аннотация. В данной работе проведена классификация видов киберпреступлений. Особое внимание уделено описанию методов совершения киберпреступлений. Одновременно с этим в статье описана юридическая ответственность за их совершение. Помимо этого, были приведены рекомендации законодателю по квалификации преступлений.

Ключевые слова: право, цифровые технологии, уголовное право, киберпреступность, классификация киберпреступлений, кибермошенничество, фишинг, легализация преступных доходов, кибератаки, сваттинг

TYPES OF CYBERCRIMES AND METHODS FOR IMPROVING THEM

Abstract. This scientific work classifies the types of cybercrimes, including those not yet studied by the scientific community, and gives clear definitions

to the studied crimes. Particular attention was paid to a detailed description of methods for committing cybercrimes. At the same time, the article describes the legal liability for their commission. In addition, recommendations were given to the legislator on the classification of crimes.

Keywords: law, digital technologies, criminal law, cybercrime, classification of cybercrimes, cyber fraud, phishing, money laundering, cyber attacks, swatting

Введение. Развитие компьютерных технологий и глобальная цифровизация жизни коренным образом изменили облик современного общества, предоставив преступному сообществу абсолютно новые инструменты совершения преступлений. Сфера таких преступлений называется киберпреступностью. Несмотря на то, что борьба с киберпреступностью ведется уже не одно десятилетие, количество преступлений в данной сфере активно растет, а показатели раскрываемости все так же находятся на низком уровне, притом что до судебного разбирательства доходит лишь четверть [1]. На это влияет множество факторов, таких как незаявление в полицию о преступлении, большой процент преступлений против преступников, быстрая эволюция способов преступлений, высокая анонимность преступников и т. д. Но основной причиной столь печальной статистики мы считаем слабую изученность видов киберпреступлений и методов их совершения.

Основная часть. Киберпреступность можно разделить на следующие категории:

Кибермошенничество и кража данных.

Вымогательство.

Легализация преступных доходов.

Кибератаки.

Сваттинг.

В киберпреступном лексиконе для цифрового мошенничества используют англицизмы – скам (scam), а сам процесс обмана – ворком (work). Наиболее популярным видом скама является фишинг. Ввиду отсутствия определения фишинга в нормативных актах его изучение затруднено, нам для более точного определения юридической ответственности за фишинг, необходимо разделить понятие фишинга на фишинг как самостоятельное преступление и фишинг как способ совершения иных киберпреступлений. Фишинг как самостоятельное преступление – вид кибермошенничества, целью которого является получение доступа к конфиденциальной информации. Фишинг как часть иного киберпреступления – способ передачи вредоносного программного обеспечения. В постановлении Пленума Верховного Суда от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [2] подтверждает двойственность фишинга. Первый вид фишинга зачастую осуществляется путем перехода жертвы по ссылке или установки приложения, где ей предлагается ввести свои данные. В свою очередь наказание за другой вид фишинга наказание неоднозначное из-за различий в правоприменительной практике, так схожие между собой преступления осуждаются по абсолютно разным составам, но зачастую это статьи: п. «г» ч. 3 ст. 158, 159, 159.6, 272, 273 УК РФ. Это является важной проблемой правоприменения, и мы считаем, что регулятору для ее решения следует как минимум дать четкое

определение фишинга, добавить фишинг в виде отдельного состава в УК РФ. Существуют и иные виды скама, которые не несут в себе такую неоднозначность и проблемы с правоприменением, как фишинг, и попадают под действие статей о мошенничестве.

Цифровое вымогательство совершается благодаря использованию программ-вымогателей без их использования. В первом случае вымогатели обычно используют вирус Locker, который шифрует данные дисков и ставит себя в автозагрузку с наивысшим приоритетом, тем самым блокируя возможность игнорирования локера. Затем вирус начинает требовать средства на указанный вымогателем адрес криптокошелька, если жертва платит, то в половине случаев получает код дешифровки, и в трети случаев код дешифрует данные без их частичной или полной утери. Данный вид кибервымогательства подходит по смыслу к ст. 163, 272, 273 УК РФ и в некоторых случаях под ст. 137 УК РФ. Вымогательство без использования программ-вымогателей в целом в своих методах не отличается от вымогательства вне просторов Сети, кроме одного специфического вида вымогательства. Им является вымогательство, в объективной стороне которого отсутствует имущественная составляющая, а основным требованием преступника является совершение жертвой каких-либо действий. Данный вид не подходит по смыслу ст. 163 УК РФ, но фактически является вымогательством. Зачастую преступник ставит жертву перед выбором: слив данных или выполнение требуемого действия. В таких случаях преступников осуждают за иные статьи, но не за вымогательство. Мы считаем, что критически необходимо расширить понятие «вымогательство» или ввести его аналог для вымогательства неимущественного характера в Уголовный кодекс, потому что если преступник угрожает распространением OSINT информации, т. е. распространением уже открытой информации, и при этом не требует совершения противоправных деяний, то он фактически не подпадает ни под признаки состава преступления, предусмотренного ст. 137 УК РФ, ни под иной состав в УК РФ, несмотря на то, что в перечень этой информации могут входить: данные паспорта, адрес, номер телефона, IP-адрес, log- и cookie-файлы, хеш паролей и т. д., все вышеперечисленное несет в себе серьезную угрозу для жертвы, но за это действие вымогатель не будет нести ответственности, так как он нашел их в открытых источниках и тем самым не нарушил ни один закон.

Легализация (отмывание) преступных доходов – процесс введения в легальное поле доходов, полученных преступным путем. Киберпреступники отмывают свои доходы, как всем привычными методами по типу создания иллюзии реальной экономической деятельности подставных компаний, так и достаточно неординарными.

К таким относятся:

Криптомиксеры – специализированные сервисы создания цепочки транзакций для увеличения сложности отслеживания сделки со стороны правоохранительных органов.

Анонимные криптовалюты – в отличие от остальных данные криптовалюты не дают возможность третьим лицам отслеживать движение монет. Самая популярная из них – Monero. За 10 лет существования валюты есть всего лишь один подтвержденный случай, когда ее смогли отследить, и сделала это финская полиция [3]. Финские правоохранители не раскрыли способ отслеживания, поэтому

многие криптовалютные аналитики предполагают, что следователи основывались лишь на сумме транзакции, а следовательно, действительных механизмов отслеживания операций в Monero нет.

Азартные онлайн-игры – под данным понятием мы подразумеваем абсолютно все онлайн-игры, где на кону стоят деньги, в том числе и ставки. В данной схеме создаются фиктивные игры, румы, матчи, партии, слоты и т. д. с целью получения отмытых денег после выигрыша.

Отмывание через цифровые ценности. Это может быть и фиктивное создание, и купля-продажа NFT, Telegram юзернеймов, игровых предметов и т. д.

Независимо от способа легализации преступных доходов, ответственность будет наступать по ст. 174 или 174.1 УК РФ.

Кибератака – попытка несанкционированного доступа к компьютерной информации и сетям с целью кражи, перехвата, модификации компьютерной информации или сетевого трафика и нарушения работоспособности сетей и устройств. Ввиду обширности понятия описание всех типов кибератак является затруднительным, поэтому мы перечислим лишь самые популярные из них.

Популярные типы кибератак:

DoS и DDoS-атаки – создание огромного количества запросов на сервер ресурса, нацеленные на перегрузку сетевых ресурсов.

Вредоносное ПО – представляет собой обширный спектр вирусов и червей различной направленности и опасности.

SQL-инъекции – внедрение кода злоумышленника приводящего к аномальному поведению исходного кода программы, ресурса и т. д. с целью получения доступа к базе данных.

Сниффинг трафика – прослушивание исходящих и входящих данных устройства путем перехвата пакетов с целью сбора данных.

В уголовных делах по вышеперечисленным кибератакам преступникам инкриминируются ст. 272 и 273 УК РФ.

Сваттинг (от англ. swat) – заведомо ложное сообщение об угрозе преступления. Сваттер совершает вызов группы быстрого реагирования по телефону диспетчеру либо отправляет электронное письмо в территориальный правоохранительный орган. Группу быстрого реагирования сами сваттеры называют «Маски-шоу».

Сваттинг совершается в целях:

Нарушения работы учреждения. В таких случаях обычно поступает сообщение о минировании и иных видов терактов.

Возникновения проблем с правоохранительными органами у физических лиц. В таких случаях сваттер сообщает о теракте от лица жертвы сватта с надеждой на то, что «Маски-шоу» как минимум изымут гаджеты жертвы для проверки, как максимум – найдут у жертвы признаки иных преступлений, не связанных с поводом для вызова, например, хранение наркотических средств. Сваттерам инкриминируется ст. 207 УК РФ в вышеперечисленных случаях.

Заключение. Подводя итоги, можно утверждать, что дальнейший рост киберпреступности будет следовать за неизбежным увеличением уровня информатизации общества, а сами киберпреступления, учитывая их разнообразие и специфику, требуют четкой классификации со стороны законодателей.

Список литературы

1. Николай Козин. Количество киберпреступлений в России выросло в 2,3 раза за пять лет // Парламентская газета. 2024, 16 апреля.
2. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48. URL: https://www.consultant.ru/document/cons_doc_LAW_283918
3. Национальное бюро расследований Финляндии отследило анонимные транзакции Monero // Bits Media. URL: https://bits.media/natsionalnoe-byuro-rassledovaniy-finlyandii-otsledilo-anonimnye-tranzaktsii-monero (дата обращения: 25.08.2024).

П. А. Дубровский,
студент,
Полоцкий государственный университет
имени Евфросинии Полоцкой

ВЛИЯНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА ФОРМИРОВАНИЕ ИДЕОЛОГИИ ГОСУДАРСТВА

Аннотация. В статье рассматриваются различные направления воздействия цифровых технологий на формирование идеологических установок и ценностей. Особое внимание уделяется исследованию искусственного интеллекта и его роли в реализации идеологической функции государства. Приводится и анализируется положительный опыт зарубежных стран по формированию идеологии государства с использованием искусственного интеллекта.

Ключевые слова: цифровизация, идеология, право, законодательство, ценности, государство, искусственный интеллект, общество

INFLUENCE OF DIGITAL TECHNOLOGIES ON THE IDEOLOGY OF THE STATE

Abstract. The article examines various directions of the impact of digital technologies on the formation of ideological attitudes and values. Particular attention is paid to the study of artificial intelligence and its role in the implementation of the ideological function of the state. The author presents and analyzes the positive experience of foreign countries in forming the ideology of the state using artificial intelligence.

Keywords: digitalization, ideology, law, legislation, values, state, artificial intelligence, society

Введение. Появление и развитие цифровых технологий ознаменовало собой новую эпоху, в которой «цифра» занимает значимое место в жизни человека, государства и общества в целом. Следовательно, на современном этапе цифровые технологии выступают в качестве инструмента реализации государством своей информационной функции [11].

Значимую роль играют цифровые технологии и при реализации идеологической функции государства, реализуемой посредством формирования и поддержания идеологических установок, общественных и государственных ценностей и др. Таким образом, при существенной простоте распространения информации цифровые технологии непосредственно влияют на формирование разного рода идей и ценностей гражданина.

Основная часть. Ценностные установки граждан, в свою очередь, в условиях демократического режима прямо или косвенно формируют идеологию государства и власти путем выборов. В результате проведенной конституционной реформы в Республике Беларусь (2022 г.) на уровне Основного Закона закреплена идеология белорусского государства в качестве важнейшей конституционной ценности (ч. 1 ст. 4 Конституции Республики Беларусь). Проведение государственной идеологической политики непосредственно оказывает влияние на устойчивость общественных отношений в государстве. Идеологические императивы являются одним из компонентов проведения правовой политики в Республике Беларусь (гл. 2 Концепции правовой политики Республики Беларусь).

Существует множество понятий идеологии: классическое (А. Дестют де Траси), марксистское (К. Маркс, В. Ленин) и понимание Франкфуртской школы (М. Хоркхаймер, Т. Адорно) и т. д. В основе проведения настоящего исследования лежит классическое понимание идеологии как системы концептуально оформленных представлений и идей, которая выражает интересы, мировоззрение и идеалы различных политических субъектов политики. Под идеологизацией понимается процесс проникновения и усвоения народом идеологических установок, который выражается как в идеологическом воздействии власти на народ (правовое просвещение молодых граждан, патриотические акции), так и в воздействии народа на власть (в частности, путем проведения референдума). Также под идеологизацией понимается процесс формирования идеологии в государстве.

Главную роль в «правовом самообразовании» человека играют информационно-правовые системы Республики Беларусь – «Эталон» и «Консультант Плюс», а также сайты государственных органов (сайт Президента Республики Беларусь, палат Национального собрания Республики Беларусь, судебных органов). Таким образом, среди спектра цифровых технологий «интернет вещей» является наиболее важным, ведь делает любую информацию, максимально доступной для всех субъектов общественных отношений.

Второй структурной частью цифровых технологий являются Большие данные (Big Data). Они представляют собой систему подходов к структурированию и предоставлению данных из разобщенных источников для наиболее эффективного использования [8. С. 38]. Данная технология занимает важное место при идеологизации, поскольку позволяет уполномоченным государственным органам «проецировать» идеологию на наибольшее количество людей. Также «Большие данные» сильно упрощают и автоматизируют существующие процессы в области идеологического образования, а также разных иных мероприятий, способствующих идеологическому воспитанию общества. Самыми явными представителями данного элемента в правовой сфере являются уже упомянутые ранее ИПС «Эталон» и «Консультант Плюс», а также другие правовые базы.

Третий элемент цифровых технологий представляет собой искусственный интеллект и связанное с ним машинное обучение [7]. В первую очередь этот элемент предназначен для автоматизации процессов во всех сферах деятельности человека и самообучения для последующего саморазвития. В настоящее время искусственный интеллект является наиболее приоритетным и потенциальным сектором развития в государстве и праве. Несмотря на то, что максимально эффективно ИИ будет действовать только в будущем, уже на сегодняшний момент существует опыт применения искусственного интеллекта в делах государства.

Технология ИИ возможна для использования на различных стадиях политического процесса. Поскольку ИИ не является носителем какой-либо идеологии, данная технология может быть использована для формирования любых идеологических ценностей и установок. Актуальным видится использование ИИ в процессе электоральной кампании в Республике Беларусь 2025 г.

Отметим несколько направлений влияния цифровых технологий на выбор идеологических ценностей гражданами. В первую очередь в цифровую эпоху людям становится открытой та информация, которая раньше была недоступна, и это повышает уровень грамотности населения. Во-вторых, цифровизация оказывает влияние на идеологию государства, формируя повестку власти, более зависимой от социальных медиа, а следовательно, и от общественного мнения, что в определенном смысле сковывает действия государственного аппарата [9. С. 58].

Важным для исследования является рассмотрение систем, существование которых поддерживают определенные идеи и ценности, составляющие в совокупности идеологию. Так, например, в некоторых европейских странах с марта 2014 по май 2016 г. работал британский проект D-CENT, целью которого было создание цифровых инструментов для прямой демократии и расширения экономических прав и возможностей граждан. Проект действовал в городах Рейкьявик, Хельсинки, Мадрид и Барселона. Результатом стало проведение анализа новых социальных, экономических, гражданских и политических моделей и выявление их эффективности. В Хельсинки гражданам было предложено подписаться на уведомления о действиях властей города и участие в обсуждении их, а в Мадриде запущена платформа для прямой демократии на муниципальном уровне [3]. В результате проекта было определено, что в государствах присутствует желание, а главное, возможности для реализации прямой демократии, что означает наличие спроса на формирование такой идеологии. Однако, несмотря на наличие спроса на прямую демократию, проект с законодательной точки зрения можно считать неудачным, поскольку дальше этого проекта ничего не пошло, что, тем не менее, не исключает будущего юридического закрепления достигнутых результатов.

Вторым идеологическим примером, реализующимся посредством цифровых технологий, является система «социального рейтинга» в Китайской Народной Республике. Данная система включает в себя базу данных китайских физических и юридических лиц (в том числе черные и красные списки) и систему поощрения и наказания. Данная система работает по аналогии с кредитным рейтингом: если маленький рейтинг – ненадежный гражданин и организация, если больше установленной цифры – порядочный гражданин и надежная компания [1]. «Социальный рейтинг» – самый яркий пример применения цифро-

вых технологий для укрепления государственной идеологии, ведь в этой системе на полную используются не только «Большие данные», но и искусственный интеллект и интернет вещей [2].

Одним из самых недавних, хотя пока не реализованных примеров применения цифровых технологий на государственном уровне, является инициатива действующего президента Аргентины, предполагающая использование ИИ для предсказания, выявления и расследования преступлений.

Что важно отметить, план предполагает контроль не только в реальном, но и виртуальном мире, что говорит о задействовании всех трех элементов цифровых технологий в данном деле. Также в связи с данным планом было создано Подразделение Министерства безопасности Аргентины по искусственному интеллекту, которое и будет заниматься контролем за предотвращением преступлений на основе машинного обучения [5]. Данный пример хорошо иллюстрирует, что цифровые технологии, помимо позитивного влияния на идеологию, могут оказывать и негативное. Однако, несмотря на характер влияния, технологии все так же служат укреплению позиции государства и власти в области идеологии и идеологического воздействия.

Стоит рассмотреть также, с какими последствиями сопряжена цифровизация общества в будущем и как она влияет на государство, граждан и идеологию уже в данный момент времени. Первое, о чем стоит сказать, – становление цифрового тоталитаризма в области идеологического воздействия государства на граждан. Как показывает еще не реализованный пример Аргентины, цифровые технологии могут использоваться властью для ограничения свободы слова в своих интересах [11. С. 44], что также является негативным проявлением использования цифровых технологий в идеологических целях. Сам цифровой тоталитаризм подразумевает под собой не только ограничение прав и свобод (в особенности свободы слова), но и контроль государства всех сфер жизни посредством цифрового контроля [6. С. 19].

Следующим последствием влияния цифровизации на идеи и ценности является деполяризация общественного мнения. Под этим термином понимается выход политических лагерей из своих так называемых эхо-камер в связи с увеличением альтернативных точек зрения, способов коммуникации и более открытой разнообразной информации, что и приведет к тому, что люди разных взглядов начнут слышать отличный от своего мировоззрения взгляд на вещи.

Третьим направлением влияния цифровых технологий на политику государства станет становление прямой демократии. Как уже было сказано ранее, на данный момент уже существуют прецеденты использования цифровых технологий для осуществления данной идеи, показавшие возможность и необходимость, также в современном мире присутствуют возможности для их реализации.

Заключение. Таким образом, несмотря на раннюю стадию своего развития, цифровые технологии активно находят свое применение в жизни граждан и в деятельности государственного аппарата. Основными направлениями воздействия цифровых технологий на идеологию государства являются: формирование политической и правовой культуры граждан в цифровой среде, усиление (ослабление) политической активности, формирование «электоральных ценностей» народа и др. Особую ценность для формирования государственной идеологии в будущем

будет играть ИИ, с помощью которого возможны формирование и распространение идеологических ценностей и установок применительно к большому количеству населения, что важно для реализации идеологической функции государства.

Список литературы

1. China Social Credit System Explained – What is it & How Does it Work? [2024] [Электронный ресурс]. URL: https://joinhorizons.com/china-social-credit-system-explained (дата обращения: 13.08.2024).

2. China 'social credit': Beijing sets up huge system – BBC News [Электронный ресурс]. URL: https://www.bbc.com/news/world-asia-china-34592186 (дата обращения: 13.08.2024).

3.D-CENT_PUBLISHABLE-SUMMARY-05-2016_A5_final_web.pdf [Электронный ресурс]. URL: https://dcentproject.eu/wp-content/uploads/2016/06/D-CENT_PUBLISHABLE-SUMMARY-05-2016_A5_final_web.pdf (дата обращения: 13.08.2024).

4. Making AI Work for the American People [Электронный ресурс]. URL: https://ai.gov (дата обращения: 11.08.2024).

5. Will Milei's AI Policing Plan Become a Tool for Social Control? [Электронный ресурс]. URL: https://reason.com/2024/08/07/could-mileis-ai-policing-plan-become-a-tool-for-oppression (дата обращения: 14.08.2024).

6. Евстратов А. Э., Шугулбаев Ж. А. К вопросу об идеологической функции государства в цифровую эпоху // Правоприменение. 2024. № 1. С. 15–23.

7. Бегишев И. Р., Хисамова З. И. Искусственный интеллект и робототехника: глоссарий понятий. М.: Проспект, 2021. 64 с. EDN: HQELSK.

8. Машевская О. В. Цифровые технологии как основа цифровой трансформации современного общества // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. 2020. № 1. С. 37–44.

9. Митрахович С. П. Эффекты цифровизации как вызовы для эффективности демократии и «массовой политики» на современном этапе // Гуманитарные науки. Вестник Финансового университета. 2022. № 12(5). С. 57–62.

10. Залоило М. В. Трансформация роли государства в современном мире: парадигмальные сдвиги концепции суверенитета // Вестник МГПУ. Серия: Юридические науки. 2023. № 2(50). С. 5–18.

11. Трощинский П. В. Цифровой Китай до и в период коронавируса: особенности нормативно-правового регулирования // Право и цифровая экономика. 2021. № 1(11). С. 44–58.

А. А. Дыев,
студент,
Полоцкий государственный университет имени Евфросинии Полоцкой

ПРАВО ЛИЧНОСТИ НА КОНТРОЛЬ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ

Аннотация. В статье рассматривается содержание понятия «цифровой аватар» как активный субъект деятельности в метавселенной. Делается акцент

на необходимость обеспечения подконтрольности виртуального пространства и установления режима законности в информационном обществе. Представлено несколько подходов к данной проблематике.

Ключевые слова: виртуальное пространство, личность, цифровой аватар, государство, контроль, право на виртуальное моделирование, соматические права

INDIVIDUAL RIGHT TO CONTROL IN THE VIRTUAL SPACE

Abstract. The article examines the content of the concept of “digital avatar” as an active subject of activity in the metaverse. The author focuses on the need to ensure control of the virtual space and establish a regime of legality in the information society. Several approaches to this problem are presented.

Keywords: Virtual space, personality, digital avatar, state, control, right to virtual modeling, somatic rights

Введение. С развитием информационных технологий появляются качественно новые сферы жизни, безусловно требующие правового регулирования в целях соблюдения порядка и общественного строя. В настоящее время технологическое развитие идет не линейно, а экспоненциально. В такой ситуации «догоняющая» тактика правовой регламентации может представлять угрозу нарушения прав личности, устойчивого развития общества и государства. Законодателю необходимо максимально быстро и при этом не теряя качества закона принимать акты о регулировании нового круга общественных отношений (в юридической науке такие отношения зачастую именуются цифровыми) [11].

В последние годы получает широкое распространение виртуальное моделирование личности, что, на наш взгляд, является одним из соматических прав человека [1. С. 43]. В связи с этим возникает потребность в законодательном установлении прав и обязанностей, норм поведения цифровой личности в виртуальной среде.

Основная часть. Понятие цифровой личности связано с понятием метавселенной [9]. На данный момент существующие виртуальные миры фрагментарны, независимы и не связаны между собой [2. С. 8]. Самыми популярными метавселенными являются Roblox, Decentraland, Sandbox, Spatial. Одной из главных особенностей метавселенных является наличие в них реальной экономики, возможности получать прибыль посредством обращения криптовалюты. Первые этапы регулирования криптовалюты в Республике Беларусь обозначены в Указе Президента Республики Беларусь от 14 февраля 2022 г. № 48 «О реестре адресов (идентификаторов) виртуальных кошельков и особенностях оборота криптовалюты» [10].

Метавселенная представляет собой совокупность множества виртуальных реальностей, в рамках которых действуют «особые субъекты права», действующие на основе юнитов искусственного интеллекта (часто именуемые цифровыми аватарами). Цифровой аватар является одной из разновидностей цифровой модели личности. С появлением метавселенной намечается реализация концепции цифрового гражданства, эти модели могут быть наделены гражданскими и политическими правами. Или владельцы таких моделей будут наделены новыми способами осуществления этих прав. Необходимо понять, каким

образом регулировать действия с этой моделью: по образу реального права или же принципиально новыми способами. У правоведов есть различные позиции по отношению к правосубъектности цифровой личности.

Первый вариант – рассматривать цифровую личность как качественно новую, самостоятельную и отдельную вариацию субъекта права. Многие правоведы, среди которых И. А. Филипова, исследуют вопрос о признании цифровых аватаров субъектами права [2]. В таком случае, скорее всего, потребуется новая правовая система, новая, виртуальная конституция, определяющая правовые основы виртуального мира, правовое положение цифровой личности и основы порядка управления виртуальным миром. К виртуальному миру следует подходить космополитично, так как не предоставляется возможность определить связь виртуального мира и его субъектов ни с национальностью, ни с территорией [3. С. 179]. В таком случае контроль над метавселенной следует отделять от государственного контроля.

Второй вариант – рассматривать аватар как виртуальную проекцию реальной личности, не наделенную разумом и самостоятельностью в своих действиях, свойственных субъекту права. То есть закрепить контроль цифрового аватара реальным человеком. В данном случае может потребоваться создание новой отрасли права, регулирующей отношения в сфере взаимодействия этих аватаров. В каждом государстве необходимо будет создать орган по учету и контролю действий с цифровыми аватарами. С рождением нового человека будет создаваться индивидуальный аватар как модель его личности, посредством которой он сможет реализовывать свои реальные права. Уже сейчас есть яркий пример возможности реализации реальных прав через виртуальный мир. В действующем законодательстве Российской Федерации уже предусмотрено электронное голосование [4], успешно и результативно работает сервис «Госуслуги», наблюдаются тенденции к платформизации государственного управления.

Есть и иные точки зрения, среди которых научный подход В. В. Архипова, в соответствии с которым аватары могут рассматриваться как предмет правоотношений в области интеллектуальной собственности [5. С. 58], т. е. в данном случае потребуется расширение уже существующего гражданского законодательства. Однако такая позиция не рассматривает вопрос отнесения цифровых аватаров к субъектам права, а предлагает доктринальное переосмысление скорее теории объекта правоотношений.

Современные правоведы проводят исследование содержания права на виртуальное моделирование личности, относя его к соматическим. Ведутся дискуссии по установлению пределов осуществления в том числе и этого права. Четко определить пределы осуществления соматических прав личности в отношении права на виртуальное моделирование с целью дублирования себя в нематериальной форме объективного существования не представляется возможным вследствие неопределенности соотношения виртуальной модели личности с телом человека в нынешней правовой парадигме. Здесь тоже возникают проблемы отделения сознательного от телесного в человеке. Возникает также вопрос о принадлежности права на контроль такой модели и соотношение реализации этого права личностью с интересами общества и государства. С позиции Э. В. Никитиной

и Д. А. Волковой, необходим приоритет государства в отношении контроля деятельности таких аватаров. Необходимо строго очертить границы дозволенного в виртуальном пространстве, запретить множественность моделей одной личности, так как новая реальность, будучи неконтролируемой, предоставит огромное поле возможностей для противоправного поведения и создаст для общества реальные угрозы нарушения правопорядка [6. С. 133]. Недопустима анонимность субъектов виртуального моделирования, требуется строгий учет моделей в целях недопущения безнаказанности в виртуальном пространстве. Необходимо также продумать и закрепить на законодательном уровне соответствующие характеристикам виртуального мира санкции, прообразы которых уже давно используются в социальных сетях и онлайн-играх (различные баны, блокировки и заморозки аккаунтов). С другой стороны, А. А. Самарин говорит о наличии тенденции к заявлению преимущественно философами-либералами о свободе киберпространства от государственного контроля, саморегуляции виртуального сообщества. Они также заявляют о примате интересов личности в киберпространстве [7. С. 667].

Заключение. Таким образом, в настоящее время есть множество подходов к проблематике виртуального моделирования личности, отношения к личности в виртуальном пространстве, контроля таких личностей, правосубъектности аватаров. Очевидно, право не может существовать в условиях неточности формулировок и зыбкости понятий, поэтому законодателям необходимо выработать единый подход, который будет сочетать в себе интересы личности, общества и государства. Безусловно, необходим правовой контроль виртуальной среды [6. С. 130], но ни в коем случае нельзя допускать захват контроля виртуальным миром против интересов человечества, вполне реальные риски коего имеются [8. С. 183]. Право должно регулировать общественные отношения, улучшая качество жизни лица, расширяя его возможности, удовлетворяя его потребности в самосовершенствовании. На наш взгляд, цифровой аватар является продолжением физической личности в виртуальном мире, предоставляющим субъекту дополнительные возможности более эффективной правореализации. Право личности на контроль в виртуальном пространстве следует относить к соматическим правам, реализуемым в сети Интернет.

Список литературы

1. Крусс В. И. Личностные («соматические») права человека в конституционном и философско-правовом измерении: к постановке проблемы // Государство и право. 2000. № 10. С. 43–50.

2. Филипова И. А. Создание метавселенной: последствия для экономики, социума и права // Journal of Digital Technologies and Law. 2023. № 1. С. 7–32.

3. Бек У. Что такое глобализация? Москва: Прогресс-традиция, 2001. 303 с.

4. Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации: Федеральный закон от 12 июня 2002 г. № 67-ФЗ // Консультант Плюс.

5. Архипов В. В. Персонажи (аватары) в многопользовательских компьютерных играх: вопросы правовой квалификации в свете междисциплинарных исследований // Закон. 2022. № 3. С. 58–74.

6. Никитина Э. В., Волкова Д. А. К вопросу о правовом ограничении свободы в виртуальной реальности // Вестник РУК. 2021. № 3(45). С. 130–136.

7. Самарин А. А. Экстерриториальное действие юридических норм в условиях стратегий глобализации // Юридическая техника. 2015. № 9. С. 666–672.

8. Скородумова О. Б. Социальные риски эпохи тотальной цифровизации // Научные исследования и инновации. 2021. № 4. С. 183–186.

9. Уголовно-правовое значение метавселенных: коллизии в праве / Р. А. Сабитов [и др.] // Правопорядок: история, теория, практика. 2023. № 4(39). С. 58–62. EDN: HEHWGN

10. О реестре адресов (идентификаторов) виртуальных кошельков и особенностях оборота криптовалюты: Указ Президента Республики Беларусь от 14 февраля 2022 г. № 48 // Эталон. Законодательство Республики Беларусь. Минск, 2024.

11. Концепция цифрового государства и цифровой правовой среды: монография. М.: ИЗиСП: Норма: ИНФРА-М, 2024.

З. Д. Жирнова,
студент,
Всероссийский государственный университет юстиции
А. А. Жукова,
студент,
Всероссийский государственный университет юстиции

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ПРОБЛЕМЫ ИДЕНТИФИКАЦИИ И ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ СЛЕДОВ В ЦИФРОВОЙ КРИМИНАЛИСТИКЕ

Аннотация. В век цифровых технологий информация стала одной из главных ценностей общества. Мы постоянно находимся в информационном пространстве, что одновременно открывает новые способы совершения преступлений для злоумышленников, и представляет большой интерес для современной криминалистики, так как является полем для составления цифровой следовой картины преступления. Киберпреступность чаще всего оказывается на шаг впереди следователей-криминалистов. Даже в условиях современного развития технологий расследование киберпреступлений остается довольно сложной задачей для сотрудников правоохранительных органов. Методика применения цифровых следов в раскрытии преступлений не до конца разработана ввиду ее новизны, несмотря на наличие различных научных исследований. Необходимо комплексное решение проблем, описанных в нашей работе, чтобы добиться максимальной эффективности в сфере цифровой криминалистики.

Ключевые слова: право, идентификация, цифровые следы, цифровая криминалистика, киберпреступность, кибербезопасность, цифровые технологии, судебная экспертиза, правоохранительная деятельность.

ORGANISATIONAL AND LEGAL PROBLEMS OF IDENTIFICATION AND USE OF DIGITAL TRACES IN DIGITAL FORENSICS

Abstract. In the age of digital technology information has become one of the main values of society. We live in the information space. Firstly, it opens new ways of committing crimes for criminals. Secondly, it is of great interest for modern forensics as it is a field for making up a digital trace picture of a crime. Cybercrime is most often one step ahead of criminal investigators. Even with the modern development of technology, the investigation of cybercrime remains quite a challenge for law enforcement officers. The methodology of applying digital traces in crime detection is not fully developed due to its novelty, despite the presence of various scientific studies. It is necessary to comprehensively address the problems described in our paper to maximize the effectiveness in the field of digital forensics.

Keywords: identification, digital traces, digital forensics, cybercrime, cybersecurity, modern technologies, forensic examination, law enforcement.

Введение. Количество пользователей Интернета увеличилось по сравнению с началом XXI в. почти в тринадцать раз [4], пропорционально ему растет и число преступлений, совершаемых в сфере телекоммуникаций и компьютерной информации. Темпы цифровизации и развития компьютерных технологий позволяют преступникам находить больше новых методов совершения неправомерных действий. «По данным МВД, каждое третье преступление было совершено с использованием цифровых инструментов. Общее их число в 2023 г. составило 677 тыс. При этом наблюдается негативная динамика. Рост к прошлому периоду составляет практически 30 %. В 2022 г. ведомство зафиксировало порядка 522 тыс. преступлений» [9].

Основная часть. В разбирательствах по уголовным делам все чаще применяются цифровые доказательства, но из-за неправильного их толкования, к сожалению, нередко невиновные оказываются за решеткой, а виновные остаются безнаказанными.

Исследование статистических данных, научных работ и учебной литературы позволило выделить несколько проблем идентификации и использования цифровых следов в цифровой криминалистике:

1) нехватка экспертов и специалистов [7. С. 57–58] в правоохранительных органах и низкая квалификация сотрудников. Более трети отечественных компаний (около 35 %) нуждаются в таких квалифицированных сотрудниках в сфере кибербезопасности [12], по данным статистики, приведенной агентством РИА «Новости». В августе 2023 г. глава Минцифры Максут Шадаев заявил, что в России имеется нехватка около 700 тыс. ИТ-специалистов. Это давний тренд, начавшийся, как сообщает CNews, еще в 2020 г. и заметно усилившийся после 24 февраля 2022 г. [1]. Опросы среди следователей показывают, что 95 % респондентов получили юридическое образование. И только 5 % обладают еще и образованием по специальности «информатика и вычислительная техника». 63 % опрошенных владеют компьютером на уровне среднего пользователя, 37 % – на уровне продвинутого пользователя. 79 % при этом постигают компьютер самостоятельно, курсы

для сотрудников правоохранительных органов посещали только 21 % и незначительный процент (5 %) – коммерческие курсы [3]. В 22 % случаев использования цифровых доказательств они оказываются неверно истолкованными [11].

Одним из возможных решений этой проблемы может стать введение новых направлений высшего и среднего специального образования, новых учебных дисциплин. Как результат, увеличение количества квалифицированных специалистов позволит создать специализированные подразделения, которые будут заниматься расследованием дел, связанных с преступлениями в цифровой среде, для эффективного противодействия злоумышленникам, расследования преступлений. К примеру, одной из задач Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации (УБК МВД России) является взаимодействие с образовательными организациями системы МВД России, иными образовательными организациями по вопросам подготовки кадров для подразделений по борьбе с киберпреступлениями;

2) недостаток релевантных методических рекомендаций по борьбе с цифровой преступностью. Она развивается с невообразимой скоростью, в связи с чем различные научные материалы, учебные пособия и другие информационные ресурсы достаточно быстро устаревают. Также в процессе развития науки и технологий появляется огромное количество новых терминов, определений, явлений, из-за чего иногда появляются разночтения и недопонимания между учеными и другими людьми, имеющими отношение к этой сфере, так как дефиниции в большинстве случаев отсутствуют. Это связано с нехваткой актуальной информации. Решением может стать написание учебной литературы практикующими специалистами по кибербезопасности и юристами в той же области (совместно с учеными). Они разбираются в трудных аспектах своей деятельности и знают многие нюансы и подводные камни, и их опыт помог бы коллегам и начинающим узнать новые методики, терминологию и т. п.;

3) недостаток международного сотрудничества в сфере пресечения киберпреступности. Не менее важным и актуальным вопросом является легитимность получения данных о преступниках из источников, принадлежащих иностранным государствам, которые не предоставляют данные пользователей спецслужбам других стран. Возможным решением нам представляется развитие международного сотрудничества: создание правовых актов и соглашений в области противодействия киберпреступности между странами, создание методических рекомендаций для служб в государствах. Однако эта проблема все еще требует разработки решения ввиду того, что международный договор о предоставлении данных граждан одного государства другому представляет собой угрозу информационной безопасности личности, общества и государства;

4) нехватка специализированной отечественной техники. Несмотря на то, что современные цифровые технологии достаточно широко используются в правоохранительной деятельности, этого порой бывает недостаточно ввиду быстрого их устаревания. В настоящее время для обработки информации в правоохранительных органах используются такие виды информационных систем, как автоматизированные системы обработки данных, автоматизированные информационно-поисковые и информационно-справочные системы, экспертные системы и тому

подобные разработки. Цифровизация в нашей стране еще продолжается, направление ей дают стратегические документы, принятые Президентом Российской Федерации – Стратегия развития информационного общества в Российской Федерации, Доктрина информационной безопасности [8]. Необходима разработка нового оборудования для экспертов-криминалистов, поскольку с появлением новых видов цифровых преступлений появляются и цифровые следы, которые ранее не использовались в качестве доказательств и их экспертиза еще не проводилась. Соответственно, может не быть оборудования, которое позволило бы качественно их исследовать и вынести верное заключение. Производство оборудования должно начаться в нашей стране, поскольку из-за обострения международной обстановки оно не доставляется из зарубежных государств;

5) дипфейки как новый способ совершения преступлений. Из-за активного развития искусственного интеллекта появляются новые виды дипфейков с реалистичной подменой фото-, видео- и аудиоматериалов, что, в свою очередь, детерминирует новые виды правонарушений, в том числе регулируемых нормами гражданского права (ст. 152.1 ГК РФ – «Охрана изображения гражданина»). Например, при создании произведений с помощью технологии дипфейка может быть нарушено авторское право на фото- и видеоматериалы. Голосовые дипфейки подвергают наибольшей опасности права человека, так как на голос авторское право не распространяется [2. С. 116]. Решить эту проблему пока довольно сложно, так как дипфейки и искусственный интеллект появились относительно недавно и находятся на стадии быстрого развития. Однако можно ввести правовые нормы, например, регулирующие применение искусственного интеллекта, защищающие авторское право на голос и ограничивающие использование биометрических данных без согласия человека (его фотографии и т. п.). Также следует попытаться разработать программное обеспечение или методики, позволяющие отличить оригинальные фото-, видео- и аудиоматериалы от поддельных, созданных с помощью дипфейка.

Один из главных принципов деятельности по борьбе с преступностью, на наш взгляд, – принцип неотвратимости наказания как принцип уголовного права [9]. Он должен быть реализован в цифровой криминалистике. С этой целью необходимо разрабатывать новые криминалистические характеристики для идентификации цифровых следов, которые могут быть использованы в качестве доказательств в судебном процессе [10].

Существенный вклад в изучение правовой проблемы идентификации и использования цифровых следов в криминалистике внесли:

– Е. Р. Россинская, разработавшая концепцию теории информационно-компьютерного обеспечения криминалистической деятельности;

– А. А. Курин и В. В. Гаужаева, сформулировавшие перечень мероприятий, которые могут быть реализованы системой на базе метапоисковой аналитической системы криминалистической регистрации на основе обработки электронно-цифровых следов;

– А. А. Бессонов, который дал определение электронных следов, указал их источники, значение в расследовании преступлений, возможности информационно-аналитических исследований больших массивов информации;

– П. Джозеф и Ж. Норман, сравнившие методы криминалистического поиска в цифровых корпусах;

– А. Рани и А. Джан, давшие представление о методах, связанных с криминалистической экспертизой цифровых изображений.

Несмотря на многие исследования и достижения в данной области, обозначенные проблемы требуют комплексной проработки ввиду ее стремительного развития. В частности, важно разрабатывать и вводить новые программы обучения в сфере цифровой криминалистики и юриспруденции в целом, соответствующие уровню развития технологий. Более того, преподаваемые дисциплины нужно постоянно актуализировать в связи с быстрым устареванием информации, которая составляет теоретическую и практическую основу деятельности. Необходимо также взаимодействие правоохранительных органов и частных компаний, занимающихся борьбой с киберпреступностью, с образовательными учреждениями высшего и среднего профессионального образования для повышения квалификации сотрудников, уже имеющих опыт работы. Не менее важно создавать обучающие материалы, авторы которых ежедневно занимаются вопросами практики с юридической и технической точек зрения и могут помочь своим коллегам углубить свои знания. Международное сотрудничество тоже играет значительную роль в предотвращении случаев киберпреступности и пресечения неправомерных действий, и его нужно развивать. Оно может помочь и в техническом обеспечении процесса сбора и исследования цифровых следов и доказательств, однако организация отечественного производства имеет большое значение. Законодательство не должно отставать от технического прогресса, ведь тогда будет сложно регулировать возникающие правоотношения и своевременно решать все вопросы, связанные, например, с использованием искусственного интеллекта [11] при совершении преступлений. Чем быстрее будут разрешены все эти проблемы, тем легче станет расследование киберпреступлений [12] для всех следователей.

Список литературы

1. В России острая нехватка ИТ-безопасников и сетевых инженеров. Компании ищут их и не могут найти. Опрос // CNews: сайт. URL: https://www.cnews.ru/news/top/2024-01-23_v_rossii_ostraya_nehvatka

2. Добробаба М. Б. Дипфейки как угроза правам человека // Lex Russica. 2022. № 11(192).

3. Киберпреступления: основные проблемы расследования // Институт судебных экспертиз и криминалистики: сайт. URL: https://ceur.ru/library/articles/obshhie_stati/item196792

4. Колычева А. Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. … канд. юрид. наук. М., 2018. 199 с.

5. Россинская Е. Р. К вопросу об инновационном развитии криминалистической науки в эпоху цифровизации // Юридический вестник Самарского университета. 2019. № 4.

6. Стрилец О. В., Семененко Г. М., Пахомов А. Н. Неотвратимость наказания как принцип уголовного права // Вестник Волгоградской академии МВД России. 2020. № 2(53).

7. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 29.05.2024) // Рос. газ. 2001, 22 декабря.

8. Цифровая криминалистика: учебник для вузов / В. Б. Вехов [и др.]. – 2-е изд., перераб. и доп. М.: Юрайт, 2024. 490 с.

9. Число киберпреступлений в России. 2024: Доля киберпреступлений в России за год достигла 38 % в общем количестве: сайт. URL: https://www.tadviser.ru

10. Шаповалова Г. М. Возможность использования информационных следов в криминалистике: Вопросы теории и практики: дис … канд. юрид. наук. Владивосток, 2006. 21 с.

11. Бегишев И. Р., Хисамова З. И. Искусственный интеллект и робототехника: глоссарий понятий. М.: Проспект, 2021. 64 с. EDN: HQELSK

12. Motives and Objectives of Crime Commission Against Information Security / A. Yu. Bokovnya [et al.] // Ad Alta. 2020. Vol. 10, № 2 S13. Pp. 7–9. EDN: SCSEBN

У. В. Жук,
студент,
Иркутский государственный университет

ТЕХНОЛОГИЯ DEEPFAKE: ЛАНДШАФТ СОВРЕМЕННОСТИ ИЛИ НОВАЯ СФЕРА, ТРЕБУЮЩАЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ?

Аннотация. В статье рассматривается феномен deepfake-технологии, позволяющей создавать фальшивые видео- и аудиозаписи с помощью искусственного интеллекта. Анализируется влияние deepfake на современное общество и подчеркивается необходимость разработки правовых механизмов для борьбы с возможным злоупотреблением этой технологией. Основная цель статьи заключается в обосновании того, что deepfake представляет собой новую сферу, требующую внимания законодателей и общественности, регулирование которой необходимо для того, чтобы защитить персональные данные, приватность и общественную безопасность.

Ключевые слова: искусственный интеллект, цифровое право, цифровизация общества, deepfake, современные технологии, дополненная реальность, правовое регулирование

DEEPFAKE TECHNOLOGY: A LANDSCAPE OF MODERNITY OR A NEW SPHERE REQUIRING LEGAL REGULATION?

Abstract. The article discusses the phenomenon of deepfake-technology, which allows creating fake video and audio recordings with the help of artificial intelligence. The author analyzes the impact of deepfake on modern society and emphasizes the need to develop legal mechanisms to combat the possible abuse of this technology. The main goal of the article is to prove that deepfake is a new sphere that requires attention of legislators and the public, regulation of which is necessary in order to protect personal data, privacy and public safety.

Keywords: artificial intelligence, digital law, digitalization of society, deepfake, modern technologies, augmented reality, legal regulation

Введение. На современном этапе развития активной цифровизации общества понятие «искусственный интеллект» ежедневно дополняется, обрастая все новыми и новыми разновидностями и сферами, в которых технологические достижения прогресса могут использоваться.

В настоящий момент активные попытки внедрения искусственного интеллекта можно наблюдать в медицине [1, 2], образовании, юриспруденции, а также во многих иных областях общественной жизни. Искусственный интеллект [3, 4] обрабатывает огромное количество информации за короткий промежуток времени, генерирует тексты, изображения, видео, осуществляет поиск и подбор релевантных предложений по запросам пользователей, генерирует идеи и ответы на сложные вопросы и казусы на основе данных, вложенных в него человеком.

Несмотря на позитивные возможности и открывающиеся перспективы использования искусственного интеллекта, в настоящий момент отсутствует четкое правовое регулирование такой разновидности искусственного интеллекта, как, например, deepfake-технология (далее – дипфейк), поэтому в контексте настоящего исследования автор считает необходимым проанализировать с точки зрения права само по себе существование дипфейка, его использование при создании и распространении вышеупомянутого контента, а также высказать авторскую точку зрения относительно вопроса привлечения к ответственности за неправомерное использование дипфейка или злоупотребление данной технологией.

Основная часть. Для более четкого понимания сущности комментируемого явления необходимо унифицировать дефиницию дипфейка, через призму которой он и будет рассматриваться в контексте настоящего исследования.

Дипфейк – это технология, основанная на искусственном интеллекте, целью которой является создание аудиовизуального и голосового контента на основе данных, которым «обучить» дипфейк сможет только человек.

Так, например, с помощью неправомерного использования и злоупотребления данной современной технологией может совершаться множество правонарушений (преступлений), влекущих определенный уровень общественной опасности как для отдельно взятого человека, так и для общества в целом:

1. Финансовое вымогательство: фальсификация фотографий или видео в изобличающей или позорящей манере в ситуациях, когда преступники вымогают деньги у своей жертвы; обход аутентификации Face ID на веб-сайтах и/или в мобильных банковских приложениях для получения несанкционированного доступа и т. д.

2. По сути, данная технология предполагает использование искусственного интеллекта для «снятия» одежды с изображения человека и создания приблизительной картины его обнаженного тела.

Преступники часто используют вышеупомянутую технологию, чтобы манипулировать ничего не подозревающими жертвами. Этот метод чрезвычайно безжалостен с точки зрения человечности и может оказать глубокое негативное влияние на психоэмоциональное состояние и социальную жизнь жертвы. Как правило, в отношении жертвы создается фейковое откровенное изображение или видео, собирается информация обо всех ее социальных контактах и взаимодействиях, а затем фейковый откровенный контент используется, чтобы шантажиро-

вать жертву для цели получения денег, имущества или ее принуждения к совершению определенных действий. Если жертва отказывается выполнять требования преступника, фейковый контент обычно распространяется среди ее окружения, а вымогательство продолжается с использованием более жестоких форм насилия. С точки зрения автора, именно deepnudes, вероятно, должно стать одним из основных направлений будущего законодательства о дипфейках.

3. Политические манипуляции: все, что касается политической сферы любого государства, обычно связано с прямым и очень сильным влиянием деятельности какого-либо лица на сознание электората, в связи с чем воссоздание виртуальной копии харизматичного политического лидера (особенно в странах с характерно выраженным культом личности) – еще одно направление неправомерного использования дипфейк-технологии. В преддверии американских президентских выборов – в социальных сетях бурные общественные волнения вызвало видео с якобы пьяной Нэнси Пелоси – спикером Палаты представителей Конгресса и одной из самых авторитетных персон Демократической партии США. После вышеприведенных прецедентов крупнейшие американские социальные сети добавили в свои правила запреты на дипфейки, которые используются для дезинформации, а в 2019–2020 ггг. четыре американских штата ввели уголовное наказание за использование дипфейков в политической рекламе [5].

Кроме того, еще одним беспрецедентным случаем использования дипфейка является мошенничество с помощью применения так называемого группового дипфейка – данный метод использовали мошенники, чтобы обмануть гонконгскую компанию на сумму в почти 26 миллионов долларов. В СМИ появилась информация о том, что транснациональная компания (название которой не разглашается) понесла значительные финансовые потери из-за действий сотрудника финансового отдела, который получил на свой рабочий аккаунт электронное письмо якобы от старшего менеджера из британского головного офиса. В письме содержалось приглашение присоединиться к видеоконференции. Финансист перешел по ссылке и оказался лицом к лицу не только со своим непосредственным руководителем, но и с несколькими другими коллегами. Спустя некоторое время оказалось, что на этой видеовстрече был настоящим только сам обманутый сотрудник. Остальные участники были сгенерированы с помощью дипфейка – их внешность и голоса были подделаны, однако настолько качественно, что у сотрудника не возникло подозрений, поэтому он перевел на указанные ими счета около 26 миллионов долларов и заподозрил неладное только спустя неделю [6].

По мнению автора, наличие вышеупомянутых случаев и потенциальная возможность совершения различных правонарушений с помощью дипфейка, заставляет задуматься о создании регулирования данной технологии с точки зрения различных отраслей права: конституционного, гражданского, административного и, безусловно, уголовного, о котором автор предпримет попытку порассуждать ниже.

Говоря о привлечении к уголовной ответственности за неправомерное использование дипфейка в контексте системы права Российской Федерации, возникает резонное предложение о введении в Уголовный кодекс РФ нового состава преступления, в соответствии с которым виновное лицо будет привлекаться к уголовной ответственности.

Введение отдельного состава преступления, который закреплял бы уголовную ответственность за использование дипфейка – действие весьма преждевременное в условиях современных российских реалий, которое может привести к избыточному правовому регулированию и созданию в уголовном законодательстве еще одной «мертвой» правовой нормы. Такое излишнее регулирование повлечет за собой возникновение квалификационных ошибок, вызванных сложностями при разграничении смежных составов преступлений, которые также могут быть совершены с использованием дипфейка (например, мошенничество, вымогательство, клевета и т. д.).

Кроме того, при введении уголовной ответственности за злоупотребление дипфейк-технологиями, законодатель и правоприменитель могут столкнуться и с иными проблемными аспектами, например, такими как установление возраста привлечения к уголовной ответственности; наличие/отсутствие умысла; зачастую полная анонимность лиц, совершающих подобные преступления; а также трудность сбора так называемых цифровых следов преступления с процессуальной точки зрения.

В контексте правового регулирования дипфейков через призму российского уголовного законодательства наиболее предпочтительным вариантом, по мнению автора, считается внесение изменений в ст. 63 Уголовного кодекса РФ в виде ее дополнения новым отягчающим обстоятельством, которое может звучать следующим образом: «совершение преступления посредством неправомерного использования технологий искусственного интеллекта». Данная мера, вероятнее всего, будет не так радикально смотреться в тексте уголовного законодательства РФ, однако однозначно будет носить превентивный характер, подразумевающий под собой осознание преступником факта применения к нему как к виновному лицу более серьезной санкции, чем могла бы быть.

В качестве «рационализаторских предложений» по разработке первоначального правового регулирования дипфейков автором могут быть предложены следующие способы снижения неправомерного использования дипфейк-технологии, направленные на приобретение и накопление положительного опыта применения возможностей искусственного интеллекта, например:

1. Создание и разработка первичной нормативно-правовой базы в данной области.

2. Законодательное закрепление за создателями программного обеспечения/программного кода, на основе которого написан дипфейк, обязанности получения лицензии в соответствующем ведомственном органе, дающей права пользования, владения и распространения технологий искусственного интеллекта, целью которых является правомерное создание дипфейк-контента для личных, профессиональных, развлекательных, научно-исследовательских и иных целей. Данная мера будет направлена на отслеживание оборота приложений/сайтов/программ, которые с завидной периодичностью выпускаются под эгидой развития технологического прогресса. По мнению автора, в данной связи целесообразным видится дополнение ст. 12 Федерального закона «О лицензировании отдельных видов деятельности» еще одним видом деятельности, на который будет требоваться лицензия.

3. Создание системы контроля за интернет-ресурсами, целевое назначение которых направлено на возможность использования дипфейка в различных целях посредством закрепления за такими ресурсами официальных сертифицированных доменных адресов, посещая которые можно будет только правомерно воспользоваться дипфейк-нейросетями, с соблюдением при этом баланса между пользовательской регистрацией и конфиденциальностью информации, включающей в себя в том числе и персональные данные зарегистрированных пользователей.

4. Закрепление за соответствующими органами исполнительной власти (например, за Роскомнадзором) обязанности по мониторингу и принудительному удалению со всех доступных интернет-ресурсов программного обеспечения, использующего дипфейк для генерации изображений обнаженного человеческого тела (Deepnudes).

Заключение. Таким образом, опираясь на все вышеизложенное и завершая раскрытие вопроса относительно необходимости правового регулирования дипфейков, автор приходит к следующим выводам. Развитие современной дипфейк-технологии – это, безусловно, новая и малоизученная сфера, требующая наличия соответствующего законодательного регулирования (как в РФ, так и в любом другом государстве). Помимо всего прочего, необходимо также помнить и о том, что контент, создаваемый дипфейком, абсолютно всегда является поддельным, однако его влияние на конкретного человека или общественность может быть вполне реальным, в связи с чем российская система права в общем и целом нуждается в организации принятия определенных мер, направленных на поддержание правомерного оборота использования дипфейков.

Однако вместе с тем принимать излишне радикальные меры, например, такие, как введение в Уголовный кодекс РФ состава преступления за неправомерное использование технологий искусственного интеллекта, не является принципиально верным и оправданным выходом из ситуации, так как конечная цель правового регулирования дипфейков – не запретить их использование в императивном порядке, препятствуя тем самым закономерному развитию достижений технологического прогресса, а принять все возможные превентивные меры для недопущения нарушения прав человека при использовании данной технологии, обеспечив их защиту с точки зрения законодательства Российской Федерации.

Список литературы

1. Bioprinting Medical Devices: Criminal Evaluation Issues / D. V. Kirpichnikov [et al.] // AIP Conference Proceedings: VII International Conference “Safety Problems of Civil Engineering Critical Infrastructures” (SPCECI2021), Yekaterinburg, 2023. Vol. 2701. P. 020032. EDN: STBLEX

2. Motives and Objectives of Crime Commission Against Information Security / A. Yu. Bokovnya [et al.] // Ad Alta. 2020. Vol. 10, № 2 S13. Pp. 7–9. EDN: SCSEBN

3. Бегишев И. Р., Хисамова З. И. Искусственный интеллект и робототехника: глоссарий понятий. М.: Проспект, 2021. 64 с. EDN: HQELSK

4. Бегишев И. Р. Об обороте роботов, их составных частей (модулей) (инициативный проект федерального закона): Препринт № 1 за 2021 г. Казань: Познание, 2021. EDN: FTFKAN.

5. Эксперты рассказали, кто может стать жертвой дипфейков. URL: https://ria.ru/20210814/dipfeyk-1745306675.html (дата обращения: 10.07.2024).

6. Компанию из Гонконга обманули почти на 26 млн долларов. Мошенники применили групповой дипфейк. URL: https://www.bfm.ru/news/543637 (дата обращения: 10.07.2024).

У. И. Зенович,
студент,
Полоцкий государственный университет
имени Евфросинии Полоцкой

ПРАВОВЫЕ И ТЕХНОЛОГИЧЕСКИЕ ОСНОВЫ ЦИФРОВИЗАЦИИ ЗАКОНОДАТЕЛЬНЫХ ОРГАНОВ

Аннотация. В представленной статье поднимается вопрос модернизации парламентов посредством использования новых цифровых технологий. При этом модернизация становится все более распространенным явлением. Рассматриваются различные аспекты внедрения цифровых технологий в деятельность законодательных органов, с критической стороны оценивая ее. Проводzтся анализ и оценка состояния электронного парламентаризма в Республике Беларусь, формулируются выводы и предложения.

Ключевые слова: парламент, цифровизация, трансформация, граждане, право, законодательство, информационно-коммуникационные технологии, информационное общество

LEGAL AND TECHNOLOGICAL BASIS FOR DIGITALIZATION OF LEGISLATIVE BODIES

Abstract. This article raises the issue of modernizing parliaments through the use of new digital technologies. At the same time, modernization is becoming increasingly common. The author examines various aspects of the introduction of digital technologies into the activities of legislative bodies, evaluating it from a critical perspective. An analysis and assessment of the state of electronic parliamentarism in the Republic of Belarus is carried out, conclusions and proposals are formulated.

Keywords: Parliament, digitalization, transformation, citizens, law, legislation, technology, information

Введение. Цифровая трансформация – неизбежный и важный процесс, поскольку технологии внедряются во все аспекты современной жизни, включая деятельность государственных органов. Однако она несет с собой риски и сложности, решение которых требует руководства, управления и значительного планирования.

Основная часть. Цифровая трансформация не является в первую очередь технологически обусловленной; это скорее рефлексивный процесс в состоянии постоянного изменения. Для изучения этой трансформации в основу должны лечь исследования в области управления, анализа дискурса, социологии технологий

и социологии количественной оценки, а также на современные теории демократии. Авторами проводятся многочисленные исследования, посвященные правовому регулированию сквозной цифровой технологии, что является, несомненно, важным шагом [10–13].

На протяжении 2011–2020 гг. происходило активное становление электронного правительства, следствием чего стало внедрение элементов электронного парламентаризма [1. С. 18]. В современный период одной из проблем, волнующих экспертов по управлению и парламентариев, является вопрос о том, как переоснастить парламенты для эпохи после пандемии, как указано в отчете Межпарламентского союза по электронному парламенту за 2020 г. (МПС 2020) [2]. В отчете говорится, что разрушительные потрясения пандемии поставили парламенты перед необходимостью реформирования и ускорения внедрения инновационных цифровых технологий, помещая информационно-коммуникационные технологии в центр повседневной деятельности парламентов.

Внедрение новых информационных систем, развитие функциональных возможностей действующих инфраструктурных элементов электронного правительства в значительной степени упростит информационное взаимодействие между гражданами, бизнесом и государством посредством применения современных цифровых решений, исключая необходимость личного посещения государственных структур и других учреждений. В настоящее время создана государственная система правовой информации, в рамках которой развивается электронная правовая коммуникация между гражданами, бизнесом и государством. Успешно функционирует автоматизированная информационная система, реализующая электронное взаимодействие между субъектами нормотворчества. На ее основе разработана автоматизированная информационная система «Нормотворчество» в целях обеспечения цифровизации процессов взаимодействия государственных органов и организаций на всех стадиях нормотворческой деятельности [4].

Выделим ряд рекомендаций, которые помогут странам, стремящимся перейти на систему электронного парламента, более эффективно и прозрачно обслуживать граждан:

Установка и эксплуатация соответствующих и безопасных цифровых систем (инфраструктуры). Функциональные возможности системы должны позволять депутатам регистрировать свое присутствие; работать и встречаться удаленно; иметь электронный доступ к документам, необходимым для обсуждений (в любое время и в любом месте); голосовать в электронном виде; вести прямую трансляцию заседаний; записывать на видео пленарные заседания; и отслеживать в цифровом виде поправки к законопроектам. Система должна быть связана с электронной библиотекой, платформами взаимодействия с гражданами и государственными системами для облегчения доступа к информации.

Развитие цифровых навыков. Согласно оценке, некоторые депутаты настаивают на использовании бумажных копий вместо электронных документов, а другие сталкиваются с трудностями при использовании предоставленных им устройств. Парламенты должны провести подробную оценку цифровых навыков депутатов, чтобы разработать ориентированную на пользователя и систематиче-

скую программу наращивания потенциала в партнерстве с соответствующими поставщиками образования и обучения для обеспечения устойчивой реализации программы.

Укрепление демократии путем внедрения стратегии использования цифровых технологий для взаимодействия с гражданами. В этой связи парламенты должны разработать стратегию коммуникаций и политику использования социальных сетей депутатами и сотрудниками. Стратегия должна включать инициативы по содействию коммуникации с организациями гражданского общества, религиозными организациями, женщинами, молодежью, маргинализированными группами и средствами массовой информации по вопросам парламентской деятельности с использованием различных цифровых платформ. Цифровые платформы должны включать социальные сети, мобильные приложения, ориентированные на граждан, и, что особенно важно, интерактивный веб-сайт парламента.

Одним из примеров успешной парламентской платформы для вовлечения граждан является Botswana Speaks, веб- и мобильное приложение, которое позволяет гражданам отправлять сообщения напрямую в онлайн-систему с помощью компьютеров, ноутбуков, планшетов и смартфонов [3]. Сообщения автоматически загружаются в трекер и регулярно просматриваются членами парламента для ответов.

В деятельности Национального собрания Республики Беларусь внедрен и используется ряд цифровых технологий. В частности, на сегодняшний день у обеих палат законодательного органа есть свои официальные сайты. Например, на сайте Палаты Представителей можно ознакомиться с законопроектами, поступившими на рассмотрение либо с депутатским корпусом. Создание официальных сайтов государственных органов было предусмотрено в качестве обязательного согласно положениям Указа Президента Республики Беларусь «О мерах по совершенствованию использования национального сегмента сети Интернет» от 1 февраля 2010 г. № 60.

Кроме того, законопроекты вносятся в Палату представителей в порядке реализации права законодательной инициативы на бумажных носителях и одновременно в электронной форме в виде файлов с текстами, соответствующими текстам на бумажных носителях [6].

Как отмечает К. С. Зеленкова, к технологиям для внедрения элементов электронного парламентаризма относятся [7]:

– система электронного голосования;

– портал для доступа граждан к информации о депутатах, политических партиях и законодательном процессе;

– электронная приемная для граждан;

– интернет-портал для коллективной работы депутатов и экспертов;

– система электронного документооборота и электронные архивы;

– система видеофиксации и трансляции парламентских заседаний;

– система видеоконференций;

– система электронных выборов и перевыборов депутатов.

Анализ данного перечня технологий позволяет выделить наиболее перспективные для внедрения в Республике Беларусь. На наш взгляд, таковыми являются

онлайн-выборы, так как в таком виде голосования сможет принять большее количество человек, чем есть в настоящий момент. Такая позиция обусловлена ограниченными физическими способностями людей (лица с инвалидностью), которые не способны самостоятельно передвигаться, электронное голосование поможет им осуществить свое право на свободу голосования, предусмотренное ст. 65 Конституции Республики Беларусь [9].

На наш взгляд, благодаря цифровой трансформации законодательные органы государств смогут получить определенные преимущества в своей деятельности:

Используя цифровые решения, парламенты могут предлагать более персонализированный пользовательский опыт, что приводит к повышению удовлетворенности и доверия.

Улучшенное управление данными: цифровая трансформация предлагает более продвинутые инструменты анализа данных, позволяющие парламентам лучше понимать тенденции, поддерживать более четкое принятие решений и повышать подотчетность.

Более быстрое принятие решений: скорость и последовательность процессов принятия управленческих решений можно улучшить, имея доступ к ключевым показателям и данным.

Повышение экологической устойчивости: многие парламенты продвинулись в своих амбициях стать более устойчивыми за счет модернизации систем и процессов. Например, стратегия, ориентированная на цифровые технологии, сокращает использование бумаги, а удаленная работа и участие в заседаниях могут сократить поездки в парламент и из него.

Сегодня цифровая трансформация стала критически важной для удовлетворения ожиданий современного информационного общества [14].

Заключение. Цифровая трансформация – это путь, который будет выглядеть по-разному в зависимости от парламента. Невозможно предписывать, что должно быть сделано или как это должно быть достигнуто. Однако цифровизированный парламент не до конца оправдывает свое положительное явление, цифровая трансформация, которая влияет на людей так же, как и на технологии, требует тщательного рассмотрения обучения и внедрения пользователей. Новые системы могут означать больше обучения, потребность в высококвалифицированных ресурсах для разработки и проблемы, которые возникают с новыми системами. Немаловажно, что многие люди воспринимают изменения как риск, что вызывает достаточно низкий уровень цифрового доверия. Однако цифровая трансформация набирает обороты, отсюда следует вывод о неизбежном «цифровом прогрессе» в законодательном органе.

Список литературы

1. Харченко О. И. Электронный парламент как стадия развития информационного общества // Вестник Саратовского государственного социально-экономического университета. 2014. № 2. С. 18–20.

2. World e-Parliament Report 2020 [Электронный ресурс]. URL: https://www.ipu.org

3. World Bank Blogs [Электронный ресурс]. URL: https://www.botswanaspeaks.gov.bw

4. О Государственной программе «Цифровое развитие Беларуси» на 2021–2025 годы [Электронный ресурс]: постановление Совета Министров Респ. Беларусь, 2 февраля 2021 г. № 66 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2024.

5. Официальный сайт Палаты представителей [Электронный ресурс]. URL: http://www.house.gov.by

6. О Национальном собрании Республики Беларусь: Закон Республики Беларусь, 8 июля 2008 г., № 370-З (в ред. Закона Респ. Беларусь от 28.06.2024) // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2024.

7. Зеленкова К. С. Деятельность парламента в условиях цифровой трансформации // Современная политическая наука о траекториях развития государства, бизнеса и гражданского общества»: II Международная научно-практическая конференция. 2021.

8. Электронный парламент [Электронный ресурс]. URL: https://www.thenetocrats.ru/tags/elektronnyj_parlament (дата обращения: 03.09.2024).

9. Конституция Республики Беларусь: с изм. и доп., принятыми на респ. Референдуме 27 февраля 2022 года // Национальный правовой интернет-портал Республики Беларусь. Минск: Нац. центр правовой информ. Респ. Беларусь, 2024.

10. Казанцев Д. А. Авторские права на результаты деятельности искусственного интеллекта и способы их защиты // Journal of Digital Technologies and Law. 2023. Т. 1, № 4. С. 909–931. EDN: PHBNKI

11. Шумакова Н. И., Ллойд Д. Д., Титова Е. В. На пути к правовому регулированию генеративного ИИ в творческой индустрии // Journal of Digital Technologies and Law. 2023. Т. 1, № 4. С. 880–908. EDN: WXWSVU

12. Айна-Пелемо А. Д., Басси И., Акподжаро Г. О. Меры профилактики нарушений авторских прав на создание контента в цифровой среде: опыт Нигерии // Journal of Digital Technologies and Law. 2024. Т. 2, № 2. С. 408–429. EDN: HIQZUJ

13. Галиндо Аюда Ф. Алгоритмы, социология права и правосудие // Journal of Digital Technologies and Law. 2024. Т. 2, № 1. С. 34–45. EDN: UUNZFP

14. Залоило М. В. Постиндустриальная культура правотворчества: новый образ реальности // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 4(92). С. 65–73.

П. А. Иллюк,
аспирант,
Институт законодательства и сравнительного правоведения
при Правительстве Российской Федерации

ИСТОРИЯ РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ВЬЕТНАМА И ШРИ-ЛАНКИ

Аннотация. Во Вьетнаме разработка законов о конфиденциальности данных началась с 2005 г. В 2018 г. был принят Закон о кибербезопасности для защиты национальной безопасности и общественного порядка в киберпространстве. До 17 апреля 2023 г. во Вьетнаме существовала разрозненная правовая база для защиты персональных данных. Принятый в 2023 Декрет № 13/2023 о защите персональных данных значительно улучшает правовую базу Вьетнама по защите персональных данных, устраняя пробелы в определениях и усиливая гарантии от несанкционированного доступа и неправомерного использования. В Шри-Ланке первые версии законопроекта о защите персональных данных были приняты в 2019 г., включая версию, которая охватывала государственный и частный секторы. Закон о защите персональных данных № 9 от 2022 г. направлен на заполнение пробелов в режиме защиты данных, в нем закреплены шесть принципов обработки персональных данных, включая законность, справедливость и прозрачность. Данный закон стал первым всеобъемлющим законодательством о защите данных в Южной Азии.

Ключевые слова: цифровизация, вьетнамское право, защита персональных данных, источники права, цифровое право, право Шри-Ланки

THE HISTORY OF THE DEVELOPMENT OF LEGISLATION ON THE PROTECTION OF PERSONAL DATA OF VIETNAM AND SRI LANKA

Abstract. In Vietnam, the development of data privacy laws began in 2005. In 2018, the Cybersecurity Law was passed to protect national security and public order in cyberspace. Until 17 April 2023, Vietnam had a fragmented legal framework for the protection of personal data. Decree No. 13/2023 on the Protection of Personal Data, passed in 2023, significantly improves Vietnam's legal framework for the protection of personal data by addressing definitional gaps and strengthening safeguards against unauthorized access and misuse. In Sri Lanka, the first versions of the Personal Data Protection Bill were released in 2019, including a version that covered the public and private sectors. The Personal Data Protection Law No. 9 of 2022 aims to fill the gaps in the data protection regime by enshrining six principles for the processing of personal data, including lawfulness, fairness, and transparency. The Act became the first comprehensive data protection legislation in South Asia.

Keywords: digitalization, Vietnamese law, personal data protection, sources of law, digital law, Sri Lankan law

Введение. Защита персональных данных становится все более актуальной во всем мире. Одним из подтверждений актуальности данной проблемы выступает резолюция ООН, в которой говорится, «что Интернет стал неотъемлемым инструментом реализации прав человека, борьбы с неравенством и развития прогресса, но вместе с тем может происходить нарушение авторских прав, кибератаки с целью завладения данными и т. д.» [2. С. 20]. Страны Азии в данном вопросе не являются исключением.

Вьетнам. В Социалистической Республике Вьетнам персональные данные, как правило, защищаются с помощью режима права на неприкосновенность частной жизни. В Конституциях Вьетнама 1959, 1980, 1992 и 2013 гг. право на неприкосновенность частной жизни признавалось и закреплялось. Например, в ст. 21. Конституции Вьетнама 2013 г. закреплено, что каждый человек имеет «неприкосновенное» право на неприкосновенность частной жизни, которое включает в себя личные тайны, семейные тайны, тайны переписки, телефонных звонков, телеграм и другие формы обмена частной информацией [9. С. 4]. Однако, согласно заявлению директора Департамента кибербезопасности и предупреждения преступности и использования высоких технологий Министерства общественной безопасности, за недавнее время во Вьетнаме был выявлен широкий круг лиц, замешанных в продаже персональных данных [4. С. 576–577], что свидетельствует об актуальности вопроса защиты персональных данных.

Закон об электронных транзакциях 2005 г. содержал краткое общее заявление о праве человека давать согласие на использование его личной информации в электронной коммерции [12. С. 368]. Следом за Законом об электронных транзакциях 2005 г. был принят Закон об информационных технологиях 2006 г., принятый для развития информационных технологий во Вьетнаме. В данном Законе в ст. 21 и 22 впервые были закреплены обязательства организаций и отдельных лиц, которые собирают, обрабатывают и используют персональную информацию. К этим обязательствам были отнесены:

– информирование отдельных лиц о форме, объеме, месте и цели использования данных;

– использование информации только в надлежащих целях;

– хранение ее в течение установленного законом периода или по согласованию;

– принятие мер для предотвращения потери, кражи, раскрытия, изменения или уничтожения данных [11. С. 16].

После принятия Закона о детях в 2016 г. был издан Декрет № 56/2017/ND-CP, в котором содержатся положения, определяющие «частную личную информацию, касающуюся детей» и описывающие меры по защите конфиденциальности такой информации в онлайн-домене [8. С. 8–9].

В 2018 г. был принят Закон о кибербезопасности для решения проблем в киберпространстве, защиты национальной безопасности и обеспечения общественного порядка и безопасности в киберпространстве. Как и в Законе об информационных технологиях 2006 г. и в Гражданском кодексе 2018 г. в данном Законе в ст. 17 законодателем используются термины «частная жизнь» и «личная тайна». Закон касается изъятия, покупки, хранения или раскрытия личных данных, затрагивающих честь, достоинство и права лиц, а также изменения или повреждения такой

информации [11. С. 16–17]. В ст. 29 данного Закона содержатся положения, касающиеся права детей на защиту личных секретов и частной жизни в киберпространстве. Стороны, предоставляющие услуги в киберпространстве, несут ответственность за обеспечение того, чтобы информация в их системах или услугах не наносила вреда детям и не нарушала права детей [8. С. 9].

До 17 апреля 2023 г. во Вьетнаме существовала разрозненная правовая база для регулирования защиты персональных данных, как и не было определения понятия «персональные данные». Использовался ряд схожих терминов, относящихся к «персональным данным», таких как «частная информация», «персональная информация», «персональная информация в Интернете» или «цифровая информация» и т. д. Однако Декрет № 52 (2013 г.) определяет «персональную информацию» как «информацию, способствующую идентификации конкретного лица, включая его имя, возраст, домашний адрес, номер телефона, медицинскую информацию, номер счета, информацию о личных платежных операциях и другую информацию, которую лицо хотело бы сохранить в тайне», но «не включает в себя служебную контактную информацию и другую информацию… опубликованную в средствах массовой информации» [9. С. 6]. Осознавая необходимость более согласованного подхода, правительство Вьетнама 9 февраля 2021 г. опубликовало проект, который претерпел несколько изменений до официального обнародования Декрета о защите персональных данных [10. С. 5–10].

Декрет № 13/2023 впервые во вьетнамском законодательстве определяет персональные данные как «информацию в виде символов, письма, чисел, изображений, звука или аналогичного в электронной среде, связанную с конкретным лицом или помогающую идентифицировать конкретное лицо». Согласно Декрету № 13/2023, обработка персональных данных требует согласия субъекта данных.

1 июля 2023 г. Вьетнам принял Декрет о защите персональных данных, представляющий собой важнейшее событие в системе защиты данных страны. Данный Декрет, который разрабатывался путем широких публичных консультаций и поправок в течение пяти месяцев, считается важной вехой в создании режима защиты данных во Вьетнаме, которого ранее не существовало. Его примечательные особенности включают расширенное определение данных, применимость как к внутренним, так и к международным организациям, подробный перечень конфиденциальных персональных данных и особые меры защиты несовершеннолетних [9. С. 97–99]. Однако во Вьетнаме указы подчинены законам и содержат подробные инструкции по их реализации. Роль Указа № 13/2023 ограничена его иерархическим положением, и фрагментированное состояние защиты ПД сохранится, если не будут решены вопросы согласования между правовыми документами [11. С. 17–20]. По мнению вьетнамских исследователей данных, «Декрет является основополагающим шагом на пути к будущему законодательству и направлен на консолидацию существующих законов и нормативных актов в комплексную и единую структуру для защиты данных физических лиц» [10. С. 5–10].

Шри-Ланка. Еще в 1996 г. правительство Шри-Ланки предприняло первые меры по защите персональных данных, издав Закон о телекоммуникациях от 1996 г., в котором незаконный перехват данных был впервые признан правонарушением в Шри-Ланке. Следующей мерой стало издание Закона о компьютерных преступлениях от 2007 г. однако закон подвергся критике, так как защита, обеспечиваемая

в соответствии с данным Законом, недостаточна для противодействия всем современным угрозам киберпространства [6. С. 64].

В этой версии был предусмотрен Орган по защите данных (ст. 19). В законопроекте предусматривались «особые персональные данные», к которым в том числе относились генетические и биометрические данные (ст. 46).

К персональным данным законотворцы не относили данные для личного, «бытового использования» и анонимные данные («необратимо анонимизированные таким образом, что личность становится неидентифицируемой»). В соответствии с версией от сентября 2019 г. (ст. 25) государственные органы могут обрабатывать персональные данные только в Шри-Ланке, если соответствующий надзорный орган не классифицируют данные как разрешенные для обработки за границей. Права субъектов данных в ч. II, включают в себя такие понятия, как «право на забвение» и «право на удаление» (в данном случае это подвид права на забвение) [12. С. 2–4].

Третий вариант законопроекта о защите персональных данных Шри-Ланки был выпущен в июле 2021 г. Министерством цифровой инфраструктуры и информационных технологий. Проект был утвержден Генеральным прокурором как конституционный, и Министерство цифровой инфраструктуры и информационных технологий присвоило ему приоритетный статус. В окончательном проекте предусматривалось, что каждый контролер, если он не освобожден от действия настоящего Закона, обязан назначить сотрудника по защите данных для обеспечения соблюдения требований законодательства [7. С. 107–108].

В соответствии с Разделом II контролеры данных обязаны исправлять или дополнять неточные или неполные данные. Кроме того, право на стирание также гарантируется ст. 16 Закона при определенных обстоятельствах. Еще одна важная функциональность органа по защите данных заключается в том, что он может издавать директивы для субъектов, которые не соблюдают положения предлагаемого закона и могут налагать административные взыскания.

Несмотря на вышеупомянутые сильные стороны Закона о защите персональных данных, некоторые его критики ставят под сомнение эффективность его положений. Основная критика Закона касается его расплывчатых определений. Утверждается, что эта правовая неопределенность может препятствовать притоку иностранных инвестиций в страну. Помимо этого, Закон не содержит положения, облегчающего данные передачи с согласия пользователей [16. С. 108.]. Мы предполагаем, что, как и в случае законодательства в сфере защиты персональных данных в КНР, в которой «неточность текстов регулирующих документов зачастую связана не с низким уровнем юридической техники, а с желанием правоприменителя использовать норму по своему усмотрению» [3. С. 319].

Заключение. Во Вьетнаме были приняты Закон об электронных транзакциях 2005 г., Закон об информационных технологиях 2006 г. Принятый в 2023 г. Декрет № 13/2023 о защите персональных данных значительно улучшает правовую базу Вьетнама по защите персональных данных, устраняя пробелы в определениях и усиливая гарантии от несанкционированного доступа и неправомерного использования. Однако во Вьетнаме указы подчинены законам и содержат подробные инструкции по их реализации. Роль Указа № 13/2023 ограничена его иерархи-

ческим положением, и фрагментированное состояние защиты персональных данных сохранится, если не будут решены вопросы согласования между правовыми документами.

В Шри-Ланке первые версии законопроекта о защите персональных данных были изданы в 2019 г., включая версию, которая охватывала государственный и частный секторы. В июле 2021 г. был выпущен третий вариант законопроекта, который был утвержден как конституционный и получил приоритетный статус. 8 марта 2022 г. Шри-Ланка приняла Закон о защите персональных данных № 9 от 2022 г., став тем самым первой страной Южной Азии, установив шесть принципов обработки персональных данных, включая законность, справедливость и прозрачность.

Список литературы

1. Во К. З. Понятие, признаки и организационно-правовые формы юридических лиц как участников уголовно-процессуальных отношений (сравнительно-правовой анализ по законодательству России и Вьетнама) / К. З. Во, Д. А. Иванов // Симбирский научный вестник. 2020. № 1–2(39–40). С. 105–109. – EDN FRPRHB.

2. Пашенцев, Д. А. Концепция цифрового государства и цифровой правовой среды: монография / под общ. ред. Н. Н. Черногора, Д. А. Пашенцева. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: Норма: ИНФРА-М, 2024. 244 с.

3. Трощинский П. В., Молотников А. Е. Особенности нормативно-правового регулирования цифровой экономики и цифровых технологий в Китае // Правоведение. 2019. Т. 63, № 2. С. 309–326.

4. Хан Ф. Н. Об обеспечении безопасности личности в киберпространстве во Вьетнаме // Вопросы российской юстиции. 2024. № 30. С. 571–581.

5. Bach T. N. N. Addressing the Challenges of Data Privacy Protection Law in Vietnam // VNU Journal of Science: Legal Studies. 2023. Vol. 39, № 1.

6. Balendra S., Emerging Challenges in Regulating E-Commerce: The Sri Lankan Context // KDU Law Journal. 2022. Vol. 02, Iss. II, September. Pp. 55–76.

7. Bentototahewa V. A Framework for Acceptance and Implementation of Global Data Privacy and Security Policies by States (A Case Study of Sri Lanka and United Kingdom). Cardiff Metropolitan University, 2021.

8. Dang M. T., Doan T. A. Children's Data Protection in Vietnam: Legal Framework and Challenges // Journal of Law and Sustainable Development. 2023. Vol. 11, № 12. Pp. e2675-e2675.

9. Dao K. T. Harmonizing vietnamese personal data protection law with Asean standards: lessons learned from the singaporean // ADM. 2025. Pp. 24–25.

10. Ha H. T., Van Vu T. Potential conflicts in personal data protection under current legislation in Vietnam compared with European general data protection regulation. https://ajee-journal.com/upload/attaches/att_1724712710.pdf

11. Hang N. H. B. Addressing Fragmentation in Vietnam's Data Protection Laws: Recommendations for a Unified Legal Framework // Vietnamese Journal of Legal Sciences. 2024. Vol. 11, № 2. Pp. 14–26.

12. Greenleaf G. Asian data privacy laws: trade & human rights perspectives. OUP Oxford, 2014.

13. Greenleaf, Graham, Advances in South Asian Data Privacy Laws: Sri Lanka, Pakistan and Nepal (December 1, 2019) // Privacy Laws & Business International Report. 2019. Pp. 22–25.

14. Greenleaf, Graham, Pakistan and Sri Lanka's Data Privacy Bills Move Forward (September 20, 2021) // Privacy Laws & Business International Report. 2021. № 173. Pp. 24–27.

15. Rajapakse RLW. Personal Data Protection in the Context of Employment: A Discussion of Law in Sri Lanka in the Light of the GDPR. URL: http://ir.kdu.ac.lk/handle/345/4511

16. Sachintha S. A Critical Analysis on the Adequacy of the Existing Legal Framework for Safeguarding E-Consumer Rights in Sri Lanka // KDU Law Journal. 2022. Vol. 02, Iss. II, September. Pp. 107–117.

17. Thusitha B. Abeysekara, Amali E. Ranasinghe, Holistic Approach in Introducing Proper Legal Framework to Regulate Data Protection and Privacy in Sri Lanka // Vidyodaya Journal of Management. 2022. Vol. 8(I). Pp. 169–200.

С. А. Израилова,
студент,
Саратовский государственный университет имени Н. Г. Чернышевского
В. С. Салогорова,
студент,
Саратовский государственный университет имени Н. Г. Чернышевского

О НЕОБХОДИМОСТИ ТРАНСФОРМАЦИИ НАВЫКОВ ДОЛЖНОСТНЫХ ЛИЦ ТАМОЖЕННЫХ ОРГАНОВ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. Данное исследование посвящено необходимости формирования у должностных лиц таможенных органов ключевых навыков, которые будут способствовать обеспечивать слаженное функционирование таможенных органов в современных условиях цифровизации. Выделены ключевые аспекты цифровизации таможенной деятельности. Кроме того, для их реализации приведены некоторые аспекты, способствующие адаптации и трансформации уже имеющихся профессиональных навыков у должностных лиц таможенных органов.

Ключевые слова: цифровизация, таможенная деятельность, должностные лица таможенных органов, навыки, обучение, профессиональная деятельность, информационные технологии

ON THE NEED TO TRANSFORM THE SKILLS OF CUSTOMS OFFICIALS IN THE CONTEXT OF DIGITALIZATION

Abstract. This study is devoted to the need to develop key skills among customs officials that will help ensure the smooth functioning of customs authorities in the modern conditions of digitalization. Key aspects of digitalization of customs activities are highlighted. In addition, for their implementation, some aspects are given that contribute to the adaptation and transformation of existing professional skills among customs officials.

Keywords: digitalization, customs activities, customs officials, skills, training, professional activity, information technology

Введение. Цифровизация таможенной деятельности становится ключевым направлением в условиях глобализации и технологического прогресса. Этот процесс включает автоматизацию процедур, что позволяет ускорить обработку грузов и минимизировать ошибки. Искусственный интеллект помогает анализировать данные и выявлять риски, повышая уровень контроля и безопасности на границе [1, 2]. Использование блокчейна обеспечивает надежность сделок, позволяя участникам взаимодействовать на основе единой информации. Интеграция систем облегчает обмен данными между таможней и другими госорганами, улучшая оперативность решений. Оптимизация регуляторных процессов упрощает правила и снижает бюрократические преграды. Важно также обучение специалистов для эффективного использования современных инструментов и обеспечение кибербезопасности данных [3]. Адаптация законодательства и синхронизация с международными стандартами способствуют устойчивому развитию глобальной торговли [4].

Основная часть. Ключевые аспекты цифровизации включают:

1. Вызовы цифровизации: киберугрозы, недостаточная защита данных и неразрешенные правовые вопросы в этой сфере могут затруднить процесс трансформации.

2. Инновационные технологии: автоматизированные системы играют значительную роль в ускорении процессов декларирования. Они минимизируют человеческий фактор и уменьшают количество ошибок. Искусственный интеллект позволяет обрабатывать большие объемы информации, предсказывая возможные риски и упрощая выявление нарушений. Блокчейн-технологии, благодаря своей прозрачной и децентрализованной природе, повышают доверие к информации, используемой в цепочке поставок.

3. Оптимизация процессов: цифровизация позволяет сократить время обработки документов и упрощает взаимодействие между различными участниками внешнеэкономической деятельности. Эффективные электронные платформы позволяют всем участникам оперативно обмениваться данными, что снижает время ожидания и ускоряет таможенные процедуры.

4. Юридические аспекты: для успешного внедрения цифровых технологий требуется соответствующая законодательная база. Необходимы новые регулятивы, учитывающие специфику цифровизации и защищающие права как бизнеса, так и потребителей.

5. Взаимодействие между государственными органами и бизнесом: эффективная цифровизация требует плотного сотрудничества между государственными органами и частным сектором. Создание совместных рабочих групп, обмен опытом и лучшими практиками поможет ускорить внедрение новых технологий и сделать процессы более эффективными.

Следует выделить следующие ключевые аспекты профессиональной подготовки должностных лиц таможенных органов:

Обеспечение цифровых навыков, таких как компьютерная грамотность, свободное владение компьютерной техникой, знание программных продуктов, используемых в таможенном деле, работа с различными типами файлов, безопасность в Сети. Использование специализированных программных комплексов невозможно без прохождения обучения работе с автоматизированными системами декларирования, электронного документооборота, информационными базами данных, системами управления рисками. В современных условиях должностным лицам таможенных органов необходимо знание основ баз данных, сетевых технологий, систем информационной безопасности, общих принципов функционирования информационных систем в таможне.

Новые инструменты и технологии требуют обучение работников взаимодействию с системами, использующими искусственный интеллект (ИИ) для анализа данных, выявления рисков, автоматизации рутинных задач, прогнозирования и предоставления рекомендаций.

Коммуникационные навыки, такие как развитие навыков письменной и устной коммуникации в электронном формате, владение современными инструментами коммуникации (видеоконференции, чат-боты, электронная почта).

Взаимодействие с участниками внешнеэкономической деятельности требует понимания особенностей взаимодействия с представителями бизнеса в цифровой среде, способность эффективно объяснять процедуры и требования таможни.

Работа в команде: развитие навыков совместной работы в цифровой среде, использование современных инструментов для обмена информацией и координации действий.

Непрерывное обучение: постоянное повышение квалификации, прохождение курсов и тренингов по использованию новых технологий и инструментов, знакомство с изменениями в таможенном законодательстве и практике применения цифровых технологий.

Самостоятельное обучение: развитие навыков самостоятельного поиска информации, анализа и применения новых знаний на практике.

Участие в конференциях, семинарах, вебинарах: получение новых знаний и практического опыта от лидеров отрасли и специалистов в области цифровых технологий в таможенном деле.

На основе изложенного материала можно сделать следующие выводы:

– цифровая трансформация таможенной системы не только существенно улучшает административные процессы, но и открывает новые горизонты для повышения уровня безопасности и сокращения коррупционных рисков;

– применение современных цифровых технологий, таких как искусственный интеллект и блокчейн, позволяет значительно упростить контроль за перемещением товаров и реальным временем отслеживания данных.

Тем не менее успешное внедрение цифровых решений требует комплексного подхода. Обучение кадров играет ключевую роль, так как без квалифицированных специалистов невозможно эффективно использовать новые системы. Обеспечение кибербезопасности также является критически важным, чтобы защитить данные от потенциальных киберугроз.

Роль человеческого фактора в цифровой таможне является ключевой для успешной реализации и функционирования автоматизированных систем. Несмотря на значительное развитие технологий и внедрение цифровых решений, эффективность таможенных процедур напрямую зависит от квалификации, адаптивности и готовности персонала к изменениям.

Человеческий фактор влияет на многие аспекты работы, включая принятие решений в нестандартных ситуациях, взаимодействие с новыми технологиями и коммуникацию внутри команд. Важно, чтобы специалисты обладали необходимыми знаниями и навыками, а также были вовлечены в процесс цифровой трансформации.

Заключение. Обучение и развитие навыков сотрудников – это неотъемлемая часть стратегии цифровизации таможенных органов, что способствует повышению доверия к системам и улучшению общего качества обслуживания. Следовательно, инвестиции в человеческий капитал становятся критически важными для достижения долгосрочных целей и повышения конкурентоспособности таможенных служб в условиях глобализации. Таким образом, баланс между технологическими решениями и человеческим потенциалом определяет успех перехода к современной, цифровой таможне.

Список литературы

1. Михайлова А. В. Цифровая экономика: вызовы и возможности. М.: Научное издательство. Глава 1. 2021. С. 7–16.

2. Плетухина А. А., Хвостова И. П., Степанова Е. П. Повышение уровня информационного обеспечения деятельности юриста // Вестн. Северо-Кавказского федерал. ун-та. 2014. № 6. С. 68–72

3. Motives and Objectives of Crime Commission Against Information Security / A. Yu. Bokovnya [et al.] // Ad Alta. 2020. Vol. 10, No. 2 S13. Pp. 7–9. EDN: SCSEBN

4. Смирнова Н. И. Психология взаимодействия персонала и технологий в таможенных органах. Санкт-Петербург: Наука, 2021. С. 26–40.

А. В. Козлов,
студент,
Российский университет дружбы народов имени Патриса Лумумбы

ИСПОЛЬЗОВАНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ В ГРАЖДАНСКОМ ПРАВЕ: ПРАВОВОЕ ОБЕСПЕЧЕНИЕ И ЗАЩИТА ИНТЕРЕСОВ УЧАСТНИКОВ

Аннотация. В данной работе рассматриваются правовые аспекты использования блокчейна, особенности его создания и регулирования, а также потенциал для повышения прозрачности и уменьшения мошенничества в гражданском обороте. Основное внимание уделено тому, как происходило развитие блокчейн-технологий, а также как блокчейн может поддерживать правовые отношения, обеспечивать безопасность данных и подтверждать обязательства сторон.

Ключевые слова: блокчейн, гражданское право, правовое обеспечение, защита интересов, прозрачность, мошенничество, цифровые обязательства, регулирование

USE OF BLOCKCHAIN TECHNOLOGIES IN CIVIL LAW: LEGAL SUPPORT AND PROTECTION OF PARTICIPANTS' INTERESTS

Abstract. This paper examines the legal aspects of blockchain use, the specifics of its creation and regulation, and its potential to increase transparency and reduce fraud in civil turnover. The focus is on how blockchain technology has evolved and how blockchain can support legal relationships, ensure data security, and confirm the obligations of parties.

Keywords: blockchain, civil law, legal support, interest protection, transparency, fraud, digital obligations, regulation

Современные блокчейн-технологии имеют достаточно серьезный путь развития, начавшийся с концептуальных основ, предложенных в 1991 году. Тогда была предложена Концепция блокчейна Стюартом Хабером и У. Скоттом Стормом. Они разработали систему, которая использовала метки времени для цифровых документов, чтобы предотвратить их подделку и изменение даты [2]. При дальнейшем развитии в 2008 году появляется первая децентрализованная одноранговая (P2P) система электронных денежных средств, известной как «биткоин», разработанной Сатоши Накамото. Это событие стало поворотным моментом, так как блокчейн начал рассматриваться как основа для криптовалют. И уже в 2010-е годы блокчейн начинает активно исследоваться и применяться в различных сферах, помимо финансов. Появляются новые криптовалюты и платформы, такие как Ethereum, которые вводят концепцию смарт-контрактов, позволяя автоматизировать выполнение соглашений. На сегодняшний день блокчейн находит применение в государственных и муниципальных управленческих предложениях, включая регистрацию сделок с недвижимостью, онлайн-голосование и другие сферы. Примеры успешного использования технологии в России включают общероссийское голосование по поправкам в Конституцию и проекты ФНС России. Отчетливо видно, как блокчейн прошел путь от теоретической концепции до практического инструмента, используемого в различных областях, включая государственное управление, финансы и другие сферы.

Рассматривая более подробно такое явление, как смарт-контракты, можно выделить несколько преимуществ, которые находят свое отражение в государственном управлении. Так одним из основных явлений выступает автоматизация процессов, при которых смарт-контракты позволяют роботизировать выполнение и контроль за исполнением юридически значимых действий, что снижает необходимость в ручном управлении и минимизирует ошибки. И как основной итог – это снижение затрат, так как при условии автоматизации и упрощения процессов приведет к снижению административных ресурсов, направленных на поддержание различных государственных функций. Все это делает смарт-контракты важным инструментом для цифровой трансформации государственного управления [1, 3, 4, 5–9].

Использование блокчейн-технологий в гражданском праве открывает новые горизонты для правового обеспечения и защиты интересов участников договорных отношений, в том числе для государственных взаимоотношений. Инновационные свойства блокчейна, такие как децентрализация, неизменяемость данных и возможность автоматизации процессов через смарт-контракты, значительно улучшают уровень доверия между сторонами и снижают риски недобросовестности и коррупциогенности контрагента. Однако, несмотря на все преимущества, необходимо учитывать и существующие угрозы, связанные с правом, такие как проблемы с законодательным регулированием, защитой прав потребителей, в том числе и государственного заказчика, а также соблюдением стандартов конфиденциальности. Важно, чтобы законодательство адаптировалось к новым технологиям и обеспечивало правовую основу для безопасного и эффективного использования блокчейна.

Список литературы

1. Арсланов К. М. О правовом регламентировании блок-чейн-отношений // Вестник СГЮА. 2019. № 6 (131).

2. Васильева Т. В., Кудрявцева Л. В. К проблеме правового регулирования блокчейн технологий // Право и практика. 2024. № 2.

3. Motives and Objectives of Crime Commission Against Information Security / A. Yu. Bokovnya [et al.] // Ad Alta. 2020. Vol. 10, № 2 S13. Pp. 7–9. EDN: SCSEBN

4. Хубиев А. Р. К вопросу о потенциале искусственного интеллекта, генеративного искусственного интеллекта и технологии блокчейн в гражданском процессе // Государственная служба и кадры. 2024. № 2.

5. Концепция цифрового государства и цифровой правовой среды: монография. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: Норма: ИНФРА-М, 2024.

6. Ауду П. Ф., Шабих Ф Применение смарт-контрактов в сфере международной торговли и перспективы дальнейшей эволюции Инкотермс // Journal of Digital Technologies and Law. 2024. Т. 2, № 2. С. 308–327. EDN: ZKUAGZ

7. Варбанова Г. Правовая природа смарт-контрактов: договор или программный код? // Journal of Digital Technologies and Law. 2023. Т. 1, № 4. С. 1028–1041. EDN: IGAZIZ

8. Ламаппулаге Донн Т. Д. Смарт-контракты в международной торговле: европейские правовые стратегии преодоления трудностей // Journal of Digital Technologies and Law. 2023. Т. 1, № 4. С. 1042–1057. EDN: GVBWBI

9. Болатбеккызы Г. Правовые проблемы трансграничной передачи данных в эпоху цифровизации государственного управления // Journal of Digital Technologies and Law. 2024. Т. 2, № 2. С. 286–307. EDN: PPLJHU

А. О. Кулажина,
магистрант,
Финансовый университет
при Правительстве Российской Федерации

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ИНСТРУМЕНТ РАЗВИТИЯ КОРПОРАТИВНОЙ СОЦИАЛЬНОЙ ОТВЕТСТВЕННОСТИ

Аннотация. Научная статья посвящена анализу потенциального влияния искусственного интеллекта на развитие корпоративной социальной ответственности в условиях глобализации. В работе рассмотрен вопрос о принятии высокотехнологичных решений в области устойчивого развития в компаниях с помощью инновационных технологий, перечислены риски, связанные с принятием решений в области устойчивого развития в контексте использования искусственного интеллекта, приведены подходы к возможному внедрению правового регулирования в использования искусственного интеллекта компаниями.

Ключевые слова: искусственный интеллект, корпоративная социальная ответственность, корпоративное управление, глобализация, стандарты отчетности

ARTIFICIAL INTELLIGENCE AS A TOOL FOR THE DEVELOPMENT OF CORPORATE SOCIAL RESPONSIBILITY

Abstract. The scientific article is devoted to the analysis of the potential impact of artificial intelligence on the development of corporate social responsibility in the context of globalization. The paper considers the issue of making high-tech decisions in the field of sustainable development in companies using innovative technologies, lists the risks associated with decision-making in the field of sustainable development in the context of the use of artificial intelligence, and provides approaches to the possible introduction of legal regulation in the use of artificial intelligence by companies.

Keywords: artificial intelligence, corporate social responsibility, corporate governance, globalization, reporting standards

Введение. При решении задач устойчивого развития компаний искусственный интеллект – противоречивый инструмент. Искусственный интеллект может значительно улучшить решение сложных экологических и социальных проблем. С другой стороны, инновации могут также привести к новым рискам, таким как системные ошибки и проблемы с этикой. В связи с этим в работе рассмотрена необходимость решения проблем устойчивого развития и устранения рисков, связанных с искусственным интеллектом в контексте повышения корпоративной социальной ответственности. Это может быть достигнуто проработкой нормативно-правовой базы, улучшением корпоративной политики и требованиям к отчетности.

Основная часть. Организация экономического сотрудничества и развития (далее – ОЭСР) определяет искусственный интеллект (далее – ИИ) как «технологию общего назначения, которая обладает потенциалом для улучшения благосо-

стояния людей, содействия позитивной устойчивой глобальной экономической деятельности, повышения инноваций и производительности, а также для оказания помощи в реагировании на глобальные вызовы» [7]. Европейская комиссия полагает, что ИИ относится к «системам, которые демонстрируют разумное поведение, анализируя окружающую среду, предпринимая действия с определенной степенью автономии для достижения конкретных целей» [11. С. 359–385].

Искусственный интеллект возник в результате воспроизведения человеческого разума через компьютер. ИИ становится все более распространенным в повседневной жизни. Настоящая эпоха глобализации представляет собой время ИИ и когнитивных технологий. Машинное обучение как подотрасль искусственного интеллекта используется для радикального изменения и совершенствования предпринимательства в целях содействия устойчивому развитию. По мнению профессора Д. Чжао, ИИ может автоматически обучаться и приобретать знания на основе больших объемов данных и использовать их для помощи людям в достижении их практических и технических целей [22].

ИИ – это многогранный инструмент. У применения ИИ есть свои преимущества. Например, связанные с большими данными, ценностью для предпринимательства за счет скорости и автоматизации. В то же время организации и частные лица столкнутся с проблемой, которую С. Порро, Л. К. Бирс обозначили следующим образом: «Избыток данных и неуверенности в том, что с ними делать» [19]. В корпоративной среде, по мнению А. Накви, ИИ может применяться для повышения эффективности программ корпоративной социальной ответственности (далее – КСО) [17. P. 66]. Компании и другие заинтересованные лица будут пользоваться преимуществами искусственного интеллекта, так как он принесет много выгоды с точки зрения экономической ценности и принятия новых решений, способствующих повышению устойчивости компаний к социальным вызовам. Однако важно изучить потенциальную опасность, создаваемую ИИ, и проблемы, связанные с этой технологией, чтобы применение ИИ могло быть согласовано с общепринятыми гуманными ценностями и убеждениями [24].

Несмотря на то, что применение ИИ для обеспечения устойчивого развития находится на ранней стадии, эта тенденция уже начинает влиять на корпоративную устойчивость в аспекте применения ИИ для достижения целей устойчивого развития. Например, для сокращения выбросов CO2 или применение машинного обучения для улучшения продукции садоводства [20]. Применение искусственного интеллекта на благо граждан и окружающей среды включает в себя формальные и неформальные механизмы повышения осведомленности о практике КСО, стандартизации и внедрении. Применение ИИ должно соответствовать этике, подкреплено нормативной базой, чтобы обеспечить его устойчивое развитие [21. Pp. 1–10]. Невыполнение этого требования может привести к тому, что применение ИИ будет противоречить закону и этическим нормам [23]. Внедрение ИИ также может приводить к негативным последствиям, таким как нарушение конфиденциальности и системные ошибки. Организации должны анализировать данные от ИИ, совершать этичные действия. Использование нормативной базы – решение для достижения более социально ответственного искусственного интеллекта пу-

тем мониторинга и снижения связанных с ним рисков. Так, ИИ может оказать более широкое влияние на многие секторы, что уже продемонстрировано его влиянием на достижение целей устойчивого развития.

В идеале компании и пользователи ИИ полагают, что работа ИИ будет более прозрачной, логичной, этичной. А также он будет в достаточной мере обученным, имеющим необходимые данные и без ошибок в системе.

При принятии бизнес-решений эти моменты воплощаются в вопросах, касающихся ИИ и деловой этики, стратегического управления, политики в отношении заинтересованных сторон и КСО. Эффективное корпоративное управление основано на внедрении принципов взаимодействия, участия и тщательного контроля заинтересованных сторон в процесс принятия решений. Использование ИИ может укрепить эти принципы. Интеграция ИИ и корпоративных решений осуществляется в двух направлениях, включая «ИИ для устойчивого развития» и «Устойчивость ИИ». Что касается первого направления, то компании, применяющие ИИ, полностью интегрируют этические нормы и подотчетный ИИ. По мнению К. Дарно, Т. Парколе, М. Моршид, «отсутствие правовой системы, регулирующей применение и разработку ИИ, может привести к росту частной стандартизации, поскольку добровольная стандартизация ИИ обеспечивает устойчивое формирование будущей правовой базы» [15]. Касательно второго направления, ИИ и большие данные помогут компаниям внедрить эффективные принципы корпоративного управления, такие как подотчетность, прозрачность и сотрудничество с заинтересованными сторонами. Кроме того, ИИ поможет создать системы управления, которые эффективно снижают риски КСО для достижения экономической и социальной выгоды на основе больших данных.

В зарубежной и отечественной литературе отсутствует единое мнение о том, изменит ли ИИ текущую практику предпринимательской деятельности или даже основы корпораций и как это произойдет, начиная от подходов, предусматривающих новую парадигму автономных корпораций, и заканчивая другими, утверждающими, что существенных изменений не произойдет. Петрин М. Петрин утверждает, что ИИ сократит потребность в человеческом управлении и связанные с ним затраты, повысив точность и эффективность корпоративных действий [18. Pp. 965–1030]. М. Банкевиц, С. Берг, С. Тейхерт полагают, что руководство компании превратится в «виртуальные сети людей» или будет полностью заменено решениями на основе ИИ под влиянием цифровизации [12. Pp. 58–64]. Однако другие исследователи по-прежнему скептически относятся к способности технологий изменить фундаментальные нормативные вопросы предпринимательства и уменьшить потребность в человеческом участии в управлении бизнесом [13. Pp. 431–458]. Существует мнение, что чрезмерно оптимистично прогнозировать возможности ИИ и придерживаться упрощенного представления о функциях управляющих компаний. Автор согласен с мнением И. Ю. Беляевой, Б. С. Батаевой, О. В. Даниловой, что ИИ может изменить корпоративное законодательство и систему КСО, перейдя к более устойчивой модели корпоративного управления [10. С. 96]. Для этого, возможно, необходимо учитывать международные и отечественные стандарты отчетности в рамках КСО:

– Стандарты отчетности в области устойчивого развития «Глобальной инициативы по отчетности»;

– AccountAbility AA1000 (Стандарт социальной отчетности компаний AA1000);

– London Benchmarking Group (LGB);

– Social Accountability International (SA 8000);

The Ethical Trading Initiative;

– Investors in people;

– Руководство по социальной ответственности Международной организации по стандартизации (ISO 26000);

– Стандарт «Социальная ответственность организации. Требования» Международный стандарт IC CSR-08260008000 (Всероссийская организация качества);

– Социальная хартия российского бизнеса;

– «12 принципов ведения дел в России» Торгово-промышленной палаты РФ;

– «Социальная отчетность предприятий и организаций, зарегистрированных в Российской Федерации. Методические рекомендации»;

– Меморандум о принципах корпоративной социальной ответственности, который разработан Ассоциацией менеджеров России [10. С. 93–95].

КСО включает в себя развитие устойчивого развития, развитие корпоративного управления и достижение корпоративных целей, защиту заинтересованных предпринимателей и социально ответственные инвестиции. Это концепция, которая охватывает множество инициатив, основана на стремлении поддерживать высокие стандарты во всем, с чем приходится сталкиваться бизнесу. По мнению А. Джонстона, тот термин подразумевает процесс, с помощью которого компании выявляют и нейтрализуют негативное воздействие, которое их корпоративные действия и операции могут оказать на общество [16. P. 221].

С 1990-х годов КСО активно исследуется. В рамках развития ИИ можно выделить несколько ключевых характеристик КСО для развития нормативной базы рассматриваемой технологии. Во-первых, цель КСО состоит в том, чтобы сбалансировать интересы сторон за рамки ориентира на получение прибыли. Во-вторых, что касается сферы применения этого термина, то КСО направлена на решение широкого спектра задач, в первую очередь связанных с охраной окружающей среды и правами человека, с целью улучшения качества жизни и гармонизации общества в целом, способствуя созданию более устойчивого общества в целом за счет вклада корпораций и результатов их деятельности. В-третьих, КСО формировалась по пути превращения в обязательство по поддержанию легитимности корпоративных действий и решению задач устойчивого развития.

Во-первых, корпоративные решения принимаются в соответствии с обязательными правовыми нормами, закрепленными в национальных законах, которые защищают участников предпринимательской деятельности и потребителей, таких как трудовое законодательство, закон о защите прав потребителей, экологическое законодательство или законодательство о несостоятельности. Обязанности по соблюдению этих законов неотделимы от корпоративного права и корпоративного управления. То есть свобода действий управляющих компаний ограничена на законодательном уровне. Существующие в мировой практике законодательные подходы в корпоративном праве позволяют защитить предпринимателей. Например,

«Обязанность содействовать успеху компании», закрепленная в ст. 172 Закона о компаниях Великобритании 2006 года. Согласно этому акту, директора обязаны учитывать долгосрочные интересы корпорации, а также учитывать интересы поставщиков, сотрудников и сообществ, являться примером предусмотренного законом механизма преодоления трудностей [1]. Также часто бывает трудно установить прямую причинно-следственную связь между неправомерным поведением корпораций и ущербом социальной сфере, окружающей среде или правам человека, и, как правило, практически невозможно установить личность одного виновного. Поэтому необходимо обосновать необходимость защиты уязвимых сторон с наибольшей степенью зависимости как превентивным, так и компенсационным образом. Этот превентивный подход, основанный на внутреннем влиянии на поведение корпорации и решения советов директоров, также фокусирует внимание членов совета директоров на более активном участии в этических инициативах до того, как будет нанесен необратимый ущерб.

ИИ поможет компаниям определить новый образ мышления для разработки политики в области КСО и ее внедрения. ИИ и робототехника будут играть ключевую роль в долгосрочном развитии общества и достижении общего блага [9]. Это развитие согласуется с бизнес-стратегией компаний за счет оптимизации стратегии КСО и снижения рисков КСО. Сильный искусственный интеллект, имитирующий человеческий мозг, будет способствовать внедрению технологических инноваций, которые позволят собирать большие данные в режиме реального времени и составлять отчетность на основе данных. Это является новым средством коммуникации с заинтересованными сторонами, способствующим инновационной КСО.

Аспекты устойчивого развития впервые были упомянуты в докладе Брундтланд в 1987 году. В этом докладе устойчивое развитие рассматривается как удовлетворение «потребностей настоящего без ущерба для способности будущих поколений удовлетворять свои собственные потребности» [8]. Так, Организация Объединенных Наций разработала Повестку дня на период до 2030 года и набор из 17 целей устойчивого развития, которые объединяют и уравновешивают эти цели. Повестка постоянно дополняется. Ее необходимо пересматривать, чтобы усовершенствовать ее содержание и адаптировать к новым социальным и экологическим вызовам [3].

В 2010 году Европейский союз сформулировал Европейскую стратегию разумного, устойчивого и инклюзивного роста до 2020 года, пропагандирующую экономику, основанную на устойчивом развитии, знаниях и инновациях [2]. Актуальность этой стратегии была подтверждена в 2019 году, когда Европейская комиссия представила Европейское зеленое соглашение как возможность усовершенствовать экономическую модель для достижения климатической нейтральности к 2050 году [6]. Комиссия одобрила Инвестиционный план устойчивой Европы (SEIP) для достижения этой цели, подчеркнув, что цифровые технологии необходимы для создания умных, инновационных и адаптированных решений проблем, связанных с климатом.

Принимая корпоративное решение, директора должны найти баланс между тем, что хорошо для общества и что выгодно компании и ее акционерам. Пример

законодательного подхода, который способствует КСО, – ст. 172 Закона о компаниях Великобритании 2006 года. В ней закреплено, что у директоров есть право учитывать интересы заинтересованных сторон, не являющихся акционерами, при выполнении ими своих обязанностей. Этот подход учитывает социальные и экологические аспекты при принятии решений. Кроме законодательного закрепления, есть пример из судебной практики. Верховный суд Канады заявил, что при определении того, как компания должна действовать, совет директоров должен учитывать интересы акционеров, сотрудников, поставщиков, кредиторов, потребителей, правительств и окружающей среды [9].

Можно сделать вывод о том, что интеграция направлений устойчивого развития в деятельность организации выгодна с точки зрения репутации, производительности и доступа к финансовым ресурсам. Усилия компаний в этом направлении положительно скажутся на финансовых показателях компании. Организации смогут получить лучшие ресурсы, более квалифицированных сотрудников и более широкие возможности. Многие корпорации воспринимают этот путь не как проблему, а как перспективу укрепления своих долгосрочных интересов и отношений с поставщиками, сотрудниками.

ИИ включает в себя различные технологии с различными функциями и потенциальными рисками. Универсального решения текущих проблем при использовании ИИ не существует. Традиционные инструменты регулирования не подходят для немедленного реагирования в условиях глобализации. По этой причине автор полагает, что настало время для нового подхода, основанного на более высоком или более низком риске конкретного решения, который определяет набор общих принципов и минимальных стандартов, которые должны соблюдаться в каждой конкретной ситуации. Такое «минимальное» регулирование позволило бы создать единую модель, которая применялась бы к различным участникам рынка, но одновременно не препятствовала бы технологическому развитию и инновациям.

Соответственно, целесообразно внедрить подход, который широко используется в таких различных областях, как окружающая среда, финансы, продовольствие и юридические услуги. Регулирование, основанное на оценке рисков, как особый комплекс методов, используемых регулирующими органами, может включать разработку механизмов принятия решений для определения приоритетов регулирующей деятельности и оценки рисков. Для этого требуется определение рисков в качестве отправной точки, характеризует элементы этих рисков, такие как их природа, тип, уровень и вероятность, и создает рейтинг рисков на основе этих оценок. Такой подход поможет компаниям развивать ИИ в безопасном и выгодном направлении. Преимущества регулирования, основанного на оценке рисков, позволят компаниям быстрее внедрять тщательный анализ потенциальных рисков в корпоративные решения. В конечном счете регулирование, основанное на оценке рисков, помогает «надежному управлению, способствуя эффективному использованию ресурсов регулирующих органов и осуществлению мероприятий, пропорциональных рискам» [14].

Такая модель была одобрена Европейской комиссией в ее предложении о регулировании ИИ. Учитывая негативные последствия, которые может повлечь за собой использование ИИ для заинтересованных сторон, работников и других

лиц, предлагаемая нормативная база направлена на то, чтобы сбалансировать различные цели и интересы вовлеченных сторон и избежать потенциальных нарушений основных прав. В целях защиты конфиденциальности, личных данных и другой конфиденциальной информации он тесно связан с Директивой об открытых данных [5], Предложением о Регламенте европейского управления данными 184 и предлагаемым Законом о данных 185 и дополняет Общий регламент по защите данных (GDPR) [4], а также законодательство о защите прав потребителей, недискриминации и защите окружающей среды. Уровень ограничений следует оценивать в каждом конкретном случае, чтобы убедиться, что он не выходит за рамки того, что необходимо для предотвращения и смягчения рисков для безопасности и нарушений основных прав. Кроме того, для обеспечения последовательности, избежания дублирования и минимизации дополнительной нагрузки нормативная база подлежит интеграции в существующее отраслевое законодательство в области безопасности.

Заключение. Таким образом, регулирование ИИ требует коллективных усилий с привлечением междисциплинарных специалистов, определяющих особенности ролей, связанных с внедрением ИИ в зале заседаний. Искусственный интеллект стал неотъемлемой частью практически любого цифрового взаимодействия, и разумное регулирование прокладывает путь к этому; такой подход может быть адаптирован для решения конкретных социальных, экологических проблем и проблем в области прав человека.

Список литературы

1. Закон о компаниях Великобритании от 8 ноября 2006 года. [Электронный ресурс]. URL: https://www.legislation.gov.uk/ukpga/2006/46/section/172 (дата обращения: 04.09.2024).

2. Europe 2020: a strategy for smart, sustainable and inclusive growth. Brussels, 03.3.2010. [Электронный ресурс]. URL: https://www.eea.europa.eu

3. Traore D. From the Theory of the African Origin of Humankind to Modern Social, Legal and Technological Innovations: a Brief Analytical Excursion into Anthroposociogenesis // Journal of Digital Technologies and Law. 2024. № 2. Pp. 473–486. https://doi.org/10.21202/jdtl.2024.24

4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu

5. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. URL: https://eur-lex.europa.eu

6. The European Green Deal. Brussels, 11. 12.2019. URL: https://eur-lex.europa.eu

7. Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. 2021. URL: https://legalinstruments.oecd.org

8. Report of the World Commission on Environment and Development: Our Common Future (Brundtland Report»), United Nations. Oxford University Press, Oxford. 1987. URL: https://www.are.admin.ch

9. Бегишев И. Р. Криминологическая классификация роботов: риск-ориентированный подход // Правоприменение. 2021. Т. 5, № 1. С. 185–201. EDN: TBUVGY

10. Развитие корпоративных стратегий и технологий в российских компаниях / И. Ю. Беляева, Б. С. Батаева, О. В. Данилова [и др.]. Тверь: Финансовый университет при Правительстве Российской Федерации. 2019. 387 с.

11. Филипова И. А., Коротеев В. Д. Будущее искусственного интеллекта: объект или субъект права? // Journal of Digital Technologies and Law. 2023. № 2. С. 359–385.

12. Bankewitz M., Åberg C., Teuchert C. (2016) Digitalization and boards of directors: a new era of corporate governance? // Business Manage Res. 2016. Vol. 5, № 2. Pp. 58–64.

13. Bruner C. Distributed ledgers, artificial intelligence, and the purpose of the corporation // Cambridge Law J. 2020. Vol. 79, № 3. Pp. 431–458.

14. Coglianese C. (2019). What does risk-based regulation mean? // The Regulatory Review. 2019, July 8. URL: https://www.theregreview.org

15. Darnault C., Parcollet T., Morchid M. Artificial intelligence: a tale of social responsibility. // Hal. 2020, January 26. URL: https://hal.archives-ouvertes.fr

16. Johnston A. (2011) Facing up to social cost: the real meaning of corporate social responsibility // Griffith Law Review. 2011. Vol. 20, № 1. P. 221.

17. Naqvi A. Artificial intelligence for asset management and investment: a strategic perspective. Wiley, Hoboken, 2021. 320 p.

18. Petrin M. Corporate management in the age of AI // Columbia Business Law Rev. 2019. Pp. 965–1030.

19. Porro C., Bierce K. (2018) AI for good: what CSR professionals should know. CECP, 29 June 2018. [Электронный ресурс]. URL: https://cecp.co/what-csr-professionals-should-know-about-artificial-intelligence (дата обращения: 04.09.2024).

20. Riffle C. What artificial intelligence means for sustainability // Greenbiz. 2017. URL: https://www.greenbiz.com

21. Vinuesa R., Azizpour H., Leite I., Balaam M., Dignum V., Domisch S., Felländer A., Daniela Langhans S., Tegmark M., Fuso Nerini F. The role of artificial intelligence in achieving the Sustainable Development Goals // Nat Commun. 2020. № 11. Pp. 1–10.

22. Zhao J., Artificial Intelligence and Corporate Decisions: Fantasy, Reality or Destiny // Cath. U. L. Rev. 2022. № 71. P. 663. URL: https://scholarship.law.edu

23. Шутова А. А. Цифровой паспорт здоровья: этические и правовые проблемы // Вестник Казанского юридического института МВД России. 2021. Т. 12, № 2(44). С. 236–241. EDN: DPUAMG

24. Концепция цифрового государства и цифровой правовой среды: монография. М.: ИЗиСП: Норма: ИНФРА-М, 2024.

Н. С. Купцов,
студент,
Российский государственный университет правосудия

ПРАВО НА ИНДИВИДУАЛЬНОСТЬ ГРАЖДАНИНА КАК УСЛОВИЕ ОХРАНЫ НЕМАТЕРИАЛЬНЫХ БЛАГ В МИРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Аннотация. В настоящей статье рассматривается актуальная, на взгляд автора, проблема необходимости дополнения существующего в отечественном гражданском законодательстве перечня охраняемых нематериальных благ с учетом стремительного развития цифровых технологий и многократного увеличения количества противоправного использования их продуктов. В этой связи предлагается возможность внедрения и гарантии со стороны государства права гражданина на индивидуальность как совокупность личностных поведенческих и анатомо-физиологических особенностей. В статье последовательно анализируются понятие и содержание человеческой индивидуальности, рассматриваются отдельные недостатки имеющихся на сегодняшний день механизмов защиты личных неимущественных прав гражданина, разъясняется принципиальная значимость провозглашения права на индивидуальность в момент практически неконтролируемого развития технологий искусственного интеллекта и генерируемого цифрового контента.

Ключевые слова: гражданское право, личные неимущественные права, нематериальные блага, индивидуальность, искусственный интеллект, защита права.

THE RIGHT TO THE INDIVIDUALITY OF A CITIZEN AS A CONDITION FOR THE PROTECTION OF INTANGIBLE BENEFITS IN THE WORLD OF HIGH TECHNOLOGIES

Abstract. This article examines, in the author's opinion, the urgent problem of the need to supplement the list of protected intangible goods existing in domestic civil legislation, taking into account the rapid development of digital technologies and the multiple increase in the number of illegal uses of their products. In this regard, the possibility of introducing and guaranteeing by the state the right of a citizen to individuality as a set of personal behavioral and anatomical and physiological characteristics is proposed. The article consistently analyzes the concept and content of human individuality, examines some shortcomings of the currently available mechanisms for protecting personal non-property rights of a citizen, explains the fundamental importance of proclaiming the right to individuality at the time of the practically uncontrolled development of artificial intelligence technologies and generated digital content.

Keywords: civil law, personal non-property rights, intangible benefits, individuality, artificial intelligence, protection of law

Введение. Известно, что право, являясь наиболее эффективным социальным регулятором общественных отношений, всегда чутко реагирует на любые из-

менения политических, экономических, социальных и духовных условий общественной жизнедеятельности [16]. Иного и невозможно предположить: поскольку важнейшей целью существования социальных (и собственно правовых) регуляторов, их основополагающей функцией выступает регулирование общественных отношений между людьми [12. С. 63] путем установления общих правил поведения в конкретный период времени на отдельной территории, постольку такие правила подвержены неизбежному изменению как в силу естественных, эволюционных процессов, так и в ходе резких революционных преобразований. Сказанное особенно верно в отношении правового регулирования: так, история имеет немало примеров стремительного разрушения всей правовой системы государства, в одночасье приобретшего качественно иную форму политического устройства, и воздвижения на ее руинах принципиально нового правопорядка.

Современный мир, несмотря на кажущееся достижение определенной стабильности в процессе собственного развития, вовсе не избавлен полностью от внезапно возникающих вызовов устоявшимся нормам и принципам правового регулирования. Вместе с тем сегодня подобные вызовы следует ожидать не столько от всевозможных геополитических, социально-экономических и духовно-культурных обстоятельств, сколько от фактора, ставшего особенно ощутимым в последнее время, – широкого развития цифровых технологий, возможности и сфера применения которых с каждым годом становятся все пространнее. Масштаб ощущаемого влияния цифровой среды и высоких технологий на всю систему правового регулирования общественных отношений столь огромен, что не кажутся сегодня излишними замечания исследователей о необходимости системного изменения существующих правовых институтов и моделей юридического мышления [10. С. 135], технологических изменениях рубежа XX–XXI столетий как наиболее серьезном вызове праву за всю историю его существования [3. С. 14].

Представляется, что наиболее ощутимо давление всей совокупности технологических новшеств сказывается на тех правовых институтах, которые традиционно принято рассматривать базовыми, основополагающими. К таким институтам относится, в частности, институт личных неимущественных прав в гражданском праве, призванный установить и гарантировать правовую защиту нематериальных благ, принадлежащих гражданам от рождения и самой своей природой предполагающих обязанность неограниченного круга лиц воздерживаться от какого бы то ни было противоправного посягательства на них. Перечень таких благ установлен законодательно: п. 1 ст. 150 ГК РФ [4] к ним относятся жизнь, здоровье, достоинство личности, имя гражданина, его личная и семейная тайна и другие нематериальные блага; при этом следует обратить внимание, что перечень не является исчерпывающим. В данном случае очевиден распространенный прием законодательной техники: в тексте закона сознательно не приводится закрытый перечень юридических конструкций с целью преодоления необходимости внесения в него правок в ходе изменения условий применения правовой нормы.

Однако временами системообразующий, «глобальный» характер вынужденной модернизации правовой нормы является слишком мощным вызовом для всего правового института и устоявшейся практики его реализации, чтобы его можно было бесспорно вписать в категорию «иных», заблаговременно предусмотренную в тексте конкретной нормы. В этом случае велика потребность в более

детальной разработке правового регулирования, отвечающего масштабу такого изменения. Думается, ярким примером в подтверждение сказанного может стать предполагаемая автором необходимость разработки механизма правового регулирования и защиты в современных условиях личного неимущественного права гражданина на его индивидуальность.

Основная часть. Индивидуальность человека – одна из традиционных философских категорий, относящихся к этапам становления и развития человека, наряду с понятиями «индивид» и «личность». Общепринято при этом говорить, что становление человеческой индивидуальности представляет собой процесс взаимосвязанного формирования каждым индивидом собственных, уникальных физических, психологических и социальных черт, образующихся под неизбежным и обязательным воздействием окружающего мира и социума [15. С. 16]. Такой взгляд на существо индивидуальности человека не нов: отечественная философия в целом презюмирует индивидуальность как неповторимую идентичность каждого конкретного человека; не случайно Т. С. Васильева еще в конце прошлого столетия справедливо замечает, что индивидуальность означает «быть самим собой», «быть причиной самого себя» [2. С. 17]. Понимание же индивидуальности человека в бытовом отношении в самом общем виде зиждется на совокупности отдельных черт конкретной личности, обусловленных как физиологически, так и социально: голоса и особенностей речи, внешности, особенностей движения (походки), отдельные черты поведения, сформированные под воздействием темперамента, возраста, условий жизни и окружающей среды, и других. Принципиально важно в свете настоящего исследования указать на то, что подобные качества, составляющие индивидуальность каждого человека, всегда выступают своеобразными «маркерами», позволяющими с высокой степенью вероятности идентифицировать конкретного индивида, а при совпадении всех признаков и вовсе идентифицировать бесспорно. По крайней мере, так было до относительно недавнего времени.

Появление новейших технологических разработок, которые в силу чрезвычайной открытости современного мира стремительно перестают быть специальными инструментами ученого и профессионального сообщества, переходят в достояние общества, грозит нанести «неприкосновенности» человеческой индивидуальности серьезный ущерб. И надо отметить, что дело не только и не столько в актуальной философской проблеме противостояния человеческого и технологического миров. Широкое и неконтролируемое распространение цифровых технологий, позволяющих с нуля создавать изображения, видео- и аудиофайлы, содержащие в себе визуальные или звуковые черты конкретного индивида без его выраженного согласия (особо среди таких технологий выделяется искусственный интеллект, создающий результат работы алгоритма вовсе без участия человека), множит случаи неправомерного использования подобного контента, тем самым предъявляя серьезный вызов праву. Своеобразным апогеем обозначенной проблемы можно считать распространение в цифровой среде так называемых дипфейков – технологий крайне реалистичной подмены изображения и голоса посредством использований генеративных нейросетей; отдельными авторами дипфейк обозначается не иначе, как угроза национальной безопасности государства

[7. С. 56–61]. Не остаются в стороне и факты телефонного мошенничества, основанные на генерации голоса человека, знакомого с жертвой злоумышленников; для обмана в данном случае правонарушителями используется узнаваемость голосовых признаков, составляющих элемент человеческой индивидуальности. На взгляд автора, это свидетельствует о крайней актуальности проблемы и необходимости ее скорейшего урегулирования.

Следовательно, генерация или высококачественное создание посредством использования информационных технологий облика, внешности, голоса и иных узнаваемых черт конкретного человека гипотетически могут повлечь для него определенные негативные последствия, поскольку создание подобного контента зачастую осуществляется с заведомо противоправной целью. В качестве таковых возможно рассматривать не только причинение ощутимых физических и нравственных страданий, вызванных фактом несогласованного грубого воспроизведения личностного образа, но и существенные репутационные, имиджевые потери: зачастую поведение подобного «цифрового двойника», видимое или озвучиваемое посредством технических средств, разительно отличается от того, каким было бы поведение настоящего человека в сравнимых обстоятельствах. В этой связи вопрос о правовой защите гражданина от подобного противоправного поведения со стороны иных лиц приобретает ярко выраженное практическое значение.

Нельзя сказать, что в действующем отечественном законодательстве способы защиты отдельных личных индивидуализирующих человека благ полностью отсутствуют. Так, Федеральным законом № 231-ФЗ [14] еще в 2006 году первая часть Гражданского кодекса РФ дополнена статьей 158.1, установившей режим правовой охраны изображения гражданина. Его обнародование и использование отныне допускались исключительно с согласия гражданина, за исключением немногочисленных изъятий из данного правила; любой факт неправомерного использования изображения мог привести к уничтожению материальных носителей, на которых оно содержится, а равно к пресечению его распространения в сети Интернет. Достаточно обширная правоприменительная практика использования указанной нормы может обусловить возникновение соблазна применения ее для защиты нематериальных благ гражданина, пострадавшего от распространения сгенерированного контента, содержащего его внешний образ, по аналогии. Вместе с тем автору такой подход представляется недопустимым.

Прежде всего необходимо оговориться, что предоставление изображению гражданина правовой охраны направлено на защиту внешнего облика человека в качестве одного из принадлежащих ему нематериальных благ. В этом смысле согласимся с позицией Е. А. Брайцевой, понимающей под изображением «отображение... основных черт человека» [1. С. 323], по которым его можно идентифицировать неопределенному кругу лиц. Еще ближе к истине представляется определение А. П. Рабец и А. А. Коростиева, обоснованно указавших на важный признак любого изображения – его статичность, фиксированность на материальном носителе в конкретный момент времени; при этом авторы корректно разделяют понятия «изображения» и «внешнего облика», замечая, что последний выступает более широкой категорией, охватывающей в том числе динамическое отображение внешних черт конкретного гражданина [11. С. 82]. В схожем ключе рассуждает М. Н. Малеина, понимающая под индивидуальным обликом человека не только

собственно внешность, но и фигуру, физические данные, одежду [8. С. 25]. Думается, что именно в этом кроется невозможность применения ст. 158.1 ГК РФ для защиты гражданина от использования его индивидуальности в созданном искусственным интеллектом контенте: предоставляя правовую охрану статичному отображению внешности, указанная норма не затрагивает охраны иных внешних идентифицирующих черт человека в их динамике (например, если речь идет о видеофрагменте, где сгенерированный облик реального человека не просто воссоздан внешне, но и использует яркие особенные жесты, характерные для этого гражданина движения, элементы одежды, имиджа и пр.). Верно и другое замечание: поскольку речь идет о внешнем облике человека, созданном исключительно посредством технологии искусственного интеллекта (т. е. вне прямого взаимодействия с настоящим обладателем отображаемой внешности), принципиальную важность приобретает вопрос о допустимости рассмотрения такого отображения в качестве изображения в целом. В этом смысле не кажется неуместным мнение А. С. Киселева о том, что сгенерированный облик человека не является его реальным изображением, а значит, регулирование правоотношений по созданию и распространению подобного контента выходит за рамки ст. 158.1 ГК РФ [7. С. 60]. Автор настоящего исследования позволит себе с этим согласиться.

По схожим причинам не может рассматриваться в качестве универсальной правовой нормы, позволяющей защитить индивидуальность гражданина, ст. 19 ГК РФ, гарантирующая право на имя. Несмотря на теоретическую возможность расширительного толкования и подразумевания под понятием «имя» собственно человеческой личности во всем многообразии ее уникальных черт, автор согласится с позицией А. Х. Ульбашева, понимающего под именем лишь «буквенное обозначение человеческой личности» [13] – ни больше, ни меньше.

Если в отношении визуальных черт человека, воспринимаемых в качестве его индивидуализирующих признаков, существуют хотя и неприменимые к решению обозначенной в работе проблемы, но все же объективно закрепленные в законодательстве способы правовой защиты, то иные индивидуальные черты гражданина остаются вовсе лишенными охраняемого статуса. К таковым можно отнести прежде всего физиологические и речевые особенности голоса человека: его тембр, высоту, силу, звонкость; а равно лексикон, словарный запас, культуру речи, яркие и запоминающиеся речевые обороты, фразеологизмы и др. Высококачественный уровень создания генерируемого контента с использованием современных технологий делает возможным полное копирование голоса и речи конкретного гражданина, приводящее к невозможности различения «оригинала» и «подделки» без использования специальных технических средств или профессиональных знаний (значительный рост случаев успешного для злоумышленников телефонного мошенничества в сфере корпоративных и трудовых правоотношений – лишнее тому подтверждение) [6]. Несмотря на это, отечественное гражданское законодательство сегодня не имеет в себе предпосылок для предоставления голосу человека в совокупности его индивидуальных признаков статуса охраняемого нематериального блага; избегает острого обсуждения на этот счет и основная масса общественности, если не считать разрозненные попытки воздействовать на законотворчество путем внесения предложений отдельных профессиональных сооб-

ществ [5]. Однако необходимость фиксации голоса гражданина в качестве охраняемого нематериального блага в рамках института личных неимущественных прав все шире аргументируется в среде ученого сообщества – на этом настаивает, в частности, Е. А. Моргунова [9. С. 315–316].

Следует ли в такой ситуации напоминать об иных индивидуальных чертах человека, не нашедших хотя бы контурной защиты в рамках института личных неимущественных прав граждан: особенностей характера, темперамента, привычек, характерных аксессуаров, элементов одежды, возрастных, этнических или профессиональных особенностей? Уровень развития генерирующего искусственного интеллекта уже на сегодняшний день (не говоря о дне завтрашнем) не предоставляет возможности вести речь об этом вопросе как о надуманном.

По мнению автора, единственно возможным способом обеспечить всестороннюю защиту индивидуальных нематериальных благ граждан на современном этапе является законодательное закрепление в тексте ГК РФ права гражданина на индивидуальность; в свою очередь, в перечень поименованных в ст. 150 ГК РФ нематериальных благ, охраняемых законом, следует включить индивидуальность как совокупность любых объективных анатомо-физиологических или личностных поведенческих признаков, способствующих опознанию, «идентификации» конкретного гражданина неопределенным кругом лиц. Такой подход позволит не только обеспечить действенный механизм защиты личных неимущественных прав гражданина, нарушенных в результате несогласованного использования его индивидуального образа для создания сгенерированного цифрового контента, предоставить правовые основания для возможности восстановления нарушенного права, но и сделать значительный шаг к разрешению системной проблемы правовой неопределенности в вопросе взаимодействия человека и общества с технологиями искусственного интеллекта. При этом признание индивидуальности человека в качестве самостоятельного нематериального блага позволит избежать усложнения текста нормативных правовых актов, избавит от необходимости отдельного закрепления в и без того обширном по своему объему Гражданском кодексе РФ конкретных благ, составляющих человеческую индивидуальность. В пользу указанного предложения свидетельствует и тот факт, что уровень технологического развития нейросетевых технологий сегодня способен создать образ человека в целостной взаимосвязи его идентифицирующих признаков, перечень которых может существенно различаться в зависимости от обстоятельств создания и распространения конкретного сгенерированного контента. Отдельно отметим, что законодательное признание и гарантия права на индивидуальность человека не повлечет пересмотра или существенного изменения способов его защиты: думается, что в качестве таковых могут рассматриваться ставшие уже традиционными компенсация морального вреда (ст. 12 ГК РФ); признание факта нарушения права, требование пресечения и запрещения действия – в данном случае создания и распространения сгенерированного противоправного контента (ст. 150 ГК РФ); требование о защите чести, достоинства и деловой репутации (ст. 152 ГК РФ).

Заключение. Таким образом, быстрое и неконтролируемое развитие современных цифровых технологий (в особенности генеративного искусственного интеллекта) и все увеличивающийся объем противоправных деяний с их использо-

ванием вынуждает вести речь о необходимости качественной и всесторонней модернизации правового регулирования. Одной из важных и назревших перемен в этом смысле представляется необходимость дополнения перечня охраняемых законом нематериальных благ понятием «индивидуальности» и сопутствующего законодательного закрепления права гражданина на индивидуальность как совокупность личностных поведенческих и анатомо-физиологических особенностей конкретного человека, позволяющих идентифицировать его неопределенным кругом лиц. Данный шаг, несмотря на известную революционность, позволит не только значительно повысить степень защищенности личных неимущественных прав гражданина, обеспечить надлежащий уровень их охраны и восстановления на современных условиях, но и может стать первым шагом к установлению действенного правового регулирования отношений, связанных с использованием технологий искусственного интеллекта, их взаимодействия с человеком и обществом.

Безусловно, такое изменение неизбежно приведет к возникновению новых теоретических вопросов: например, о возможности отнесения отдельных элементов, составляющих человеческую индивидуальность, к объектам права интеллектуальной собственности. Думается, что в данном случае возникающие трудности могут быть решены посредством эффективного взаимодействия ученого сообщества и правоприменения.

Список литературы

1. Брайцева Е. А. Право на изображение гражданина, его реализация и охрана // Евразийское научное объединение. 2020. № 11–5. С. 323–325.

2. Васильева Т. С. Проблема индивидуальности и философская антропология // Новые идеи в философии. 1997. № 6. С. 17–25.

3. Гаджиев Г. А. Онтология права (критическое исследование юридического концепта действительности): монография. М.: Норма: ИНФРА-М, 2021. 320 с.

4. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 08.08.2024) // СПС «Консультант Плюс».

5. Дикторы попросили Госдуму защитить их голоса от искусственного интеллекта // Информационный портал «РБК». URL: https://www.rbc.ru

6. Им голос был, он звал успешно: бизнес атакуют мошенники новой аудиогенерации // Информационное агентство «Коммерсантъ». URL: https://www.kommersant.ru

7. Киселев А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2021. № 3. С. 54–64.

8. Малеина М. Н. Право обучающегося и преподавателя на индивидуальный облик // Lex Russica (Русский закон). 2019. № 3(148). С. 24–33.

9. Моргунова Е. А. Исполнение как объект правовой охраны // Пермский юридический альманах. 2021. № 4. С. 310–323.

10. Мусалов М. А. Цифровая эпоха: проблемы и особенности взаимодействия публичного и частного права // Аграрное и земельное право. 2024. № 1(229). С. 134–137.

11. Рабец А. П., Коростиев А. А. Право гражданина на внешний облик и изображение в системе личных неимущественных прав // Тенденции развития науки и образования. 2020. № 67–6. С. 80–88.

12. Рукавишникова И. В. Право: учебник для среднего профессионального образования / под ред. И. В. Рукавишниковой, И. Г. Напалковой, А. Н. Позднышова. 2-е изд., перераб. М.: Норма: ИНФРА-М, 2023. 576 с.

13. Ульбашев А. Х. Общее учение о личных правах. М.: Статут, 2019. 255 с.

14. О введении в действие части четвертой Гражданского кодекса Российской Федерации: Федеральный закон от 18 декабря 2006 г. № 231-ФЗ (ред. от 29.12.2022) // СПС «Консультант Плюс».

15. Человек: индивид, индивидуальность, личность: монография / под науч. ред. проф. И. И. Кального. М.: ИНФРА-М, 2022. 351 с.

16. Черногор Н. Н., Емельянов А. С., Залоило М. В. Программирующая и кодирующая функции права в эволюционной изменчивости его социального назначения // Вопросы истории. 2022. № 3(2). С. 90–98.

П. А. Лебедь,
студент,
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации;
приглашенный студент,
Пекинский университет

ЗАЩИТА ГОЛОСА ЧЕЛОВЕКА: СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ ПРАВА РОССИИ И КИТАЯ

Аннотация. В последнее время все актуальнее становится проблема признания и использования права человека на голос как личного неимущественного права физического лица. В данной статье приводится общий обзор текущего положения законодательного регулирования защиты голоса человека в России и Китае, а также анализ китайской судебной практики для возможного дальнейшего заимствования некоторых практических аспектов китайского гражданского права и правоприменения, связанных с защитой голоса человека.

Ключевые слова: защита голоса, личные неимущественные права, сравнительное право, гражданское право России, гражданское право Китая, защита прав

PROTECTION OF RIGHT FOR VOICE. LEGAL COMPARATIVE STUDY OF THE LAW OF RUSSIA AND CHINA

Abstract. Recently, the problem of recognition and use of the human right to voice as a personal non-property right of an individual has become increasingly relevant. This article provides a general overview of the current state of legislative regulation of human voice protection in Russia and China, as well as an analysis of Chinese judicial practice for possible further borrowing of some practical aspects of Chinese civil law and law enforcement related to the protection of human voice.

Keywords: voice protection, personal non-property rights, comparative law, Russian civil law, Chinese civil law, rights protection

Введение. Для обозначения проблематики данной статьи для начала необходимо определиться с ключевым ее понятием – понятием голоса. Согласно определению Музыкальной энциклопедии, голос – это «разнообразные звуки, образующиеся при помощи голосового аппарата и служащие для общения между живыми существами. У человека это общение осуществляется в основном посредством речи и пения» [9]. Высокую оценку получает голос как благо для лиц определенных профессий (артист оперы, диктор радио и телевидения, пародист, имитатор, врач-психотерапевт, экскурсовод и пр.). Кроме того, голос – одна из уникальных черт личности, а с юридической точки зрения он является объектом личных неимущественных прав физического лица и одной из форм биометрической аутентификации, позволяющей идентифицировать личность человека по совокупности своих уникальных характеристик [2].

Основная часть. В современном российском законодательстве голос фигурирует в основном как «биометрический» показатель (см., например, Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановление Правительства РФ от 30 июля 2018 г. № 772, распоряжение Правительства РФ от 30 июня 2018 г. № 1322-р и др.). Так, согласно ст. 11 ФЗ № 152, биометрическими персональными данными признаются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность. В современном мире голос уже является примером таких сведений и применяется в ряде методов информационной защиты, требующих для разблокировки, к примеру, не просто ввести верный пароль, но произнести его голосом владельца аккаунта.

Несмотря на то, что голос как объект личных неимущественных прав в России пока не охраняется, предполагаем, что суд может применить по аналогии нормы, защищающие изображение (ст. 152.1 ч. 1 Гражданского кодекса РФ), придя к выводу, что, например, запись голоса человека может быть обнародована и использована в дальнейшем только с его согласия либо, после его смерти, с согласия детей, пережившего супруга или родителей.

На фоне стремительного развития цифровых технологий и технологии искусственного интеллекта, создания компьютерных программ для синтеза голоса либо его изменения («автотюн»), появления технологии создания так называемых дипфейков (от англ. deep learning – «глубокое изучение» и fake – «подделка») и прочих факторов проблема признания голоса человека как отдельного объекта гражданских прав встает все острее. Так, в январе 2023 года Союз дикторов обратился к главе комитета Государственной Думы по информационной политике А. Е. Хинштейну с просьбой об установлении специального регулирования синтеза человеческого голоса и использований технологии искусственного интеллекта, так как использование подобных технологий влечет прямую угрозу существованию таких профессий, как, например, диктор или актер озвучивания (дубляжа) [12].

На текущий момент во многих странах мира голос человека является объектом его нематериальных прав наравне с изображением (см. п. 6 ст. 2 ч. 1 Закона Израиля о защите частной жизни, п. 18 ст. 66 Конституции Эквадора, п. 7 ст. 2

Конституции Перу и ст. 15 ГК Перу, ст. 3344 (а) ГК Калифорнии, п. 2 ст. 1023 ГК КНР и др.). Отношение к подобному «приравниванию» права на голос к праву на изображение может быть спорной позицией. Так, М. Н. Малеина полагает аналогию закона неприменимой, несмотря на одинаковую цель нематериальных благ (облика и голоса) – индивидуализацию гражданина [7], в то время как А. Г. Матвеев и Е. Ю. Мартьянова, наоборот, считают аналогию очевидным инструментом защиты права на голос [8].

Подобной позиции придерживается и китайский законодатель. Часть 2 ст. 1023 ГК КНР гласит: «К защите голоса физических лиц по аналогии применяются соответствующие положения о защите изображения» [3. С. 353]. В то же время в дальнейшей китайской юридической практике защита голоса человека обрастает множеством нюансов, изначально не свойственных защите изображения. Например, в отношении голоса используется так называемый критерий известности [15]. Концепция этого критерия заключается в том, что необходимо по-разному подходить к защите голоса широко известных лиц (крупные политики и религиозные деятели, артисты, теле- и радиодикторы, крупные бизнесмены), лиц, известных в определенном кругу (ученые, преподаватели, местные политики) и «незнаменитостей» (обывателей) [17], так как неправомерное использование голоса широко известного лица может повлиять на мнение значительного процента населения, голоса лица, известного в определенном кругу – на широкую группу населения (коллег ученого, студентов преподавателя и т. д.), а голоса «незнаменитости» – преимущественно на ближайшее окружение конкретного человека (семью, друзей, коллег). Таким образом, если неправомерное использование голоса «незнаменитости» чаще всего нарушает лишь личные неимущественные права конкретного лица, то неправомерное использование голоса широко известного лица может даже стать угрозой национальной безопасности [16]. Схожей позиции придерживаются и некоторые наши исследователи, например, об этом говорит А. С. Киселев на примере использования дипфейков бывшего президента США Б. Обамы с осуждающей речью в сторону бывшего президента США Д. Трампа [5].

Следует также отметить, что теме дипфейков уделено внимание и в ГК КНР. Так, ст. 1019 запрещает «подделывание (изображения) с помощью использования средств информационных технологий». Согласно ч. 2 ст. 1023, то же относится и к подделыванию голоса. Данное положение было введено именно для предотвращения возможной угрозы национальной безопасности и общественным интересам, о чем прямо говорится в сводном докладе Конституционной и правовой комиссии ВСНП об изменениях в разделе «Личные неимущественные права» проекта Гражданского кодекса от 20 апреля 2019 года [10].

Еще одним важным аспектом является способ обнародования и/или использования записи голоса. Об этой проблеме в 2015 году писала еще М. Н. Малеина [6], а сейчас эта проблема внезапно стала одной из наиболее актуальных, после того как в августе 2023 года актриса озвучивания Алена Андронова подала в суд на АО «Тинькофф Банк» за распространение на платной основе TTS-функции с ее голосом в системе Tinkoff VoiceKit без ее согласия, так как по заключенному между А. Андроновой и АО «Тинькофф Банк» в 2019 году договору голос актрисы должен был использоваться только для обучения голосового помощника колл-центра Тинькофф [1].

В Китае способу дальнейшего использования записи изображения и голоса человека также уделяется большое внимание. Так, в апреле 2021 года Управление по вопросам киберпространства, Министерство общественной безопасности, Министерство коммерции, Министерство культуры и туризма, Государственная налоговая администрация, Главное государственное управление по контролю и регулированию рынка и Главное управление по делам радио, кино и телевидения Китая приняли проект «Мер по управлению онлайн-маркетингом». Статья 25 «Мер» утверждает, что использование лица или голоса третьего лица во время прямого эфира законно исключительно с согласия лица, и предупреждает о незаконности подделки этих персональных данных техническими средствами [11]. Уже в сентябре того же года Интернет-суд Пекина вынес решение по делу (2021) 京 0491 民初 23000 号, которое вызвало немалые споры в китайском юридическом сообществе. Согласно обстоятельствам дела, гражданин Хэ Гохуан заключил договоры об участии в рекламной кампании в качестве режиссера с компанией Beijing Sunshine Yinyi Technology Co., однако под давлением начальства сам стал участником более 30 коротких видео, записанных в рамках этой рекламной кампании. Позднее данные видео были выложены в видеосервисе Douyin (TikTok) не только на официальном аккаунте указанной компании, но и на аккаунте «Чжэнь-нян» («Сестрица Чжэнь»), официальном аккаунте Shenzhen Sunshine Yinyi Technology Co. Хэ Гохуан подал иск в Интернет-суд Пекина против обеих компаний с требованием компенсации ему морального вреда за незаконное использование его изображения и голоса в размере 25 000 юаней (~300 000 рублей) от каждой из компаний, так как с шэньчжэньской компанией он вообще не заключал каких-либо соглашений, а пекинской компании не давал согласия на использование своего образа (изображения) и голоса. Требования были частично удовлетворены [4].

Еще более запутанным оказалось дело, рассмотренное Пекинским интернет-судом 23 апреля 2024 г. Истец Инь, занимающийся дубляжом, случайно обнаружил, что на платформе широко распространилось видео, в котором он озвучил его собственный голос. После отслеживания источника выяснилось, что дубляж вышеупомянутого видео был выполнен с помощью продукта преобразования текста в речь, которым управляет ответчик А. Истец однажды записал звукозапись для Ответчика Б (медиакомпании), а Ответчику Б принадлежали авторские права на звукозапись. Ответчик Б позже предоставил аудиозапись ответчику С (компании – разработчику программного обеспечения), что позволило ему «использовать, копировать и изменять данные в коммерческих или некоммерческих целях для своих продуктов и услуг». Ответчик С использовал аудиозаписи в качестве учебных материалов по искусственному интеллекту для создания продуктов преобразования текста в речь, задействованных в деле, и продавал их на платформе ответчика D (платформа облачного сервиса). Ответчик А подписал договор о продаже онлайн-услуг с ответчиком Е (компанией по разработке технологий), а ответчик Е приобрел продукт преобразования текста в речь, участвующий в деле, у ответчика С. Ответчик А использовал интерфейс прикладной программы для прямого доступа к продукту (без технической обработки) и использования его на своей платформе. По решению суда медиакомпания и компания-разработчик были приговорены к выплате крупной компенсации [13]. Это было первое дело в Китае,

связанное с защитой права на голос в связи с неправомерным его использованием для создания сгенерированного ИИ синтезированного голоса [14].

Более того, в Китае практикуется не только защита голоса реальных граждан, но и защита синтезированных голосов популярных виртуальных персонажей как объектов авторского права юридических лиц на художественные или аудиовизуальные произведения. Как правило, в такой защите нуждаются так называемые виртуальные айдолы. Виртуальный айдол – это продукт, для создания которого используются компьютерная графика, инструменты ИИ и другие современные технологии; искусственно созданные виртуальные персонажи, опирающиеся на современные технологии имитации и создания изображения и голоса, используя понимание современных архетипов популярных персонажей и популярную психологию, создаваемые в виде двумерного или 3D-образа. За последние 10 лет технологии создания подобных «виртуальных звезд» становятся все популярнее – помимо виртуальных айдолов, в китайском шоу-бизнесе стали появляться виртуальные телеведущие, бойз-бенды и даже актеры. В китайской судебной практике уже имеются дела о защите голосов Лумин, виртуального айдола китайской компании – разработчика игр MiHoYo (Genshin Impact и др.), Хацунэ Мику, популярнейшего японского вокалоида-айдола, права на которого на территории Китая принадлежат компании Shanghai Xinchuanghua Culture Development Co., Ltd., и др. [18].

Однако для защиты синтезированного голоса виртуального персонажа в Китае необязательно даже признание их объектами авторского права, что особенно актуально для виртуальных персонажей, принадлежащих физическим лицам и используемых ими в коммерческих или даже личных целях. Еще в 2015 году Бэйлиньский районный народный суд города Сиань в решении по гражданскому делу Ма Лин против Кун Вэй № 05065 признал незаконное использование синтезированного голоса виртуального персонажа, принадлежащего физическому лицу, равносильным незаконному использованию голоса самого физического лица с соответствующими последствиями, а использование такого синтезированного голоса для озвучивания материалов, порочащих честь и достоинство, – нарушением права на честь и достоинство физического лица – владельца виртуального персонажа [19]. Судебная практика по данному вопросу довольна скудна (автору удалось найти лишь еще одно дело 2019 года с аналогичной позицией народного суда), однако по ней мы видим, что, помимо защиты голоса гражданина, в Китае развивается то, что можно было бы назвать «защитой голоса второго порядка», или «вторичной защитой голоса», что пока что трудно представимо, например, в российском законодательстве.

Мы видим, что сегодня голос человека рассматривается в российском законодательстве практически исключительно как биометрический параметр, но не как объект гражданского права, что, на наш взгляд, является исправимым недостатком российского правового поля. Возможно, российский законодатель может воспользоваться опытом китайских коллег и, уже видя конкретные варианты последствий принятия принципа защиты голоса по аналогии с защитой изображения в китайском законодательстве и правоприменении, добавить схожее положение в российское законодательство. Например, можно дополнить ст. 152.1 положением о регулировании отношений, связанных с защитой голоса, по аналогии; или добавить ст. 152.3, отдельно регулирующую данные отношения.

В конце 2023 года заместитель председателя совета по развитию цифровой экономики при Совете Федерации Артем Шейкин заявил, что наши сенаторы разрабатывают документ, который закрепит понятие «синтез голоса» при помощи искусственного интеллекта и ответственность за создание не согласованной с гражданином аудиодорожки.

С каждым годом количество ситуаций, требующих гражданско-правового регулирования личного неимущественного права физического лица на голос, становится все больше, а сами они становятся все разнообразнее. Мы уверены, что российская гражданско-правовая наука будет идти в ногу со временем и отвечать все новым запросам, которые перед ней ставит развитие современных технологий, и нам кажется, что мы можем рассматривать опыт Китая в отношении регулирования права человека на голос как одну из моделей развития нашего гражданского права.

Список литературы

1. ixbt.com: Тинькофф украл голос нейросетью? Актриса дубляжа требует с компании 6 млн рублей и вместе с другими актерами и дикторами добивается защиты от синтеза [Электронный ресурс]. URL: https://www.ixbt.com/news/2023/08/31/tinkoff-ukral-golos-nejrosetju-aktrisa-dubljazha-trebuet-s-kompanii-6-mln-rublej-i-vmeste-s-drugimi-akterami-i.html (дата обращения: 19.08.2024).

2. Брагина Е. К., Соколов С. С. Современные методы биометрической аутентификации: обзор, анализ и определение перспектив развития // Вестник АГТУ. 2016. № 61. С. 40–43.

3. Гражданский кодекс Китайской Народной Республики / отв. ред. П. В. Трощинский. М.: Синосфера, 2020

4. Гражданское решение первой инстанции по спору об ответственности за правонарушение в Интернете между Хэ Гохуаном и Shenzhen Sunshine Yinyi Technology Co., Ltd. // PKU Law [Электронный ресурс]. – URL: https://pkulaw.com/pfnl/95b2ca8d4055fce1b78930aca98f6fb2da7f5cba6d4dbe50bdfb.html (дата обращения: 19.08.2024).

5. Киселев А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2021. № 3.

6. Малеина М. Н. Личные неимущественные права граждан: понятие, осуществление, защита: дис. … д-ра юрид. наук. М., 1997.

7. Малеина М. Н. Право человека на индивидуальный голос и его защита // Юрист. 2015. № 13. С. 17–22.

8. Матвеев А. Г., Мартьянова Е. Ю. Гражданско-правовая охрана голоса человека при его синтезе и последующем использовании // Ex Jure. 2023. № 3. С. 118–131.

9. Музыкальная энциклопедия: [в 6 т.] / гл. ред. Ю. В. Келдыш. М.: Советская энциклопедия; Советский композитор, 1973–1982.

10. Сводный доклад Конституционной и правовой комиссии ВСНП об изменениях в разделе «Личные неимущественные права» проекта Гражданского кодекса // PKU Law [Электронный ресурс]. URL: https://pkulaw.com/protocol/8981d2f8dd57877201ca1e6cb622e277bdfb.html (дата обращения: 19.08.2024).

11. Уведомление Управления киберпространства Китая, Министерства общественной безопасности и Министерства торговли о выпуске «Мер по управлению маркетингом в режиме онлайн-трансляции (пробная версия) // PKU Law [Электронный ресурс]. URL: https://www.pkulaw.com/chl/4a8b4618e3ca74a6bdfb.html (дата обращения: 28.08.2024).

12. Ъ: Лебедева В., Литвиненко Ю. У дикторов крадут голоса [Электронный ресурс]. URL: https://www.kommersant.ru/doc/5785920 (дата обращения: 19.09.2023).

13. 宋海燕、肖漪涟 (Сун Хайянь, Сяо Илянь). **浅析** AI **克隆**艺人声音的侵权问题—**中美新近立法与司法**实践对比 (Краткий анализ проблемы нарушения прав при клонировании голосов артистов с помощью искусственного интеллекта. Сравнение последнего законодательства и судебной практики в Китае и США). Пекин: King & Wood Mallesons, 2024.

14. 张云燕、商子承、叶歆 (Чжан Юньянь, Шан Цзычэн, Е Синь). **我国首例** AI **生成声音人格**权侵权案评述 (Комментарий к первому в Китае делу о нарушении прав человека посредством использования голоса, созданного с помощью искусственного интеллекта). Пекин: Jincheng Tongda & Neal, 2024.

15. 杨立新、袁雪石 (Ян Лисинь, Юань Сюэши). 论声音权的独立及其民法保护 (О независимости права на голос и его защите гражданским правом) // **法商研究** (Юридические и коммерческие исследования). 2005. № 4.

16. 王绍喜 (Ван Шаоси). 《民法典》时代声音保护的解释与适用 (Толкование и применение защиты голоса в эпоху «Гражданского кодекса») // 法律适用 (Правоприменение). 2023. № 6. С. 35–42.

17. 王绍喜 (Ван Шаоси). 广告代言中“名人”的法律认定(Правовая идентификация «знаменитостей» в рекламных объявлениях) // 法律适用 (Правоприменение). 2017. № 17. С. 97–105.

18. 蒙晓阳、杜超凡 (Мэн Сяоян, Ду Чаофань). 虚拟偶像行业中声音侵权现象及其治理 (Феномен нарушения права на голос и распоряжение им в индустрии виртуальных айдолов) // 西南政法大学学报 (Вестник Юго-западного университета политики и права). 2021. № 5.

19. 颜卉 (Янь Хуэй). 算法驱动型虚拟数字人涉侵权纠纷的规范解决路径 (Пути решения споров о нарушении прав с участием виртуальных цифровых персонажей, управляемых алгоритмами) // 重庆大学学报（社会科学版）(Вестник Чунцинского университета (Общественные науки)). 2024. № 2. С. 182–186.

И. Ло,
магистрант,
Московский государственный юридический университет
имени О. Е. Кутафина (МГЮА)

ГОСУДАРСТВЕННОЕ УПРАВЛЕНИЕ БОЛЬШИМИ ДАННЫМИ: ОПЫТ КНР

Аннотация. В условиях построения цифрового государства управление большими данными является важной проблемой. В представленной статье анализируются основные теоретические проблемы и практические достижения в области государственного управления большими данными в Китайской Народной Республике. Статья содержит ряд выводов, представляющих практический интерес. Сделан обоснованный вывод о необходимости развития государственной Национальной платформы больших данных России, целью создания которой является использование преимуществ обработки больших данных для дальнейшего экономического роста российского государства, совершенствования системы государственного управления и улучшения качества жизни российских граждан.

Ключевые слова: цифровое государство, цифровое правительство, государственное управление, большие данные, применение технологий больших данных, платформы больших данных, управление данными, потоки данных, цифровые технологии

STATE MANAGEMENT OF BIG DATA THE CHNR EXPERIENCE

Abstract. In the conditions of building a digital state, big data management is an important problem. The presented article analyzes the main theoretical problems and practical achievements in the field of state management of big data in the People's Republic of China. The article contains a number of conclusions of practical interest. Thus, the author makes a reasonable conclusion about the need to develop the state National Big Data Platform of Russia, the purpose of which is to use the advantages of big data processing for further economic growth of the Russian state, improving the system of public administration and improving the quality of life of Russian citizens.

Keywords: Digital State, Digital Government, public administration, big data, application of big data technologies, big data platforms, data management, data flows, digital technologies

Определение понятия «государственное управление большими данными». Определение государственного управления в целом является общепринятым на международном уровне, и лишь в незначительных аспектах оно варьируется в зависимости от национального подхода.

Государственное управление – организующее воздействие государства на общество в ходе выполнения стоящих перед государством задач [1].

Согласно статье 107 Конституции КНР («县级以上地方各级人民政府依照法律规定的权限，管理本行政区域内的经济、教育、科学、文化、卫生、体育事业、城乡建设事业和财政、民政、公安、民族事务、司法行政、计划生育等

行政工作【中华人民共和国宪法第一百零七条】») [4], местные народные правительства всех уровней выше уездного управления в соответствии с установленными законом полномочиями осуществляют управление экономикой, образованием, наукой, культурой, здравоохранением, спортом, городским и сельским строительством, а также управление финансами, гражданскими делами, общественной безопасностью, национальными делами, судопроизводством и планированием семьи на своей административной территории.

Большие данные рассматриваются как новый вид стратегических ресурсов, позволяющих получить полную картину экономического и социального развития, точное прогнозирование и интеллектуальное принятие решений. В настоящее время существует общий консенсус относительно концепции больших данных, хотя по некоторым деталям еще ведутся споры.

Бывшее Главное управление по надзору за качеством, инспекции и карантину КНР и Управление по стандартизации КНР 29 декабря 2017 года выпустили национальный стандарт «Терминология больших данных в области информационных технологий» (GB/T 35295-2017), который официально введен в действие с 1 июля 2018 года. В стандарте указано, что большие данные – это «данные, содержащие большое количество наборов данных с такими характеристиками, как большой объем, разнообразные источники, чрезвычайно быстрая генерация, изменчивость и т. д., и трудно поддающиеся эффективной обработке традиционной архитектурой данных» [9].

Это определение больших данных, которое дается для области информационных технологий, может служить важным ориентиром для других областей. Для государственного управления большими данными принято считать данные, использующие множество методов сбора данных и интегрирующие множество источников данных, а также данные, методы и их технологическую интеграцию, которые обрабатываются и добываются с высокой скоростью с использованием современных информационных технологий и архитектур и которые обладают высокой степенью прикладной ценности и функциями поддержки принятия решений.

В теоретических работах выделяют следующие основные характеристики больших данных.

Большой объем данных. Размер наборов данных в человеческом обществе прошел путь от ГБ до ТБ, ПБ и даже до того, что они измеряются в ЭБ и ЗБ.

Большая прикладная ценность. После целенаправленного сбора, очистки и анализа большие данные имеют прикладное значение и поддерживают принятие государственных решений, работу бизнеса и общественное потребление.

Множество различных типов данных. Большие данные в основном включают структурированные, полуструктурированные и неструктурированные данные, такие как аудио-, видеоизображения, веб-журналы, информация о географическом положении и другие типы данных.

Высокая скорость генерации. Большие данные часто генерируются быстро в режиме реального времени в виде потоков данных. Широкое и глубокое применение мобильных телефонов, интернета вещей, планшетных компьютеров, мо-

бильного Интернета и различных датчиков создало удобные условия для повышения скорости производства больших данных. Обработка больших данных требует использования нетрадиционных технических средств, внедрения новой инфраструктуры, а также усилий по решению проблем, связанных с быстрыми вычислениями и хранением данных в реальном времени.

Согласно «非传统数据统计应用指导意见» – «Руководству по статистическому применению нетрадиционных данных КНР» (国统字【2017】160 号), выпущенному совместно Национальным бюро статистики и Национальной комиссией по развитию и реформам, большие данные являются объектом нетрадиционных данных. Основными отличиями его от традиционных данных являются (см. табл. 1)

Таблица 1

Сравнительные характеристики обычных и больших данных

Характеристики данных	**Традиционные данные**	**Большие данные**
Процесс генерации	Создается для выполнения заранее поставленной следственной задачи	Автоматически генерируется машиной, не для статистических целей
Тип данных	Структурированные данные	Неструктурированные данные
Метод выборки	На основе традиционных методов, таких как случайная выборка, стратифицированная выборка и др.	Вся совокупность является выборкой (чем больше данных, тем лучше)
Тип мышления	Причинность	Корреляция

Источник: [9].

Исходя из этого, мы понимаем, что большие данные – это только формирующийся инструмент государственного управления. Он обладает уникальными характеристиками по сравнению с традиционными средствами. Китайское правительство хочет, чтобы большие данные, являющиеся инструментом нового времени, придали новую силу его собственному государственному управлению. В связи с этим с 2017 года был разработан и выпущен ряд руководящих документов.

Теоретические основы и контекст использования больших данных в государственном управлении в Китае. Китай, как быстро развивающаяся международная сила в современную эпоху, обладает своим особым предвидением мирового развития. Уже в 2013 году китайские ученые начали обращать внимание на государственное управление большими данными.

В 2013 году китайский ученый Сунь Хунчао опубликовал в журнале «Экономика и информатизация Китая» статью «Сямэнь: большие данные для государственного управления» [5]. Это самая ранняя из найденных нами работ, посвященных государственному управлению с использованием больших данных в Китае. Поскольку это была первая опубликованная работа, понимание больших данных в ней было не таким глубоким и всеобъемлющим, как сейчас, и понимание государственного управления большими данными все еще оставалось на уровне «большие данные как направление трансформации данных для цифрового правительства». В настоящее время, с углублением исследований и практики, большие данные стали не просто данными, а важным инструментом принятия решений.

Но как первая научная работа по государственному управлению большими данными в Китае, ее новаторский и инновационный характер заслуживает восхищения.

На национальном уровне КНР придает большое значение государственному управлению большими данными в процессе цифровой трансформации государственного управления.

С тех пор как в 2014 году «большие данные» впервые появились в «Отчете о работе правительства», этот новый термин стал часто упоминаться, и вопросы на заседаниях Госсовета также неоднократно касались использования больших данных. В ходе коллективной учебы Политбюро ЦК Коммунистической партии Китая (КПК) председатель КНР Си Цзиньпин неоднократно подчеркивал важность больших данных.

«Большие данные должны использоваться для модернизации государственного управления. Необходимо создавать и совершенствовать механизмы поддержки принятия научных решений и социального управления с использованием больших данных, а также содействовать инновациям в моделях государственного управления и социального управления для достижения научного принятия государственных решений, точного социального управления и эффективного предоставления государственных услуг» [10], – отметил Си Цзиньпин 8 декабря 2017 года в ходе коллективной учебы.

До настоящего времени самым последним государственным документом по большим данным было «Руководство по созданию национальной интегрированной системы больших данных для государственных нужд» (далее – Руководство), выпущенное 28 октября 2022 года Госсоветом КНР [8].

В Руководстве подводятся итоги построения цифрового правительства и использования больших данных для государственного управления в Китае за последние годы, а также ставятся новые цели развития.

Функции управления государственными данными в Китае в основном четко определены, и с 2016 года Госсовет выпустил ряд программных документов, таких как «Временные меры по управлению совместным использованием государственных информационных ресурсов» (Guo Fa [2016] № 51) и «Мнения Главного управления Госсовета по созданию координационного механизма по созданию координационного механизма по совместному использованию государственных данных для ускорения продвижения упорядоченного совместного использования данных», с целью усиления разработки на высшем уровне, координации и продвижения работы по совместному использованию государственных данных и их применению.

Система государственных информационных ресурсов в основном сформирована. На базе национальной интегрированной платформы государственных услуг все регионы и ведомства собрали и обобщили более 3 млн каталогов государственных данных и более 20 млн информационных объектов.

Постоянно повышается базовая мощность экстранета национального электронного правительства: охват административных районов выше уездного уровня составляет 100 %, а поселков – 96,1 %.

Однако проблемы остаются. Так, наиболее важными в работе по государственному управлению большими данными являются открытость и мобильность данных на всех уровнях местного самоуправления.

Самые большие проблемы, с которыми сталкивается государственное управление большими данными, зачастую лежат не на техническом, а на институциональном уровне. Для государственного управления большими данными технический уровень проблемы в условиях бурного развития информационных технологий Интернета уже не является проблемой, но развитие системы имеет свое отставание. До наступления эры информационных технологий информация о государственном управлении хранилась в бумажном виде в архивах. После наступления информационной эры бумажная информация просто хранится в «информационном архиве». Обмен информацией между государственными ведомствами, равно как и между правительствами, не осуществлялся. Это привело к тому, что, хотя общий объем информационных данных очень велик, они изолированы друг от друга, и реализовать «унифицированные вычисления» больших данных невозможно, а ценность больших данных, соответственно, теряется.

В Руководстве отмечается, что государственные ведомства всех уровней находятся как под оперативным руководством вышестоящих органов, так и под управлением местных органов власти, поэтому необходимо уточнить полномочия и ответственность за управление государственными данными и упорядочить механизм координации. На низовом уровне все еще существуют проблемы дублирования данных, многократного ввода и плохой связности систем, что негативно сказывается на комплексном управлении и эффективном обмене правительственными данными. Трудно удовлетворить спрос на комплексный анализ межрегиональных, межведомственных и межуровневых данных, наблюдаются низкая степень открытости данных и недостаточное использование информационных ресурсов. Местный спрос на данные из вертикальной системы управления ведомств Госсовета является острым, а сложность возврата данных ограничивает применение цифровых инноваций в таких областях, как местное экономическое регулирование, рыночный контроль, социальное управление, государственные услуги и защита окружающей среды.

Руководство было выпущено с целью устранения упомянутых выше информационных проблем и создания Национальной единой платформы больших данных.

Примеры результатов практического применения государственного управления большими данными в Китае. Сегодня в КНР обработка и управление большими данными реализованы во многих системах управления отраслями экономики и социальной жизни.

1. Промышленность и торговля

Провинция Шаньси открывает «Платформу по предоставлению приложений для работы с большими данными для малых и средних предприятий провинции Шаньси» [7], опираясь на технологии больших данных, облачных вычислений и вертикальной поисковой системы.

Сервисная платформа предоставляет малым и средним предприятиям провинции в основном базовую информацию, такую как динамика развития промышленности, информация о спросе и предложении, информация о выставках, лидерах отрасли, инвестиционная информация, патентная информация, таможенная информация, информация о торгах, отчеты об отраслевых исследованиях, отраслевые данные и т. д. Она также предоставляет персонализированную и индивидуальную информацию в соответствии с различными потребностями предприятий, включая информацию о потребителях, конкурентах, сотрудниках, производстве, продажах и т. д., чтобы обеспечить информационную поддержку малых, средних и микропредприятий для всестороннего повышения их конкурентоспособности.

2. Транспортная отрасль

В октябре 2016 года муниципальные власти Ханчжоу совместно с компанией Aliyun обнародовали план создания в городе центра искусственного интеллекта – Hangzhou City Data Brain [2]. В основе «Городского мозга» будет использоваться технология ET AI компании AliCloud, которая сможет проводить глобальный анализ всего города в режиме реального времени, автоматически размещать общественные ресурсы, исправлять проблемы в работе города и в конечном итоге превратится в суперискусственный интеллект, способный управлять городом. «Мозг города» – первая попытка разгрузить городские пробки, которая уже была применена на дороге Shixin района Сяошань, где скорость движения автомобилей на некоторых участках увеличилась на 11 %.

3. Сфера образования

Муниципальное бюро образования города Сюйчжоу реализовало проект «Исследование анализа больших данных в образовании», целью которого является применение инструментов поиска данных и анализа обучения для получения, хранения, управления и анализа больших данных в образовании в режиме смешанного обучения, объединяющего онлайн-обучение и очное обучение, с целью создания принципиально новой системы оценки методов преподавания преподавателей и улучшения опыта преподавания и обучения [6].

На основе предыдущей работы необходимо использовать данные, систему показателей и инструменты анализа, имеющиеся в Центральном образовательном павильоне, для проведения поиска и анализа данных, создания единого хранилища данных о поведении преподавателей, прогнозирования текущих тенденций поведения преподавателей, предоставления услуг высокого уровня для «Учебно-методического класса города Сюйчжоу, поддерживаемого информационными технологиями», а также для создания системы и прикладных услуг, которые всегда отслеживаются и постоянно обновляются в соответствии с развитием реформ в области преподавания.

4. Сфера здравоохранения

Бюро здравоохранения нового района Пудун, являясь ведущим департаментом здравоохранения Шанхая, с помощью Microsoft SQL Server 2012 активно ис-

пользует большие данные для вывода информатизации здравоохранения и медицины на новый уровень: департамент здравоохранения может быстро выявлять инфекционные заболевания, проводить комплексное наблюдение за вспышками заболеваний с помощью базы данных медицинских карт жителей и электронных медицинских карт, охватывающих весь регион, а также благодаря интеграции процедур наблюдения за заболеваниями и реагирования на них, осуществлять оперативное реагирование. В то же время аналитика больших данных делает системы поддержки принятия клинических решений более интеллектуальными благодаря расширению возможностей анализа неструктурированных данных [3].

5. Метеорологические службы

Большие данные о землетрясениях и других стихийных бедствиях стали играть важную роль в случае стихийных бедствий, благодаря технологии больших данных будут выработаны рациональные и эффективные пути помощи при стихийных бедствиях [6]. Используя исторические метеорологические данные Метеорологического бюро и Сейсмологического бюро, исторические данные об изменениях туманностей, а также данные о городском планировании и жилищном строительстве Управления по обновлению городов, Бюро планирования и т. д., мы можем точно прогнозировать метеорологические изменения, находить оптимальные решения и планировать работу по ликвидации последствий чрезвычайных ситуаций и оказанию помощи путем построения модели оценки характера движения атмосферы и корреляционного анализа метеорологических изменений.

6. Охрана окружающей среды

Подход компании Microsoft к прогнозированию качества воздуха с помощью городских вычислений привел к запуску системы Urban Air – сервиса для мониторинга и прогнозирования качества воздуха с помощью больших данных, который охватывает более 300 городов Китая и был принят Министерством охраны окружающей среды КНР [11. С. 88–94]. Кроме того, Microsoft заключила контракты с некоторыми другими китайскими государственными организациями на предоставление необходимых услуг для различных городов и регионов. Технология позволяет прогнозировать качество воздуха на ближайшие 48 часов для городских агломераций Пекин – Тяньцзинь – Хэбэй, Дельта реки Янцзы, Дельта Жемчужной реки, Чэнду-Чунцин, а также для отдельных городов. В отличие от традиционного моделирования качества воздуха прогнозирование качества воздуха на основе больших данных опирается на подход машинного обучения, основанный на объединении данных из различных источников, т. е. прогнозирование качества воздуха основывается не только на данных о качестве воздуха, но и на данных из различных областей, таких как метеорологические данные, данные о транспортных потоках, данные о фабриках и горнодобывающей промышленности, структура дорожной сети города и т. д., которые накладываются друг на друга и дополняют друг друга, что позволяет прогнозировать качество воздуха.

7. Сфера культурного туризма

Провинция Шаньдун будет представлять собой систему общественной безопасности провинции, систему дорожного движения, статистическую систему, систему охраны окружающей среды, систему связи, более десяти секторов индустрии туризма, интеграцию элементов данных индустрии туризма провинции, раз-

работку платформы для мониторинга и управления операциями индустрии туризма. Благодаря управлению и анализу больших данных о туризме провинция Шаньдун сможет повысить уровень управления живописными местами, изучить туристические ресурсы провинции, разработать больше достопримечательностей для удовлетворения потребностей туристов, а также Nongjiale и другие услуги сельского туризма, что приведет к развитию живописных мест, особенно в сельских районах, к экономическому развитию [6].

Заключение. Развитие государственного управления большими данными в Китае началось в 2014 году, и спустя почти 10 лет совместных усилий теории и практики уже достигнуты определенные успехи. Хорошие результаты были достигнуты в различных сферах государственного управления промышленностью и торговлей [12], транспортом, здравоохранением, образованием, туризмом, метеорологией и других областях.

Тем не менее государственное управление большими данными в Китае остается несовершенным. Так, например, наблюдаются недостаточная циркуляция данных между различными уровнями власти и относительная изолированность данных между региональными органами управления; необходимо срочно укрепить способность гарантировать безопасность государственных данных, а после принятия таких законов и нормативных актов, как Закон КНР о безопасности данных, Закон КНР о защите персональной информации и Положение о защите безопасности критических информационных инфраструктур, необходимо срочно создать и усовершенствовать систему поддержки безопасности государственных данных; отсутствует единый реестр стандартов и норм в области данных.

Однако, к счастью, китайское правительство признало эти недостатки и сформулировало руководство по созданию единой национальной платформы больших данных, которое позволит продвинуться в государственном управлении большими данными в Китае еще дальше.

Изложенный выше опыт государственного управления большими данными в Китае, его результаты или недостатки могут послужить определенным ориентиром для России в процессе цифровой трансформации государственного управления.

Так, очевидна необходимость развития государственной Национальной платформы больших данных России, целью создания которой является использование преимуществ обработки больших данных для дальнейшего экономического роста российского государства, совершенствования системы государственного управления и улучшения качества жизни российских граждан.

Список литературы

1. Автономов А. С. Государственное управление // Большая российская энциклопедия: научно-образовательный портал. URL: https://bigenc.ru/c/gosudarstvennoe-upravlenie-d5248b/?v=5388368

2. Пэн Кофэн, 杭州城市大脑发布 阿里云人工智能 ET 宣战拥堵, 科学网 sciencenet.cn. URL: https://news.sciencenet.cn/htmlnews/2016/10/358247.shtm (дата обращения: 27.09.2023).

3. 上海市浦东新区人民政府,浦东史志办,信息化, 2022-06-30 . URL : https://www.pudong.gov.cn/008006035019/20220630/703542.html (дата обращения: 27.09.2023).

4. 中华人民共和国宪法 (Конституция Китайской Народной Республики: Электронная версия (2018). URL: https://www.gov.cn/guoqing/2018-03/22/content_5276318.htm (дата обращения: 27.09.2023).

5. 中国知网 : 孙宏超, 厦门:公共管理用上大数据, (CNKI : Сунь Хунчао, «Сямэнь: большие данные для государственного управления») . URL: https://chn.oversea.cnki.net/KCMS/detail/detail.aspx?dbcode=CJFD&dbname=CJFD2013&filename=YHJS201302049&uniplatform=OVERSEA&v=zDu_pEtZZUEW7FhBqFLN8tiwa29ZuIXr6YjP-ABQzhtp-iCwTO6fe1gas_ANLCPK (дата обращения: 27.09.2023).

6. 借助大数据应用平台 搭建"社会智能服务"新模式 (Построение новой модели «Службы социальной разведки» с помощью прикладной платформы больших данных) 中国信息协会大数据分会 China Information Industry Association Big Data Branch. URL: https://www.ciiabd.org.cn/articles/p9lmlk.html (дата обращения: 27.09.2023).

7. 北京海淀区人民政府信息公开平台 (Открытая информационная платформа Народного правительства района Хайдянь, Пекин) // URL: https://zyk.bjhd.gov.cn/jbdt/auto4488_51784/auto4488_52160/auto4488/auto4488_52179/201810/t20181003_3507379.shtml (дата обращения: 27.09.2023).

8. 国务院办公厅关于印发全国一体化政务大数据体系建设指南的通知 (Циркуляр Главной канцелярии Государственного совета об издании руководства по созданию национальной интегрированной системы больших данных для государственных дел) : 国办函〔2022〕102 号 Электронная версия (2022). URL: https://www.gov.cn/zhengce/content/2022-10/28/content_5722322.htm (дата обращения: 27.09.2023).

9. 政府统计中如何使用大数据 (Как использовать большие данные в государственной статистике) . URL: http://www.stats.gov.cn/zs/tjws/tjzn/202301/t20230101_1903936.html (дата обращения: 27.09.2023).

10. 新华网, 习近平 : 实施国家大数据战略加快建设数字中国 (Си Цзиньпин: реализовать национальную стратегию больших данных для ускорения создания цифрового Китая) . URL : http://www.xinhuanet.com//politics/2017-12/09/c_1122084706.htm (дата обращения: 27.09.2023).

11. 曾钰, 易敏, 陈贝贝, 龙睿, 文新宇, 湖南省生态环境遥感监测平台建设思考. 环境监控与预警, 2022, 14(3), 88-94. DOI: 10.3969/j.issn.1674-6732.2022.03.015. ZENG Yu, YI Min, CHEN Bei-bei, LONG Rui, WEN Xin-yu. Thinking on the Construction of Remote Sensing Monitoring Platform for Hunan Provincial Ecological

Environmental Monitoring. Environmental Monitoring and Forewarning, 2022, 14(3), 88–94.

12. Хашими С. К., Магоге Д. С. Правовое регулирование международной торговли криптографическими продуктами и технологиями: инструменты ВТО и региональные соглашения // Journal of Digital Technologies and Law. 2024. Т. 2, № 2. С. 328–344.

А. З. Махмутова,
студент,
Уральский государственный экономический университет

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ДЕЯТЕЛЬНОСТИ КООПЕРАТИВНЫХ ТРУДОВЫХ ПЛАТФОРМ КАК НОВОЙ МОДЕЛИ УСТОЙЧИВОЙ ЗАНЯТОСТИ В КОНТЕКСТЕ ЦИФРОВИЗАЦИИ

Аннотация. В данной статье анализируются особенности кооперативной организационной модели посредством использования информационных технологий, позволяющие кооперативному сектору создавать онлайн-сети и конкурировать с традиционными цифровыми платформами – платформенные трудовые кооперативы. В нынешней экономической реальности кооперативные платформы, обладающие социальной значимостью и основанные на принципах коллективного труда, стремятся удовлетворить потребности своих участников для разрешения экономических и социальных задач. Они представляют собой эффективный альтернативный путь для обеспечения устойчивой занятости по сравнению с цифровыми платформами гигантами-монополистами, которые нацелены в основном на максимизацию прибыли. Опираясь на опыт первых платформ совместного труда во Франции, в данной статье описываются характеристики кооперативных трудовых платформ и препятствия на пути их развития, включая правовые барьеры. В то же время автором определяются проблемы, которые необходимо решить для создания и эффективного функционирования кооперативных платформ, и обсуждаются возможные меры по поддержке новой организационно-правовой формы социального предпринимательства в рамках платформ совместного труда.

Ключевые слова: платформенные кооперативы, социальное предпринимательство, занятость, цифровизация, цифровые трудовые платформы

LEGAL SUPPORT OF COOPERATIVE LABOR PLATFORMS AS A NEW MODEL OF SUSTAINABLE EMPLOYMENT IN THE CONTEXT OF DIGITALIZATION

Abstract. This article analyzes the features of the cooperative organizational model through the use of information technology, allowing the cooperative sector to create online networks and compete with traditional digital platforms - platform labor cooperatives. In the current economic reality, cooperative platforms with social relevance and based on the principles of collective labor seek to meet the needs of their members to solve economic and social problems. They represent an effective alternative path for sustainable employment compared to the digital platforms of monopoly giants,

which are mainly focused on profit maximization. Drawing on the experience of the first cooperative labor platforms in France, this article describes the characteristics of cooperative labor platforms and the obstacles to their development, including legal barriers. At the same time, the author identifies the problems that need to be solved for the establishment and effective functioning of cooperative platforms and discusses possible measures to support a new organizational and legal form of social entrepreneurship within the framework of cooperative labor platforms.

Keywords: platform cooperatives, social entrepreneurship, employment, digitalization, digital labor platforms

Введение. Эпоха глобальной цифровизации сегодня охватывает многие аспекты социальной жизни общества и является неотъемлемой частью многих видов кооперативной деятельности. Согласно рассуждениям С. Г. Головиной [10. С. 296], цифровые трудовые платформы постепенно заменяются кооперативными платформами (далее также – платформенные кооперативы), которые воплощают идеалы кооперативной экономики и социального бизнеса. Эти платформы могут существовать в разнообразных организационно-правовых формах социального предпринимательства, в том числе как платформенные кооперативы [18], и объединяют в себе ценность предоставляемых услуг (через управление цифровыми платформами и приложениями) и ценность труда (через обеспечение устойчивой занятости участников) для достижения социально значимых результатов у всех участников кооператива.

Современная кооперативная трудовая платформа, по мнению кандидата экономических наук Е. А. Савельевой [12. С. 193], – это цифровая трудовая платформа по типу классического кооператива, которая использует новейшие технологии для веб-сайта, мобильного приложения или протокола, организованная на ее совместном владении работниками, пользователями и другими заинтересованными сторонами и имеющая такие характерные черты, как демократическое управление, справедливое распределение стоимости, инновации и устойчивость.

Эти кооперативы работают на основе норм, закрепленных в Конституции РФ (ст. 30 и 34) [1], Гражданском кодексе РФ (статьи 106.1–106.6) [2] и Федеральном законе от 8 мая 1996 года № 41-ФЗ «О производственных кооперативах» (далее – Федеральный закон № 41) [4].

В соответствии с гл. 106.1 ГК РФ производственный кооператив определяется как добровольное объединение граждан, которые вступают в него на основе членства с целью осуществления общей производственной или другой экономической деятельности. Это может включать в себя производство, обработку, реализацию товаров промышленного, агрокультурного и других видов, предоставление услуг [6, 7], торговлю [16], бытовое обслуживание и пр. Основание такого кооператива строится на личном труде и иных вкладах его членов, а также на их паевом взносе в общую собственность. Законодательство и устав кооператива могут предусматривать возможность участия в его работе и юридических лиц. Производственный кооператив представляет собой корпоративную коммерческую организацию. Аналогичное определение присутствует в Федеральном законе № 41, где в первой статье также дается схожее описание.

Иными словами, платформенные кооперативы, как и традиционные кооперативы, представляют собой коллективные структуры, которыми управляют их участники для совместного производства продукции, отвечающей потребностям и интересам общества, где происходит объединение функций владельца (арендодателя) и поставщика/потребителя, как утверждает Е. А. Юрманова [15. С. 161]. В отличие от традиционных кооперативов, которые существуют в реальном мире, платформенные кооперативы функционируют в Сети и обычно включают в себя участников онлайн-сообщества. Каждое усовершенствование и оптимизация технологии платформы способствуют ее многократному распространению и усилению.

Согласно ст. 4 Федерального закона № 41-ФЗ, для образования кооператива необходимо иметь не менее пяти участников. Важно отметить, что широкий спектр возможностей позволяет кооперативам развиваться и диверсифицировать свою деятельность, что способствует укреплению их позиций на рынке и повышению конкурентоспособности. В современных условиях кооперативы становятся все более востребованными и активно участвуют в различных отраслях экономики [14, 19].

Но, на наш взгляд, именно личный трудовой вклад участников, составляющих основу производственного кооператива, является ключевым условием деятельности артели как уникальной формы организации коллективного бизнеса. Хотя участие внешних пайщиков, заказчиков, наемных работников, посредников важно для жизнеспособности кооператива, все эти факторы не определяют природу производственных кооперативов и не должны приводить к размыванию характерных для артели демократических принципов управления и самоуправления, так называемой производственной демократии.

В соответствии с положениями ст. 4 Федерального закона от 24 июля 2007 года № 209-ФЗ (в редакции от 29.05.2024) «О развитии малого и среднего предпринимательства в Российской Федерации» [5] производственные кооперативы приравниваются к субъектам малого и среднего бизнеса наравне с хозяйственными обществами и хозяйственными товариществами. Важно отметить, что в отличие от хозяйственного товарищества, которое представляет собой объединение труда (за исключением вкладчиков коммандитного товарищества), и хозяйственного общества, которое является объединением капитала, производственный кооператив представляет собой союз труда и капитала: каждый участник кооператива обязан внести свой вклад в уставный капитал путем внесения паевого взноса и принимать активное участие в деятельности кооператива, вкладывая свой личный труд или иным образом поддерживая его функционирование.

Трудовая деятельность, осуществляемая членами кооператива, находит свое законодательное основание в нескольких нормативных актах, в числе которых Федеральный закон № 41 и устав кооператива. Касаясь трудовой деятельности работников, здесь ключевую роль играет Трудовой кодекс Российской Федерации [3]. В соответствии со ст. 19 данного закона, кооперативы обладают правом устанавливать форму и систему оплаты труда для своих членов и сотрудников самостоятельно. Вознаграждение за труд, выполненный в кооперативе, может быть выплачено как в денежной, так и в натуральной форме в соответствии с утвержденными правилами оплаты труда, установленными кооперативом. Это означает,

что кооператив имеет возможность определить способы и условия оплаты труда в соответствии со своими потребностями и особенностями деятельности. Важно отметить, что такой подход способствует созданию гибкой и адаптивной системы вознаграждения, которая соответствует специфике работы кооператива и интересам его участников.

Потенциал развития кооперативных трудовых платформ в России тесно связан с готовностью граждан организовывать совместную, регулируемую и демократически управляемую кооперативную деятельность. Основанные на использовании цифровых приложений и децентрализованных электронных сетей, такие платформы предоставляют участникам право голоса при принятии решений и содействуют сотрудничеству внутри кооператива. Важно, чтобы российские граждане проявляли заинтересованность в развитии подобных инициатив и активно участвовали в их реализации, что способствует укреплению кооперативного движения в стране.

Так, результаты социологического опроса, проведенного автором статьи среди студентов юридического факультета Уральского государственного экономического университета в 2024 году, показали, что 32 % респондентов предпочитают кооперативные трудовые платформы, где работники сами определяют политику платформы и финансируют ее развитие, а 68 % респондентов предпочитают традиционные трудовые платформы, где платформы сами устанавливают цены, а работники не влияют на их политику (рис. 1). В то же время в России 72 % респондентов предпочитают российские платформы дистанционной работы (рис. 2). Хотя в настоящее время эта форма организации труда недостаточно развита по сравнению с западными странами. Однако в России мы можем наблюдать конкретные инициативы в области межплатформенного сотрудничества (например, народный кооператив «Общее дело» для таксистов).

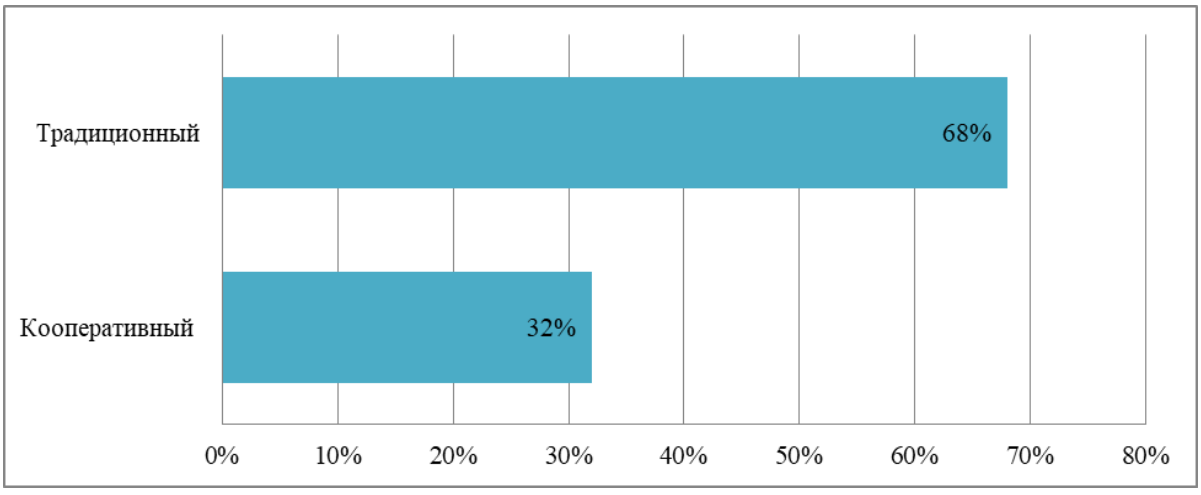

Рис. 1. Доли респондентов, ответивших на вопрос «Какой тип платформы фриланса стал бы для Вас предпочтительнее?»

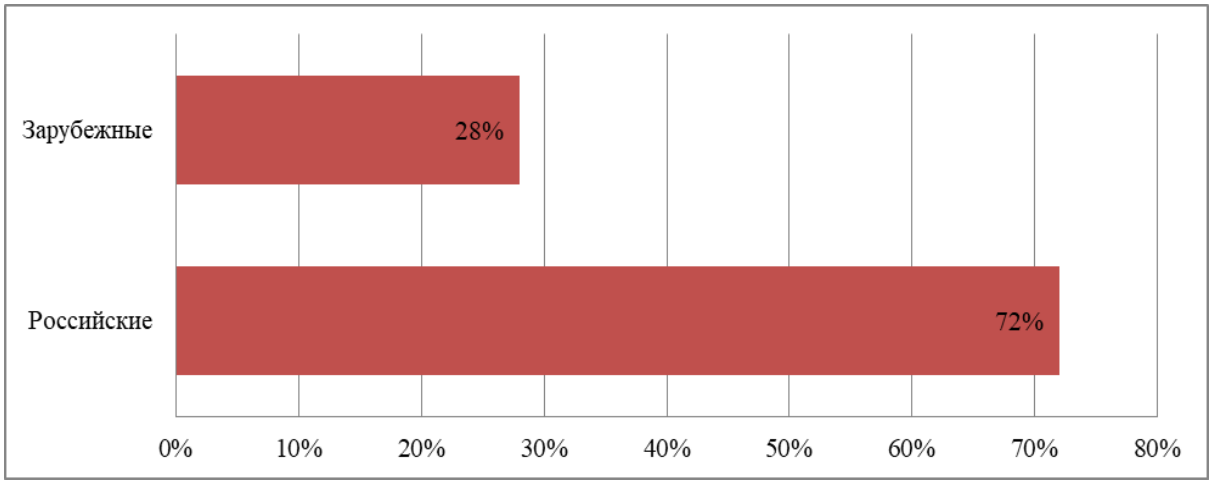

Рис. 2. Доли респондентов, ответивших на вопрос «Какие платформы фриланса для Вас предпочтительнее?»

Таким образом, кооперативные платформы способствует устойчивому развитию кооперативного сектора и обеспечивают более прозрачные и удобные условия для всех участников рынка. Основная цель этой платформы заключается в том, чтобы обеспечить более справедливые и демократичные условия для всех участников. Российским кооперативам предоставляется возможность быстрее находить клиентов, предлагать свои услуги и работы, а также устанавливать цены и согласовывать условия сделок. Благодаря кооперативной трудовой платформе кооперативы могут эффективнее контролировать выполнение условий договоров, следить за качеством предоставляемых услуг, организовывать бухгалтерский учет и выполнять другие важные функции.

Развитие платформ совместной работы тесно связано с владением бизнес-процессами, переводом персональных данных в личный информационный (цифровой) капитал. По мнению В. Н. Соловьевой, кооперативные трудовые платформы особенно значимы на местном уровне, поскольку предоставляют людям услуги, которые невозможно получить иначе, чем через кооперативы, а также обеспечивает социальную стабильность общества посредством создания предприятий, основанных на кооперативных принципах и ценностях [13. С. 443].

Сервис «Кооператив Онлайн» ПАО «Сбербанк», запущенный в 2020 г., являлся примером цифровой кооперативной деятельности, поскольку оцифровывал существующие бизнес-процессы кооператива и переводил в цифровой формат всю деятельность, например, организовывал взаимодействие членов кооператива (пайщиков) с кооперативом через личный кабинет, в том числе осуществлял сбор взносов, получал информацию о судебных исках и т. д.

Согласно Федеральному закону № 41, кооперативы обязаны вести бухгалтерский учет и отчетность, а также статистическую отчетность в соответствии с законодательством Российской Федерации, применяемым к коммерческим организациям. Кроме того, кооперативы должны предоставлять членам своего сооб-

щества доступ к судебным актам, касающимся споров, связанных с созданием кооператива, его управлением или участием в нем. Таким образом, кооперативы обязаны соблюдать не только финансовую дисциплину, но и обеспечивать прозрачность и доступность информации для своих членов, что способствует укреплению доверия и эффективному управлению внутри организации. Для принятия решений члены кооператива должны лично присутствовать на собраниях и предоставлять бумажный протокол о своем присутствии, а для вступления в члены кооператива нового пайщика необходимо личное присутствие участника и бумажное заявление от него. Данная платформа перестала функционировать в 2022 г., однако ее существование обеспечивало прозрачный и финансово безопасный процесс взаимодействия между кооперативом и потребителями, обращающимися к инструментам онлайн-покупок [11. С. 90].

Развитию кооперативных трудовых платформ препятствуют такие факторы, как отсутствие льгот для участников, неопределенная взаимосвязь между антимонопольным законодательством и кооперативными платформами, отсутствие возможности кредитных отношений между государством и кооперативом, несовершенство законодательной базы, неопределенный правовой статус работников платформ, их социальная незащищенность, вопросы контроля над персональными данными, а также, как отмечают в своей работе А. Н. Головина, Р. Ю. Левченко и К. П. Юрченко, степень доступа населения к сети Интернет и наличие цифровых навыков, без которых развитие цифрового кооперативизма маловероятно [9. С. 234].

Как и во многих других юрисдикциях, в России нет специальных законодательных положений о цифровых трудовых платформах. В настоящее время ключевой вопрос получения статуса платформенного работника решается в рамках судебной практики.

Так, в тех случаях, когда российским судам приходится определять статус работника платформы, применяется условный правовой тест с критериями для выявления наличия или отсутствия трудовых отношений. Пленум Верховного Суда РФ в своем Постановлении № 15 от 29 мая 2018 г. [7] подробно изложил эти критерии. Они включают в себя: договоренность между сторонами о том, что конкретный сотрудник выполняет определенные трудовые функции в интересах работодателя; условия труда, обеспечиваемые работодателем; выполнение трудовых обязанностей сотрудником за определенное вознаграждение; стабильность и устойчивость трудовых отношений; предоставление необходимых инструментов и оборудования; продолжительность трудовых отношений; стабильность трудовых связей; предоставление необходимых инструментов и оборудования и другие аспекты. Важно учитывать, что эти критерии играют ключевую роль в определении характера трудовых отношений между работником и работодателем.

Для обеспечения роста и развития кооперативных трудовых платформ имеет смысл активно работать над устранением различных препятствий, которые могут мешать им расцветать и становиться популярными. Кроме того, важно работать над улучшением общественного восприятия кооперативов, чтобы они стали более привлекательными и доверенными партнерами для широкой аудитории [17]. Только таким образом можно создать благоприятные условия для процветания кооперативных инициатив и их успешного развития в будущем.

Например, Франция поддерживает и поощряет появление кооперативных трудовых платформ как прямо, так и косвенно. Так, действует Всеобщая конфедерация кооперативов (CG Scop), которая объединяет в себе органы государственной власти, политические и экономические секторы, а также социальные институты. Их целью является участие в разработке законодательных актов и нормативных документов, касающихся кооперативного права. Scop – это не просто сеть, это целый мир возможностей. Она предлагает широкий спектр финансовых инструментов, способных обеспечить финансирование деятельности французских кооперативов. Среди них – долевые ссуды (Socoden), которые помогают организациям расти и развиваться, ценные бумаги (Scopinvest), открывающие новые горизонты для инвестиций, среднесрочные займы для финансирования инновационных цифровых компаний (CoopVenture) и многое другое. Таким образом, во Франции кооперативные трудовые платформы не просто существуют, они процветают благодаря поддержке и разнообразным финансовым возможностям, предоставляемым организациями типа Scop. В этой стране идеи превращаются в реальность, а потенциал каждого индивида находит свое отражение в разнообразных формах кооперации.

Исходя из предшествующего изложения, можно сделать вывод, что на протяжении длительного временного периода, даже в условиях сложной экономической, социальной и политической обстановки, кооперативы успешно формировали конкурентоспособные организации, способные адаптироваться к изменяющимся потребностям общества. Согласно мнению Е.А. Гатиной и Е. А. Астраханцевой, будущее кооперации связано с цифровой трансформацией [8. С. 26]. Однако для эффективного развития российских кооперативных трудовых платформ необходима поддержка со стороны государства и последовательная экономическая стратегия, направленная на превращение взаимодействия между платформами кооперации в отдельный, важный сектор современной российской экономики.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_28399 (дата обращения: 01.09.2024).

2. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ. 1994. № 32. Ст. 3301.

3. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 08.08.2024) // Парламентская газета. № 2–5, 05.01.2002.

4. О производственных кооперативах: Федеральный закон от 08.05.1996 № 41-ФЗ (ред. от 05.04.2021) // Собрание законодательства РФ. 1996. № 20.

5. О развитии малого и среднего предпринимательства в Российской Федерации: Федеральный закон от 24.07.2007 № 209-ФЗ (ред. от 29.05.2024) // СПС «КонсультантПлюс» [Электронный ресурс]. URL:

https://www.consultant.ru/document/cons_doc_LAW_52144/e74d46c9559d92ddcb907d7b1f144e698c099242 (дата обращения: 02.09.2024).

6. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_328854 (дата обращения: 01.09.2024).

7. Жарова А. К. О подходе к классификации информационно-технологических услуг // Государство и право. 2014. № 3. С. 32–38. EDN: SDFIQT

8. Гатина Э. А., Астраханцева Е. А. Цифровая повестка в деятельности Международного кооперативного альянса и современная практика кооперации // Вестник Российского университета кооперации. 2021. № 4(46). С. 23–27.

9. Головина А. Н., Левченко Р. Ю., Юрченко К. П. Новые контуры цифровой научно-технической кооперации // Экономика: вчера, сегодня, завтра. 2021. Т. 11, № 2А. С. 226–237. DOI: 10.34670/AR.2021.20.86.028

10. Головина С. Г. Международные практики развития цифровизации в кооперативной деятельности // Современные стратегии и цифровые трансформации устойчивого развития общества, образования и науки: сборник материалов IV Международной научно-практической конференции, Москва, 9 декабря 2022 года. М.: Алеф, 2022. С. 295–299.

11. Лихтанская О. И., Бакаева В. В., Сваровская Е. Б. Интернет-платформа как инструмент управления рынком торговых услуг в кооперативном секторе // Социально-экономическое развитие сельских территорий: тренды кооперации: сборник материалов Всероссийской (национальной) научно-практической конференции, Новосибирск, 1 ноября 2022 года / под ред. Л. П. Наговициной. Новосибирск: Сибирский университет потребительской кооперации, 2022. С. 86–91.

12. Савельева Е. А. Кооперативные трудовые платформы: трудности становления новых форм социального предпринимательства // Социальное предпринимательство и корпоративная социальная ответственность. 2021. Т. 2, № 3. С. 191–120.

13. Соловьева В. Н. На пути к кооперативизму // Междисциплинарная интеграция как двигатель научного прогресса: сборник материалов Международной научно-практической конференции, Новосибирск, 5 июня 2020 года. Ч. 1. Новосибирск: Сибирский университет потребительской кооперации, 2020. С. 442–448.

14. Чельцов М. В., Барсегян А. С., Кляузер В. А. Современные правовые проблемы кооперации и правовой статус их членов // Вестник Сибирского университета потребительской кооперации. 2021. № 2(36). С. 51–58.

15. Юрманова Е. А. Платформенные кооперативы в контексте цифровой экономики // Социально-экономические проблемы и перспективы развития трудовых отношений в инновационной экономике: материалы Всероссийской научно-практической конференции с международным участием, Омск, 22 апреля 2022 года / отв. редактор Е. А. Кипервар. Омск: Омский государственный технический университет, 2022. С. 157–165.

16. Елин В. М., Жарова А. К. Правовые аспекты торговли в сети интернет // Право и государство: теория и практика. 2012. № 10. С. 139–151. EDN: NVSBLB

17. Молинтас Д. Т. Соглашение о государственно-частном партнерстве в контексте матрицы оценки их юридических параметров и цифровизации // Journal of Digital Technologies and Law. 2024. Т. 2, № 2. С. 430–449. EDN: LVPIGR

18. Kickul J., Lyons T. Understanding Social Entrepreneurship: The Relentless Pursuit of Mission in an Ever Changing World. New York: Taylor & Francis, 2020. 374 p.

19. Кучина Я. Правовые подходы и методы регулирования финтеха в регионе Большого залива Гуандун – Гонконг – Макао // Journal of Digital Technologies and Law. 2024. Т. 2, № 1. С. 181–199.

Г. Г. Осипян,
студент,
Российский государственный университет правосудия,
Северо-Кавказский филиал

ПРИМЕНЕНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ ДЛЯ ИДЕНТИФИКАЦИИ ТЕЛ, ПОДВЕРГШИХСЯ ЭКСГУМАЦИИ

Аннотация. Эксгумация является сложным и неоднозначным следственным действием, природа которого остается в научной среде весьма спорной. Цель статьи – найти новые подходы к возможности идентификации эксгумированного трупа с помощью электронных цифровых реестров, использованию иных цифровых средств и способов фиксации полученной в результате данного следственного действия информации. Показана важность использования новых технологий для сохранения сведений, представляющих ценность для расследования преступления.

Ключевые слова: эксгумация, цифровые технологии, электронные реестры, идентификация, досудебное производство, следователь, суд

THE USE OF DIGITAL TECHNOLOGIES TO IDENTIFY BODIES THAT HAVE BEEN EXHUMED

Abstract. Exhumation is a complex and ambiguous investigative action, the nature of which remains highly controversial in the scientific community. The purpose of the article is to find new approaches to the possibility of identifying an exhumed corpse using electronic digital registers, using other digital means and methods of recording information obtained as a result of this investigative action. The author seeks to show the importance of using new technologies to preserve information of value for the investigation of a crime.

Keywords: exhumation, digital technologies, electronic registers, identification, pre-trial proceedings, investigator, court

Введение. В практической деятельности во время проведения следственных действий довольно часто возникают проблемы, связанные с отсутствием доказательств, необходимые для проведения дальнейшего расследования и поиска виновных лиц.

Наличие профессиональных знаний у специалистов, осуществляющих следственные действия, а также их четкое проведение в соответствии с процессуальным законодательством, по результатам которых определяется причастность лица к совершению противоправных деяний, – залог успеха любого расследования. Однако часто из-за тех изменений, которым подвергалось тело в процессе совершения преступления и последующего его захоронения, трудно идентифицировать эксгумированное тело.

Основная часть. В настоящее время в криминалистике довольно широко применяется цифровая и геномная идентификация. Между тем цифровые возможности позволяют также вести и использовать реестры неопознанных трупов.

Законодатель до сих пор не предоставил окончательные инструкции о порядке проведения эксгумации и упорядочении захоронения после нее с оцифровкой имеющихся данных. Это создает ряд практических проблем, требующих немедленного разрешения.

В проведении эксгумации принимают участие судебно-медицинский эксперт или, если это невозможно, квалифицированный врач, а также представитель администрации кладбища.

В настоящее время с имеющимися цифровыми возможностями и технологией искусственного интеллекта при надлежащем их правовом закреплении в УПК РФ [1] процедуру идентификации эксгумированных тел можно существенно упростить и сделать максимально эффективной.

При этом необходимо подчеркнуть, что проведение эксгумации неоднозначно с этической точки зрения, особенно для родственников потерпевшего [5. С. 245].

Факт давности захоронения, не играет существенной роли в возможности установления определенных обстоятельств смерти на основе костных останков.

Следует обратить внимание на то, что эксгумацию, так же как и получение образцов для сравнительного исследования, многие правоведы относят к действиям, имеющим вспомогательный характер [3. С. 210]. До сих пор этот вопрос не нашел своего разрешения. Но представляется, что эксгумация при определенных условиях может быть как основным, так и вспомогательным следственным действием [2; 4. С. 55].

Далее следователь фиксирует соответствующие данные в протоколе, также всю необходимую информацию о времени, месте проведения эксгумации. Необходимо отметить, что немаловажным аспектом при проведении эксгумации является обязательное требование законодателя о прикреплении к протоколу подробных фото- или видеодокументов, включающих в себя внешний вид могилы, положение гроба внутри нее, положение тела в гробу [6. С. 344], а также все действия, производимые участниками эксгумации.

Следует также отметить, что описание захороненного тела судебным медицинским экспертом либо квалифицированным врачом проводится также при проведении осмотра. Было бы рационально внести в УПК РФ изменения относительно обязательности использования этими лицами цифровых средств фиксации информации.

Заключение. Действующее уголовно-процессуальное законодательство РФ содержит пробелы и коллизии, требующие решения. В частности, по нашему мнению, необходимо конкретизировать возможность использования новых технологий с учетом морально-нравственных аспектов при осуществлении эксгумации, определить принципы ведения и формы обмена данными из разных электронных цифровых реестров, способствующих идентификации эксгумированных трупов в различных ведомствах.

Для наиболее эффективной регламентации представляется логичным внести уточнения в часть 3 статьи 178 УПК РФ, указав, что эксгумация должна осуществляться обязательно с применением цифровых средств фиксации информации.

Список литературы

1. Уголовно-процессуальный кодекс РФ (УПК РФ) от 18 декабря 2001 г. № 174-ФЗ // СПС «КонсультантПлюс».

2. Гаврилин Ю. В. Технологии обработки больших объемов данных в решении задач криминалистического обеспечения правоохранительной деятельности // Российский следователь. 2019. № 7. С. 3–8.

3. Кандакова Ю. А. Особенности производства эксгумации в уголовном процессе // Молодой ученый. 2021. № 21(363). С. 209–212.

4. Сергеев А. Б. Права и законные интересы участников уголовного судопроизводства: понятие, соотношение, степень правовой гарантированности. Постановка проблемы // Вестник Челябинского государственного университета. Серия: Право. 2022. Т. 7, № 2. С. 53–59.

5. Умярова Р. Р. К вопросу о судебном контроле за производством эксгумации при несогласии родственников // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4. С. 243–248.

6. Jonathan Cohen. Comprehensive Atlas of High-Resolution Endoscopy and Narrowband Imaging. New York, 2012. 344 p.

С. А. Сизикова,
студент,
Новосибирский национальный исследовательский
государственный университет

ПРАВОВЫЕ ПРОБЛЕМЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. В статье дается оценка проблемы абстрактности существующей легальной дефиниции персональных данных и ее применимости в условиях цифровизации, для этого в том числе проводится анализ различных видов персональных данных, возникших с развитием цифровых технологий. Также рассматриваются проблема соотношения больших данных (big data) и персональных данных, вопросы обработки персональных данных из публичных источников. На основании обобщенного анализа законодательства, правоприменительной практики

и доктрины разработаны критерии отличия персональных данных от иной информации, а также некоторые разъяснения, которые могут быть опубликованы в практических комментариях Верховного Суда РФ.

Ключевые слова: цифровизация, цифровые технологии, персональные данные, большие данные (big data), обработка, утечка данных, обезличивание данных

LEGAL PROBLEMS OF PERSONAL DATA PROCESSING IN THE CONTEXT OF DIGITALIZATION

Abstract. The article assesses the problem of the abstractness of the existing legal definition of personal data and its applicability in the context of digitalization, including the analysis of various types of personal data that have arisen with the development of digital technologies. The author also examines the problem of the relationship between big data and personal data, issues of processing personal data from public sources. Based on a generalized analysis of legislation, law enforcement practice and doctrine, the author has developed criteria for distinguishing personal data from other information, as well as some clarifications that can be published in the practical comments of the Supreme Court of the Russian Federation.

Keywords: digitalization, digital technologies, personal data, big data, processing, data leaks, depersonalization of data

Введение. Цифровизация – тенденция развития современной экономики и жизни человека в целом. Большое количество покупок, сервисов услуг перешло в онлайн-формат, что значительно облегчило ежедневную рутину и в то же время стало новым витком в развитии бизнес-процессов, рекламы. Для совершения практически любых операций в цифровом поле необходима регистрация или предоставление своих данных в том или ином объеме, т. е. почти любой сервис производит обработку персональных данных. Однако развитие технологий сопряжено также с повышением риска утечки таких данных. Например, по оценке Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, чаще всего жалобы о неправомерности обработки персональных данных поступают на действия владельцев сайтов (в том числе социальных сетей), кредитных организаций, ЖКХ, коллекторских агентств [6]. А в 2023 году в открытый доступ попало более 300 млн записей, содержащих персональные данные россиян [2]. Представляется, что данная проблема связана с неопределенностью категории персональных данных: существующее легальное определение не соответствует темпу развития технологий и не позволяет классифицировать новые разновидности данных, также цифровизация способствовала появлению новых важных особенностей обработки персональных данных, которые не отмечены ни в законодательстве, ни в практических разъяснениях Верховного Суда РФ.

Основная часть. Признаки персональных данных. На практике трудности возникают уже при решении вопроса отнесения тех или иных данных к персональным, судебная практика не сформировала единый подход, а существующая законодательная дефиниция не позволяет точно определить свойства обрабатыва-

емых в цифровом пространстве сведений. В судебной практике данные, позволяющие косвенно идентифицировать лицо, чаще всего признаются персональными в совокупности с другими сведениями, однако неясным остается вопрос о возможности признания их самостоятельной разновидностью персональных данных. Например, файлы cookies, хранящие информацию о действиях пользователя на сайте, были признаны персональными данными в деле социальной сети Linkedin, однако при регистрации на сайте обрабатывались еще и контактные, платежные и биографические данные, т. е. все сведения существовали в совокупности [7, 9].

Суд приходит к выводу, что в данном случае, в условиях сбора отчетности с предприятий при противодействии распространению Covid-19, сведения о температуре тела относятся к персональным данным, хотя в иных случаях они могли быть и не отнесены к такой категории.

Исследователи указывают на нелогичность законодательного определения персональных данных через категорию «информация», без должного уточнения признаков этой информации именно как данных [1]. Такой подход представляется некорректным с точки зрения практической деятельности. Цифровая среда изменчива, появляются новые разновидности персональных данных, и закрепить их все на законодательном уровне невозможно, так как такая норма быстро будет терять актуальность и перестанет отвечать требованиям существующей действительности.

Некоторые ученые, анализируя понятие и признаки персональных данных, обращают особое внимание на то, что персональные данные являются одной из составляющих неприкосновенности частной жизни гражданина [10].

Другие ученые обращают особое внимание на значение контекста для понимания значимости персональных данных. Так, под контекстом подразумевается свобода социальных связей человека, свобода общения с людьми [3]. Произвольное перемещение информации между контекстами может причинить вред. Причем Н. А. Дмитрик отмечает, что персональные данные как средство защиты частной жизни лица не должны его ограничивать или лишать права на оставление информации внутри контекста [3. С. 30]. Однако для закрепления в законодательстве понятие «контекст» не подходит, оно является разговорным и не имеет связи с правовой природой исследуемой категории. Скорее, справедливо указание на ограниченность получаемых сведений рамками определенной ситуации и обстоятельств.

Соотношение больших данных и персональных данных. Кроме того, на практике возникают проблемы разграничения так называемых больших данных и персональных данных. Категория больших данных не получила законодательного закрепления. Такая ситуация приводит к путанице и возможным злоупотреблениям в случае намеренного или случайного отнесения сведений лица вместо персональных данных к большим, работа с которыми должным образом не урегулирована. Стоит отметить, что разногласия возникают уже на этапе определения правовой природы больших данных. Это может быть связано с неким смешением данных – при обработке больших массивов информации техническими алгоритмами в общий поток данных могут попадать и персональные данные не всегда в обезличенной форме. Стоит обратить внимание, что персональные данные, полученные из социальных источников (социальных сетей, сайтов и пр.),

являются неотъемлемой частью больших данных и позволяют бизнесу значительно повышать качество принимаемых управленческих решений на основе детального анализа поведения потребителей. Представляется, что большие данные все же являются совокупностью огромных массивов информации и особых методов их аналитики и обработки, которая и позволяет развивать бизнес-процессы. Они не существуют отдельно в рамках технологии больших данных, иначе данная технология утрачивает смысл и свои основные преимущества. В своих более поздних работах А. И. Савельев приходит к выводу о том, что большие данные бывают двух видов: промышленные – показатели оборудования (температуры, давления и пр.) и пользовательские – данные о человеке [12]. Таким образом, логически формируется вывод о том, что персональные данные являются разновидностью больших данных. Большие данные, прежде всего, отражают информацию о клиентах в рамках предпочтений, наиболее популярного времени для покупок и прочих данных, которые позволяют настроить рекламные и коммерческие предложения, однако не раскрывают конкретные данные о личности клиента, которые позволили бы утверждать, что, к примеру, именно это лицо совершает больше всего покупок вечером пятницы.

Некоторые ученые обращают особое внимание на абсолютную недопустимость оборота персональных данных [13]. Представляется, что такой подход может значительно замедлить развитие технологий искусственного интеллекта, так как тренировка ИИ производится с помощью компиляций обезличенных сведений в особом формате. Стоит отметить, что разработка специального федерального закона о больших данных избыточна, однако разграничение больших данных и персональных данных необходимо.

Особенности обработки персональных данных при работе с большими данными. Большое значение в определении правомерности обработки данных пользователей из социальных сетей без их согласия имеет дело ООО «В Контакте» (далее – «ВКонтакте») против ООО «Дабл» (далее – «Дабл») – спор, который продлился более пяти лет, завершился заключением мирового соглашения и стал одним из самых обсуждаемых споров о персональных данных. В рассматриваемом случае взаимодействие с персональными данными рассматривается в контексте исключительного права на базу данных, однако судебное разрешение спора косвенно определило бы и судьбу парсинга социальных сетей. Под парсингом понимаются сбор и систематизация информации из открытых интернет-источников, в том числе и социальных сетей. Позиции судов различных инстанций по данному делу значительно отличались, а мировое соглашение в итоге не содержит информации о том, правомерны или неправомерны были действия «Дабл» по сбору и распространению сведений о пользователях социальной сети с их страниц. Судом первой инстанции в иске «ВКонтакте» было отказано, суд указал на недоказанность наличия базы данных пользователей; использования «Дабл» именно этих сведений; а также на отсутствие исключительного права «ВКонтакте» на базу данных в связи с тем, что изготовителем не были понесены затраты на создание такой базы – пользователи сами регистрировались и вносили сведения, необходимые на их взгляд [11]. Судом апелляционной инстанции решение первой инстанции было отменено, а требования «ВКонтакте» были удовлетворены частично. Помимо положений, противоположных указанным выше, в данном случае суд указывал еще

и на то, что, согласно лицензионному соглашению «ВКонтакте», воспроизведение, копирование, сбор, систематизация, хранение, передача информации из «ВКонтакте» в коммерческих целях или в целях извлечения базы данных или ее использования полностью или в любой части любым способом, не допускается [8]. Соответственно, сбор Дабл данных пользователей социальной сети и дальнейшее их распространение в своих продуктах без согласия субъектов персональных данных было неправомерно. Судом кассационной инстанции позиции судов первой и апелляционной инстанции не комментировались, производство по делу прекращено в связи с заключением мирового соглашения, что оставило без ответа вопрос о правомерности парсинга персональных данных из социальных сетей и иных открытых источников. Представляется, что сбор и систематизация общедоступной информации из социальных сетей должны допускаться для развития бизнеса, улучшения клиентского сервиса, однако недопустимо распространение таких сведений без согласия пользователей, а также использование персональных данных в коммерческих целях (для их дальнейшей продажи в том или ином виде).

Так, выводы о том, что распространение персональных данных, размещенных на общедоступных ресурсах, недопустимо без согласия субъекта, подтверждаются правоприменительной практикой. Например, согласно пользовательскому соглашению «ВКонтакте», другие пользователи социальной сети имеют доступ к данным, размещенным пользователем на его странице, однако это не наделяет этих лиц правом свободно распространять эти сведения в иных интернет-пространствах без согласия владельца страницы [4, 7].

Таким образом, дополнительному внесению ясности в проблему разграничения больших и персональных данных может способствовать закрепление в постановлении Пленума Верховного Суда РФ, к примеру, следующих положений: «В работе с технологиями, используемыми для обучения искусственного интеллекта, возможно использование персональных данных исключительно в анонимизированном виде, в противном случае на такие сведения распространяются правила, установленные Законом о персональных данных. Не допускается использование персональных данных без согласия субъекта таких данных».

Заключение. В условиях цифровизации работа с персональными данными сопровождается новыми вызовами, которые требуют не только практического, но и правового разрешения. Отмечается, что практика не сформировала единых подходов к вопросам отнесения данных к персональным, однако в большинстве случаев судебная практика позволит участникам гражданского оборота найти возможные примеры и в определенной степени уменьшить риски для предпринимателей путем контроля за обработкой с согласия субъекта таких категорий персональных данных, как номер банковского счета, файлы cookies и др.

Однозначно недопустимой является обработка персональных данных без согласия субъекта. В связи с использованием термина «большие данные» в кругах специалистов по работе с соответствующими технологиями, представляется, что эффективнее будет провести разграничение с персональными данными именно на уровне практики без введения новой терминологии в законодательство, т. е. важно дополнительно акцентировать внимание на следующем положении: «Для обучения искусственного интеллекта возможно использование персональных данных исключительно в анонимизированном виде».

Список литературы

1. Бундин М. В. Персональные данные в системе информации ограниченного доступа: дис. … канд. юрид. наук. М., 2017. С. 29–30.

2. В 2023 году в сеть утекло более 300 млн записей о россиянах // Информационное агентство ТАСС. URL: https://tass.ru/obschestvo/19693845 (дата обращения: 28.08.2024).

3. Дмитрик Н. А. Цифровая трансформация: правовое измерение // Правоведение. 2019. Т. 63, № 1. С. 28–46.

4. Определение Второго кассационного суда общей юрисдикции от 13 июля 2021 г. по делу № 88-15635/2021, 2-1712/2020. URL: Справочная правовая система «Консультант Плюс» (дата обращения: 26.08.2024).

5. Определение Московского городского суда от 10 нояб. 2016 г. по делу № 33-38783/2016. URL: Справочная правовая система «Консультант Плюс» (дата обращения: 01.09.2024).

6. Подведены итоги работы Роскомнадзора в 2021 году по защите прав и интересов граждан в сфере персональных данных // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: официальный сайт. URL: https://rkn.gov.ru/ (дата обращения: 28.08.2024).

7. Пользовательское соглашение ВКонтакте. URL: https://vk.com/terms?ysclid=lvtbonsb4q65548008 (дата обращения: 01.09.2024).

8. Жарова А. К. О подходе к классификации информационно-технологических услуг // Государство и право. 2014. № 3. С. 32–38. EDN: SDFIQT

9. Постановление Новоуральского городского суда Свердловской области № 5-239/2020 от 30 июля 2020 г. по делу № 5-239/2020. URL: https://sudact.ru/ (дата обращения: 30.08.2024).

10. Просветова О. Б. Защита персональных данных: дис. … канд. юрид. наук. М., 2005. С. 27–28.

11. Решение Арбитражного Суда города Москвы от 12 окт. 2017 г. по делу № А40-18827/2017. URL: https://kad.arbitr.ru (дата обращения: 26.08.2024).

12. Савельев А. И. Направления регулирования Больших данных и защита неприкосновенности частной жизни в новых экономических реалиях // Закон. 2018. № 5. С. 122–144.

13. Солдаткина О. Л. Проблемы сбора больших данных с позиции законодательства о персональных данных // Устойчивое развитие России: правовое измерение: сб. докладов X Московского юридического форума. В 3 ч. М., 2023. С. 178–180.

А. С. Сикач,
магистрант,
Дальневосточный федеральный университет
А. А. Бобылева,
студент,
Дальневосточный федеральный университет

ЗАКОНОДАТЕЛЬНАЯ БАЗА ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Аннотация. Рост сайтов, программ и социальных сетей является двигателем прогресса, но не все так радостно, как кажется на первый взгляд. Интернет дал свободу, но вместе с ним принес и новые угрозы в виде киберпреступности. Киберпреступность – это преступления, совершаемые в виртуальном мире, ставшие проблемой глобального масштаба. Расследование подобных преступлений усложняется использованием новых технологий для выявления компьютерных преступников. Статья фокусируется на анализе законодательной базы Российской Федерации в контексте использования искусственного интеллекта для борьбы с киберпреступностью. Особое внимание уделяется анализу последних изменений в законодательстве и практике за период 2021–2023 годы. Статья рассматривает ключевые аспекты и проблемы применения ИИ в сфере кибербезопасности и предупреждения киберпреступлений, а также проводит сравнительный анализ с международными подходами. На основе проведенного исследования актуальной темы приводится заключение.

Ключевые слова: искусственный интеллект, кибербезопасность, законодательство РФ, киберпреступность, федеральный закон, международный анализ, цифровой мир, компьютерные преступления, законодательная база, зарубежный опыт, Европейский союз, США, цифровизация, нейронная сеть

LEGISLATIVE FRAMEWORK OF ARTIFICIAL INTELLIGENCE IN THE FIGHT AGAINST CYBERCRIME

Abstract. The growth of websites, programs and social networks are the engines of progress, but not everything is as joyful as it seems at first glance. The Internet gave freedom, but along with it, it brought new threats in the form of cybercrime. Cybercrime is a crime committed in the virtual world that has become a global problem. Investigation of such crimes is complicated by the use of new technologies to identify computer criminals. The article focuses on the analysis of the legislative framework of the Russian Federation in the context of using artificial intelligence to combat cybercrime. Particular attention is paid to the analysis of the latest changes in legislation and practice for the period 2021-2023. The article considers the key aspects and problems of using AI in the field of cybersecurity and cybercrime prevention and also conducts a comparative analysis with international approaches. Based on the research conducted of the current topic, a conclusion is given.

Keywords: artificial intelligence, cybersecurity, Russian legislation, cybercrime, federal law, international analysis, digital world, computer crimes, legislative framework, foreign experience, European Union, USA, digitalization, neural network

Введение. Быстрое развитие цифровых технологий во всех направлениях науки и техники подталкивает рост организованной высокотехнологичной киберпреступности, отвоевывающей свои позиции в преступном мире. Киберпреступность в XXI в. представляет одну из наиболее серьезных угроз как для информационной безопасности государства, так и для его экономического развития, являясь одной из важнейших проблем современности. Искусственный интеллект применяют как для совершения преступлений, так и для его искоренения. С каждым годом уровень киберпреступлений постепенно растет, из-за чего требуется регулирование данного вопроса при помощи искусственного интеллекта. Разработка новых законов по данному вопросу позволяет эффективно нейтрализовать эту угрозу на определенное время, предотвратив угрозу безопасности персональных данных, да и информационной безопасности в целом.

Основная часть. Благодаря проведению мониторинга в области законодательства строится фундамент для эффективного разрабатывания новых принципов права, которые будут подталкивать к защите от компьютерных угроз, а также пополнению новых кадров специалистов по кибербезопасности. С этим могут помочь цифровые технологии, которые могут использовать как преступники, так и правоохранительные органы [6. С. 404–405].

Применение цифровых технологий и искусственного интеллекта способствует искоренению преступлений и вычислению преступников, невзирая на их местоположение и место проживания, но необходимо учитывать соблюдение этических норм, защиту персональных данных граждан [3, 8, 9].

Активное развитие законодательства в этой сфере требует постоянного изменения и мониторинга к возможностям, представляющимся искусственным интеллектом. Сюда входит подготовка новых кадров в сфере IT, и не только в сфере кибербезопасности [2. С. 1055].

Основным аспектом ИИ в сфере кибербезопасности является способность автоматизировать и оптимизировать процессы, которые традиционно выполнялись вручную. Сюда входят мониторинг сетевой активности, анализ угроз, обнаружение вредоносных программ и реагирование на инциденты кибербезопасности. Системы ИИ способны быстро адаптироваться к изменениям в инфраструктуре и корректировать параметры безопасности, что особенно важно в условиях постоянно развивающихся компьютерных угроз и технологических изменений [1. С. 9].

Постоянный мониторинг специалистами приводит к понижению работоспособности, а искусственный интеллект является цифровым помощником, помогающим в фильтрации и определении приоритетности этих уведомлений, повышая эффективность работы специалистов по кибербезопасности.

Правовой анализ зарубежных государств о роли искусственного интеллекта в борьбе с киберпреступностью фокусируется на различиях и сходствах законодательных подходов. Соединенные Штаты, Европейский союз и Китай являются пионерами в разработке правовой базы для использования ИИ в контексте кибербезопасности.

В Соединенных Штатах децентрализован подход к регулированию ИИ в сфере кибербезопасности, который во многом зависит от инициатив частного

сектора. Законы Калифорнии, такие как Закон Калифорнии о конфиденциальности потребителей (CCPA), содержат рекомендации по вопросам конфиденциальности и безопасности данных, важных для ИИ в сфере кибербезопасности [5. С. 70].

Европейский союз решает этот вопрос более систематически и устанавливает строгие требования к обработке данных, в том числе данных, используемых системами искусственного интеллекта. GDPR требует от организаций принимать соответствующие меры для защиты данных от киберугроз, что влияет на использование ИИ в сфере кибербезопасности [4. С. 38].

В Китае более централизован подход к использованию ИИ в сфере кибербезопасности. Правительство Китая активно вмешивается в разработку и внедрение ИИ посредством различных правительственных инициатив и законов, таких как Закон Китая о кибербезопасности, который требует от компании обеспечивать безопасность данных и сети.

Подход РФ к регулированию ИИ сконцентрирован на разработке и поддержке его использования, в отличие от строгих нормативных ограничений в ЕС.

Во-первых, это обеспечение конфиденциальности, требующее досконального обеспечения защиты личных данных.

Во-вторых, это дискриминация, увеличивающая риск в обработке баз данных.

В-третьих, ответственность, возникающая насчет использования искусственного интеллекта в обеспечении кибербезопасности и ответственности лица в его использовании.

В-четвертых, законность, в рамках которой используется искусственный интеллект с соблюдением норм законодательства во избежание негативных последствий.

В-пятых, достоверность данных, требующая обеспечения точности данных при использовании ИИ во избежание серьезных последствий.

В-шестых, защита персональных данных, требующая усиления защиты ИИ от взлома злоумышленниками в те или иные объекты для совершения взломов систем.

Вызовы и перспективы применения искусственного интеллекта в борьбе с киберпреступностью рассматриваются с разных точек зрения:

1. Сложное приспособление. Компьютерные злоумышленники постоянно совершенствуют новые методы совершения цифровых преступлений.

2. Недостаточность данных. Для большего искоренения преступности необходимо больше данных о компьютерных преступлениях, не имеющих доступа к ним из-за конфиденциальности.

3. Вопросы этики. Они касаются неприкосновенности частной жизни и ее нарушения.

Невзирая на вызовы, искусственный интеллект представляет больше перспектив в его использовании:

1. Автономное обнаружение компьютерных атак. Искусственный интеллект способен обнаружить угрозу за менее 1 минуты, что помогает эффективно искоренять источник его возникновения.

2. Анализ огромного объема данных. Позволяет ИИ обрабатывать большие объемы данных для идентификации паттернов и трендов в компьютерных угрозах.

3. Прогнозирование угроз. Использование ИИ позволяет предвидеть возникновение угроз для принятия мер предосторожности.

Анализ законодательной базы РФ, связанной с применением искусственного интеллекта для противодействия киберпреступности, выявил значительные шаги в правовом регулировании данной сферы. Российское законодательство, включая Федеральный закон от 24 апреля 2020 г. № 123-ФЗ и Указ Президента от 10 октября 2019 г. № 490, акцентирует внедрение ИИ в систему кибербезопасности, но требует постоянной адаптации к изменяющейся технологической среде. При анализе использования ИИ для предотвращения киберпреступности было показано, что ИИ способен решать проблемы, которые для человека сложны из-за объема и сложности данных. Эффективность использования ИИ в сфере кибербезопасности значительно повышает способность системы предотвращать, обнаруживать угрозы и реагировать на них в режиме реального времени. Подход Российской Федерации направлен на сбалансированную поддержку развития искусственного интеллекта и обеспечения кибербезопасности. Особое внимание уделяется адаптации законодательства к угрозам в киберпространстве и развитию технологий ИИ.

Список литературы

1. Абдуллаев Э. А. Кибербезопасность: вызовы и стратегии защиты в цифровую эпоху // Молодой ученый. 2023. № 33(480). С. 8–9.

2. Азизов А. А., Хорошилов А. С. Перспективы использования современных информационных технологий в криминалистике, направленных на эффективное раскрытие киберпреступлений // Вопросы российской юстиции. 2020. № 9. С. 1052–1060.

3. Владимир Путин в режиме видеоконференции принял участие в основной дискуссии конференции по искусственному интеллекту Artificial Intelligence Journey (AI Journey 2020) на тему «Искусственный интеллект – главная технология XXI века» // Президент России. 2020, 4 декабря. URL: http://www.kremlin.ru

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

5. Журтов А. Б. О новых методах противодействия киберпреступности в современных условиях // Журнал прикладных исследований. 2023. № 5. С. 68–72.

6. Сикач А. С. Роль искусственного интеллекта в расследовании преступлений // Технологии XXI века в юриспруденции: материалы Пятой международной научно-практической конференции, Екатеринбург, 19 мая 2023 года. Екатеринбург: АНО «Центр содействия развитию криминалистики «КримЛиб», 2023. С. 404–413.

7. О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»): Указ Президента РФ от 10.10.2019 № 490 [Электронный ресурс]. URL: https://www.consultant.ru

8. Motives and Objectives of Crime Commission Against Information Security / A. Yu. Bokovnya [et al.] // Ad Alta. 2020. Vol. 10, № 2 S13. Pp. 7–9. EDN: SCSEBN

9. О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных»: Федеральный закон от 24.04.2020 № 123-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_351127/

10. Концепция цифрового государства и цифровой правовой среды: монография / под общ. ред. Н. Н. Черногора, Д. А. Пашенцева. М.: ИЗиСП: Норма: ИНФРА-М, 2024.

А. С. Сикач,
магистр,
Дальневосточного федерального университета
Е. В. Рубанов,
студент,
Российский университет дружбы народов
имени Патриса Лумумбы

ПРОБЛЕМЫ МАШИНОЧИТАЕМОГО ПРАВА

Аннотация. Машиночитаемое право исследует применение информационных технологий в сфере права с целью обеспечения эффективной обработки и использования правовой информации. Машиночитаемое право представляет собой использование компьютерных алгоритмов для создания машиночитаемых версий правовых документов. У машиночитаемого права имеются преимущества, такие как повышенная точность, анализ правовых норм, ускорение процессов поиска и анализа правовой информации, а также возможность создания автоматических систем управления правовыми процедурами.

Ключевые слова: машиночитаемое право, автоматизация права, искусственный интеллект, машинное обучение, нормативно-правовые акты, правотворчество, сравнительно-правовой анализ, база данных, информационные технологии, алгоритмы

PROBLEMS OF MACHINE-READABLE LAW

Abstract. Machine-readable law explores the application of information technology in the field of law, in order to ensure the effective processing and use of legal information. Machine-readable law is the use of computer algorithms to create machine-readable versions of legal documents. Machine-readable law has advantages, such as increased accuracy in the analysis of legal norms, acceleration of the processes of searching and analyzing legal information, as well as the possibility of creating automatic systems for managing legal procedures.

Keywords: machine-readable law, automation of law, artificial intelligence, machine learning, normative legal acts, law-making, comparative legal analysis, database, information technologies, algorithms

С появлением новых возможностей, с развитием НТП в разные области человеческой жизнедеятельности внедряются новые технологии. Правотворчество – сложный процесс создания норм, регулирующих общественные отношения. Для успешной реализации этой деятельности человек должен обладать специальными знаниями в таких областях, как теория права, юридическая техника, практика применения правовых норм, формальная логика, экономика и т. д. При создании законов возникают трудности из-за невозможности предвидеть все аспекты и последствия их реализации. В связи с этим было бы большим упущением не использовать достижения НТП и не внедрять новые технологии. Одной из таких технологий является машиночитаемое право, которая позволит облегчить работу юристам.

Существует множество научных трудов и правовых актов [2. С. 101], посвященных машинизации права. Мнения по этому вопросу различны, но стоит более детально рассмотреть плюсы и минусы автоматизации и машинизации права.

Идея создания машиночитаемого права давно присутствует среди исследователей. Так, Р. Сасскинд полагал, что «…юридическая практика и отправление правосудия в завтрашней правовой парадигме больше не будут во власти бумажных и печатных форм. Вместо этого правовые системы информационного общества быстро разовьются под значительным влиянием как никогда более мощных информационных технологий» [5. С. 292]. Неоспоримо, за последние три десятилетия общество и право претерпели значительные изменения, которые влияют на разные области общественной жизни. Этот прогресс продолжается и сегодня, охватывая широкий круг вопросов и вызовов. Сегодня мы можем наблюдать рост интереса к использованию машиночитаемого права не только со стороны юристов, но и со стороны бизнеса и государства. Это связано с тем, что такие технологии позволяют значительно сократить время на поиск и анализ правовой информации, а также уменьшить вероятность ошибок. Одним из самых важных направлений развития машиночитаемого права является создание специализированных программ, способных автоматически анализировать большие объемы юридической информации. Такие программы уже сегодня используются для автоматизации процессов подготовки документов, проверки соответствия действующему законодательству и мониторинга изменений в законодательстве.

Автор в данной статье рассматривает возможность внедрения машиночитаемого права в правовое поле Российской Федерации. Существует несколько определений для данной технологии. Данная область только развивается, поэтому конкретной терминологии пока что нет. Только с развитием вычислительных технологий стало возможным внедрение данной системы. Унифицированные правила могут упростить процесс создания и реализации правовых норм унификации (от лат. unio – «единство» и facere – «делать» (толковый словарь Ушакова)).

Машиночитаемое право, или LegalTech, – это сфера, которая активно развивается и привлекает все больше внимания специалистов из различных областей.

Возможности использования технологий в правовой сфере становятся все более разнообразными и широкими, что открывает перед нами огромные перспективы.

Одной из основных тенденций в развитии машиночитаемого права является увеличение эффективности юридических процессов за счет автоматизации и оптимизации работы юристов. Это позволяет существенно сократить время, затрачиваемое на подготовку документов, поиск необходимой информации и анализ сложных юридических вопросов.

Благодаря использованию технологий в правовой сфере возникает возможность создания новых сервисов и продуктов, способных упростить процесс оказания юридических услуг как для юристов, так и для клиентов.

Одним из самых важных направлений развития машиночитаемого права является создание специализированных программ, способных автоматически анализировать большие объемы юридической информации. Такие программы уже сегодня используются для автоматизации процессов подготовки документов, проверки соответствия действующему законодательству и мониторинга изменений в законодательстве.

Другим важным направлением развития машиночитаемого права является углубленный анализ внутри айсберга. Это означает использование технологий и методов искусственного интеллекта для выявления скрытых закономерностей и трендов в юридической информации, которые могут быть невидимы на первый взгляд. Такой подход позволяет более точно предсказывать развитие событий и принимать более обоснованные решения.

Автоматизация права – сложный процесс, требующий значительных усилий и финансовых затрат. Это включает в себя создание машиночитаемой системы, для чего необходимо разработать технические и программные механизмы, а также внести изменения в юридическую технику. Несмотря на сложности, комплексная машинизация права будет значительным достижением. В разных юрисдикциях мира уже обсуждаются вопросы автоматизации права и создаются специальные платформы, такие как X-Road, позволяющие упростить обмен данными между государственными органами. Эта система уже успешно функционирует в нескольких странах, таких как Эстония, Финляндия, Япония, Азербайджан, Намибия, обеспечивая эффективное взаимодействие между разными информационными системами [15].

В США успешно функционирует система электронного правосудия, дающая стране лидерство в этой области, как отмечают С. Г. Рогожина и Н. С. Щербинина [12. С. 89]. Эти системы предоставляют удобный способ взаимодействия с судебной системой и управления делами, обеспечивая прозрачность и доступность информации [14]. PACER обеспечивает круглосуточный доступ к материалам дела и онлайн-просмотр документов.

Применение технологий машиночитаемого права значительно изменяет работу с юридическими документами, переводя текст в цифровую форму и программный код.

При переводе юридического текста в информационно-технологическую плоскость осуществляются анализ норм, смыслов слов и подтверждение действий людей. Информационная система может предварительно анализировать действительность и формировать правовые тексты на основе выведенных зависимостей.

Отечественные информационные системы могут создавать правовые тексты автоматически, а также проводить анализ правоприменительной практики с помощью цифровых технологий.

Машиночитаемое право как явление характеризуется следующими основными чертами: возможностью обработки правовых норм, алгоритмизацией правил, использованием информационных систем и соблюдением легальности.

Характеристики цифровизации правовой сферы включают обрабатываемость норм с помощью цифровых технологий. Легальность машиночитаемого права зависит от признания системы сторонами или нормативным актом, будь то корпоративные правовые системы или единая информационная система в сфере закупок.

В ближайшем будущем можно ожидать дальнейшего увеличения объема применения машиночитаемого права в различных сферах: от юриспруденции и юридических консультаций до юридической аналитики и работы юридических отделов корпораций. Машиночитаемое право открывает перед нами огромные перспективы для развития юридической сферы и повышения качества предоставляемых юридических услуг. Технологии машинного обучения и искусственного интеллекта становятся неотъемлемой частью работы юристов и позволяют существенно улучшить эффективность и качество правовой помощи. В ближайшем будущем можно ожидать дальнейшего роста интереса к LegalTech и появления новых инновационных решений, способных изменить ландшафт юридической сферы навсегда.

Заключение. Таким образом, машиночитаемое право представляет собой перспективное направление развития правовой сферы. Перспективы и тенденции развития машиночитаемого права обещают значительное углубление и расширение функциональности таких технологий, что открывает новые возможности для эффективного и точного анализа юридической информации. Применение технологий машинного обучения и искусственного интеллекта в обработке правовой информации значительно упрощает и повышает эффективность работы юристов и других специалистов в области права. Машиночитаемое право способствует автоматизации процессов обработки правовых норм, а также повышению точности и надежности их интерпретации. Однако для успешной реализации концепции машиночитаемого права необходимо решить ряд технических, этических и юридических вопросов, связанных с обработкой больших объемов данных, защитой персональной информации и ответственностью при автоматическом принятии решений.

Список литературы

1. Дремлюга Р. И., Дремлюга О. А. Искусственный интеллект – субъект права: аргументы за и против // Правовая политика и правовая жизнь. 2019. № 2. С. 120–125.

2. Заметина Т. В., Комбарова Е. В. Искусственный интеллект и конституционные вопросы его внедрения в современной России // Правовая политика и правовая жизнь. 2021. № 1. С. 180–189.

3. Бегишев И. Р. Криминологическая классификация роботов: риск-ориентированный подход // Правоприменение. 2021. Т. 5, № 1. С. 185–201. EDN: TBUVGY

4. Зорькин В. Д. Право будущего в эпоху цифр. Индивидуальная свобода или сильное государство? // Российская газета. URL: https://rg.ru/2020/04/15/zorkin-pravo-budushchego-eto-te-zhe-vechnyecennostisvobody-i-spravedlivosti.html (дата обращения: 05.12.2020).

5. Кашкин С. Ю., Тищенко С. А., Алтухов А. В. Правовое регулирование применения искусственного интеллекта для борьбы с распространением COVID-19: проблемы и перспективы с учетом мирового опыта // Lex Russica (Русский закон). 2020. Т. 73, № 7. С. 105–114.

6. Конференция Artificial Intelligence Journey (AI Journey 2020) на тему «Искусственный интеллект – главная технология XXI века». URL: http://kremlin.ru/events/president/news/64545 (дата обращения: 05.12.2020).

7. Концепция развития технологий машиночитаемого права (утв. Правительственной комиссией по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 15.09.2021 № 31).

8. Концепция развития технологий машиночитаемого права (утв. Правительственной комиссией по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 15.09.2021 № 31) [Электронный ресурс]. Доступ из системы ГАРАНТ // ЭПС «Система ГАРАНТ».

9. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации. 2017. № 41. Ст. 5700.

10. О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ от 10 октября 2019 г. № 490 (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года) // Собр. законодательства Рос. Федерации. 2019. № 20. Ст. 2901.

11. 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.

12. Рогожина С. Г., Щербинина Н. С. «Электронное правосудие»: сравнительно-правовой анализ // Журнал юридических исследований. 2020. № 3. С. 86–91.

13. Цифровые помощники позволят сократить количество ошибок в работе адвокатов и судей // Коммерсантъ. 2021. URL: https://www.kommersant.ru/doc/5049048 (дата обращения: 30.10.2021).

14. Case Management / Electronic Case Files. // PACER Public Access to Court Electronic Records. URL: https://www.pacer.gov/cmecf/ (дата обращения: 28.10.2021).

15. X-Road Платформа межгосударственного обмена данными // TADVISER: Государство. Бизнес. Технологии. 2018. URL: https://www.tadviser.ru/index.php/Статья:X-Road_Платформа_межгосударственного_обмена_данными (дата обращения: 29.10.2021).

А. Ю. Таначева,
магистрант,
Санкт-Петербургская академия
Следственного комитета Российской Федерации

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ТЕЛЕГРАМ КАК СПОСОБ ПРОФИЛАКТИКИ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ

Аннотация. В представленной статье исследуются такие проблемные вопросы, как особенности идентификации пользователей социальной сети «Телеграм» в качестве способа профилактики правонарушений. Выделены инструменты идентификации пользователей. Изучены особенности правового регулирования в представленной области, сформулированы выводы, рассмотрены риски и угрозы использования социальной сети, вопросы безопасности.

Ключевые слова: телеграм, идентификация, пользователь, законодательство, шифрование, цифровизация, цифровые платформы

IDENTIFICATION OF TELEGRAM USERS AS A WAY TO PREVENT ILLEGAL ACTIONS

Abstract. This article examines such problematic issues as the features of identifying users of the telegram social network as a way to prevent crime. User identification tools are highlighted. The features of legal regulation in the presented area are studied, conclusions are formulated, the risks and threats of using the social network, and security issues are considered.

Keywords: Telegram, identity, user, legislation, encryption, digitalization, digital platforms

Введение. Современное общество большинство исследователей называют не иначе как информационным, все большее количество людей проводят большое количество времени за обработкой информации в тех или иных целях. В Интернете пользователи работают, развлекаются и, к сожалению, совершают противоправные действия или становятся жертвами таких действий. В настоящее время наблюдается активное использование мессенджера «Телеграм» (Telegram) в России и странах бывшего Советского Союза.

Основная часть. Телеграм является кроссплатформенной системой мгновенного обмена сообщениями, функциями обмена текстовыми, аудио- и видеосообщениями, а также иными файлами различных форматов. Кроме того, телеграм позволяет осуществлять аудио- и видеозвонки, организовывать многопользовательские каналы и группы.

Идея создания данного мессенджера пришла Павлу Дурову в 2011 году. 14 августа 2013 года был представлен первый клиент телеграм для устройств на платформе iOS протокола Диффи – Хеллмана для обмена 2048-битными RSA-ключами между двумя устройствами и ряда хеш-функций. Протокол допускает использование шифрования end-to-end с опциональной сверкой ключей. Мессенджер имел следующий слоган: Taking back our right to privacy – «Возвращаем свое право на неприкосновенность личной жизни».

При этом имеются различия в функциях, так, например, при использовании телеграм на мобильных устройствах, являющихся основными для данного мессенджера, на них доступны все ключевые функции, включая чаты, группы, каналы, аудио- и видеозвонки, стикеры и GIF-изображения. Также возможен обмен мультимедиа, так как у приложения имеется доступ к файлам, хранящимся в памяти устройства. Кроме того, осуществляется поддержка ботов и интеграционных сервисов, мгновенных уведомлений о новых сообщениях. Десктопные же приложения имеют более просторный интерфейс, позволяющий одновременно просматривать несколько чатов и медиа, поддержку горячих клавиш, также имеется возможность совершения аудио- и видеозвонков (в зависимости от версии), при этом часто отсутствуют ограничения на размер файлов, которые можно отправить, по сравнению с мобильными версиями. Веб-версия позволяет использовать телеграм без установки приложения, доступна через любой браузер, однако, как правило, имеет меньше функций, чем десктопные и мобильные приложения, сохраняя доступ лишь к основным функциям. При этом не все функции, связанные с безопасностью и конфиденциальностью, могут быть доступны.

В телеграм также есть различия в шифровании в зависимости от типа чатов. Все сообщения в обычных чатах (личные чаты, группы и каналы) шифруются на стороне клиента протоколом шифрования MTProto. Сообщения хранятся на серверах телеграм, что позволяет синхронизировать их между устройствами. Несмотря на шифрование, телеграм имеет доступ к содержимому сообщений на своих серверах.

Эта платформа стала заметным местом для создания и распространения новостей, политических обозрений, развлекательного материала и прочего. Такое широкое применение телеграм делает его ключевым элементом в управлении политическими идеями и процессами, к тому же платформа становится полем для геополитических баталий и столкновения интересов государственных структур с различными преступными группировками. С началом специальной военной операции, проводимой Российской Федерацией на территории Украины, цифровые платформы включая социальные сети, онлайн-порталы, современные медийные каналы и телеграм, превратились в ключевые арены для проведения психологических операций.

Так, ранее телеграм сыграл значительную роль в событиях государственного переворота и массовых протестах в Беларуси и Казахстане, поскольку этот мессенджер стал одним из основных каналов для организации, координации действий и распространения информации среди участников протестов.

В Беларуси после оглашения результатов президентских выборов 9 августа 2020 года почти сразу же начались протесты, и телеграм стал важным инструментом для организаторов и участников. Такие каналы, как NEXTA, использовались для распространения информации о митингах, акциях, а также для документирования репрессий со стороны властей. В телеграм-каналах также подводились итоги репрессий, нападений на протестующих и расследования случаев насилия со стороны силовых структур. Более 1 000 000 подписчиков у NEXTA привлекли внимание к событиям в стране.

В Казахстане, как и в Беларуси, телеграм стал инструментом для координации массовых протестов, спровоцированных ростом цен на сжиженный газ,

в начале января 2022 года. Пользователи мессенджера создали множество каналов, где делились новостями, организовывали митинги и сообщали о ситуации в различных городах.

И в Беларуси, и в Казахстане власти предпринимали меры по блокировке интернет-доступа и остановке работы телеграма, чтобы подавить информацию о протестах, воспрепятствовать действиям по руководству незаконными митингами и несанкционированными акциями протеста. Однако использование VPN и других средств анонимизации позволяло некоторым пользователям продолжать его использование.

Исследователи в России подчеркивают усиление угроз безопасности из-за сильного диссонанса между возрастающим влиянием враждебной информационно-психологической кампании на российских пользователей Интернета и эффективностью реакции со стороны правительственных структур. В этом контексте возникают опасения по поводу потенциальных пагубных последствий. Противостояние, которое обозначено, приводит к серии последствий, угрожающих стабильности существования общества [3].

Положение телеграм, известной мессенджер-платформы, по-прежнему остается неясным. В соответствии с законодательством России, использование этого приложения юридически запрещено на ее территории. Запрет был обусловлен принятием Федерального закона № 374-ФЗ от 6 июля 2016 года, который внес изменения в законодательство по борьбе с терроризмом и наркоторговлей, и укреплению общественной безопасности, требуя от поставщиков услуг связи архивировать данные о звонках и текстовых сообщениях пользователей для возможности их последующей передачи Федеральной службе безопасности [2].

Законодательство, направленное на усиление контроля над общением в Интернете, включая приложение для обмена сообщениями телеграм, предполагает улучшение возможностей для предупреждения и расследования преступлений, особенно терроризма [10, 11]. Однако реализация этих мер столкнулась с трудностями, поскольку не все телекоммуникационные компании были готовы соответствовать нововведениям. От руководства телеграма поступило объявление, что они не в состоянии предоставить данные сообщений из-за шифрования, что делает их технически недоступными. После того как поданное заявление вызвало судебные споры, было решено заблокировать доступ к телеграм в России. При этом попытки Роскомнадзора применить это решение на практике столкнулись с техническими сложностями. Несмотря на официальный запрет, приложение телеграм остается доступным для загрузки и использования пользователями в России. Его популярность как средства мобильной связи не только сохранилась, но и продолжает расти [1].

Разработчики телеграм также несут определенную ответственность за предотвращение противоправных действий на своей платформе. Они могут использовать различные инструменты для обнаружения и блокировки противоправного контента, а также для идентификации пользователей, которые нарушают правила использования телеграм. Однако ответственность разработчиков за предотвращение противоправных действий на платформе остается важной и сложной темой, затрагивающей аспекты безопасности, конфиденциальности и свободы

слова. Так, сквозное шифрование для секретных чатов затрудняет доступ к содержимому сообщений даже для разработчиков, также телеграм придерживается политики, согласно которой он не сохраняет данные о пользователях или чаты, что усложняет отслеживание противоправных действий. Кроме того, телеграм не имеет такой же степени модерации контента, как другие социальные сети.

В некоторых странах телеграм и аналогичные платформы обязаны сотрудничать с правоохранительными органами. Некоторые страны требуют от платформы удаления контента, связанного с радикализацией, насилием или другими противоправными действиями.

Газета The New York Times выпустила публикацию, в которой раскрывается, что в распоряжение Федеральной службы безопасности и полиции России поступили передовые средства мониторинга общения в популярных зашифрованных мессенджерах, включая телеграм, Signal и WhatsApp. В новостях говорится о том, что, опираясь на внутренние источники от поставщиков технологий для силовых структур, было выяснено, что теперь возможно отслеживать, между кем происходит обмен сообщениями и в какое время, несмотря на то, что доступ к содержанию сообщений остается закрытым. В материале подчеркивается, что за последние годы российские органы власти значительно расширили свой инструментарий для интернет-надзора, о чем свидетельствуют документы, полученные из внутренних источников среди российских разработчиков технологий для правоохранительных органов. На передовой позиции в данной отрасли находится «Цитадель» благодаря своему продукту NetBeholder, разработанному ее филиалом «МФИ Софт». Этот инструмент обладает возможностью анализа направлений зашифрованных данных от популярных мессенджеров, включая телеграм, позволяя не только идентифицировать отправителей и получателей сообщений, но и фиксировать время с местом их отправления [4].

В дополнение NetBeholder способен определить, содержит ли сообщение какие-либо файлы, и даже выяснить, пользуется ли пользователь несколькими телефонными номерами, связывая их с устройствами других людей. Функционал программы расширяется до возможности слежения за совпадением местоположения телефонов в определенный момент времени, что позволяет устанавливать местонахождение участников общения внутри России или идентифицировать страну происхождения иностранных пользователей. Упор делается на то, что, хотя шифрование эффективно скрывает содержание взаимообмена сообщениями между пользователями, оно бессильно перед возможностью отслеживания другой информации о трафике. Из заявления представителя телеграм становится ясно, что полное скрытие трафика является задачей нерешаемой, однако были разработаны специальные функции, нацеленные на усложнение процесса его идентификации [4].

Существует несколько методов идентификации пользователей телеграм:

Верификация номера телефона: телеграм требует от пользователей верификацию номера телефона при регистрации. Это позволяет связывать аккаунт с реальным человеком и облегчает поиск злоумышленников. Однако мессенджер предоставляет возможность скрывать номер телефона, оставляя только пользовательское имя.

Идентификация через государственные базы данных. В некоторых странах существует возможность идентификации пользователей телеграм через государственные базы данных, например, по паспорту или другим документам, удостоверяющим личность.

Биометрическая идентификация. В будущем возможна идентификация пользователей телеграм с помощью биометрических данных, таких как распознавание лица, сканирование радужной оболочки глаза или анализ голоса.

Использование элементов искусственного интеллекта. Искусственный интеллект может использоваться для анализа текстовых сообщений, выявления подозрительных аккаунтов, определения связи между пользователями и обнаружения противоправной деятельности.

Использование встроенных функций самого телеграм. Например, такая функция, как «Люди рядом», позволяющая передавать локацию в радиусе 500 метров. Также в телеграм существует функция создания стикерпаков, каждый из которых содержит ID автора.

Использование специального программного обеспечения. Российские разработки, такие как «Охотник», «Окулус», помогают вовремя идентифицировать неизвестных авторов преступных действий в телеграм-каналах и далее привлекать их к ответственности в рамках действующего законодательства, определенно заслуживает отдельного упоминания.

ПО «Охотник» является системой для поиска и анализа информации, полученной из открытых источников, может собирать данные о пользователях, анализировать социальные сети, выявлять связи и потенциальные угрозы. Система может использоваться для мониторинга экстремистской деятельности, мошенничества и других противоправных действий.

ПО «Окулус» – это система, предназначенная для видеонаблюдения и анализа видеоинформации, которая может интегрироваться с камерами наблюдения и другими источниками видеоинформации, а также анализировать записи с целью выявления преступной деятельности. «Окулус» включает функции распознавания лиц и транспортных средств, что может быть полезно при анализе сообщений, переданных в мессенджере в автономном режиме.

Важно подчеркнуть, что успехи, достигнутые ФСБ и МВД РФ в этой области, не дают повода останавливаться на достигнутом. В деле предотвращения распространения экстремистских идей среди общества, в особенности среди молодежи, следует активно работать над улучшением уровня цифровой и политической осведомленности. Инициатива по учреждению в вузах России уникальных центров, которые бы сосредоточились на анализе эмоционального состояния студентов и рассмотрении социальных разногласий среди молодежи, представляется чрезвычайно важной для повышения информационной осведомленности. В контексте этого не менее серьезным остается вопрос о злоупотреблении возможностями Телеграм для достижения противозаконных целей, что влечет за собой угрозы политической стабильности страны. Это вызов, требующий совместных усилий не только от государственных и правоохранительных органов, но и от академического сообщества, особенно в сфере разработки стратегий по формированию навыков критического восприятия информации среди молодежи [3].

Заключение. Таким образом, активное применение разнообразных подходов идентификации пользователей, включая информационное противодействие недостоверной информации, административное взаимодействие со стороны Роскомнадзора и его работы с владельцами интернет-платформ, образовательные инициативы и дипломатические усилия для продвижения международных правил, предотвращающих злоупотребление информационными технологиями в незаконных целях, может эффективно снизить уровень происшествий в рамках данной проблематики.

Список литературы

1. NYT: ФСБ и полиция России научились отслеживать пользователей Telegram, Signal и WhatsApp. URL: https://www.ixbt.com/news/2023/07/04/nyt-telegram-signal-whatsapp.html (дата обращения: 27.07.2024).

2. Журналистика и медиакоммуникации в цифровой среде: сборник научных статей II Международной студенческой научно-практической конференции (Москва, 23 марта 2023 г.) / отв. ред. Д. В. Неренц. М.: РГГУ, 2023. 170 с.

3. Малашенко А. В., Нисневич, Ю. А., Рябов А. В. Становление постиндустриальной цивилизации: от цифровизации до варварства: монография. М.: Юрайт, 2024. 212 с.

4. Медиасистема России: учебник / Е. Л. Вартанова, А. В. Вырковский, А. В. Вырковский [и др.]; под. ред. Е. Л. Вартановой. 2-е изд., испр. и доп. М.: Аспект Пресс, 2021. 424 с.

5. Мяханова А. Н. К вопросу об использовании Telegram-каналов как инструмента профилактики правонарушений / А. Н. Мяханова, Ж. П. Гунзынов // Уголовно-исполнительное право. 2019. Т. 14, № 4. С. 390–393.

6. Никодимов И. Ю. Введение в информационные технологии: учебное пособие для специализированных вузов / И. Ю. Никодимов, М. Ю. Новиков; под общ. ред. Е. А. Пахомовой. М.: Издательско-торговая корпорация «Дашков и К», 2023. 236 с.

7. Жарова А. К. О подходе к классификации информационно-технологических услуг // Государство и право. 2014. № 3. С. 32–38.

8. Суходолов А. П., Бычкова А. М. Цифровые технологии и наркопреступность: проблемы противодействия использованию мессенджера "Телеграм" в распространении наркотиков // Всероссийский криминологический журнал. 2019. Т. 13, № 1. С. 5–17.

9. Шпаковский А. П. Практика использования мессенджера Telegram для дестабилизации политической ситуации в России // Власть. 2024. № 3. С. 85–90.

10. Абделькарим Я. А. Применение концепции «обязанность защищать» (R2P) для введения универсальной юрисдикции в отношении кибертерроризма // Journal of Digital Technologies and Law. 2023. Т. 1, № 4. С. 994–1027.

11. Абделькарим Я. А. Демаркация киберпространства: политико-правовые последствия применения концепции национальных интересов суверенных государств // Journal of Digital Technologies and Law. 2024. Т. 2, № 2. С. 262–285.

И. Н. Тарасов,
магистрант,
Поволжский государственный технологический университет

ТОКЕН И КРИПТОВАЛЮТА КАК РАЗНОВИДНОСТЬ ЦИФРОВЫХ ПРАВ

Аннотация. В работе приведена оценка имеющихся в научной литературе и нормативно-правовой базе определений понятий «токен» и «криптовалюта», с высказыванием авторской позиции об их относимости, всесторонности и актуальности, а также предпринята попытка разобраться в отличиях и сходствах указанных категорий и найти их место в системе цифровых прав. Так как «частные деньги» в виде токенов и криптовалют приобретают все большую популярность в предпринимательском обороте, указанные категории становятся предметом изучения не только технических, но и гуманитарных и социальных наук, в том числе и правовой науки.

Ключевые слова: цифровизация, цифровые права, цифровые финансовые активы, цифровая валюта, утилитарные цифровые права, предпринимательский оборот, токен, криптовалюта

TOKEN AND CRYPTOCURRENCY AS A FORM OF DIGITAL RIGHTS

Abstract. The paper provides an assessment of the definitions of the concepts “token” and “cryptocurrency” available in the scientific literature and legal framework, with the author's position on their relevance, comprehensiveness and relevance, as well as an attempt to understand the differences and similarities of these categories and find their place in the system of digital rights. Since “private money” in the form of tokens and cryptocurrencies are becoming increasingly popular in business circulation, these categories are becoming the subject of study not only of technical, but also of humanities and social sciences, including legal science.

Keywords: digitalization, digital rights, digital financial assets, digital currency, utilitarian digital rights, entrepreneurial circulation, token, cryptocurrency

Введение. В условиях жесткого мирового противоборства [1] за различные ресурсы и возможность доминировать на глобальных рынках, в том числе и на цифровых, одной из главных задач государства является обеспечение ускоренного развития цифровых технологий и форсированное введение их во все отрасли экономики, политики и науки, одновременно с этим особняком выступает социальная сфера. Понимая, что цифровизация общества обеспечивает гигантский масштаб торговли, значительно расширяет доступ к новым платформам и продуктам, руководители нашей страны предпринимают активные попытки развивать это направление. Бесспорно, одним из главных шагов стало наделение цифровых прав официальным статусом и законодательное их признание, что оказало существенное влияние на развитие экономики страны в целом и предпринимательского оборота в частности.

В связи с тем, что цифровые права отнесены к объектам гражданских прав сравнительно недавно, они изучены недостаточно полно и поэтому существует

неопределенность критериев для их оценки и классификации. На этой почве в кругах специалистов имеются различные подходы к градации цифровых прав, касающиеся определения места токенов и криптовалют в системе цифровых прав.

Тема является малоизученной и достаточно актуальной, по которой глубокого анализа учеными до настоящего времени не проводилось.

Основная часть. В первоначальной версии законопроекта о цифровых правах между ними и токенами проводилась тождественная параллель, отдельные представители законодательной власти даже высказывали мнения о том, что вместо термина «цифровые права» в Гражданский кодекс Российской Федерации (далее – ГК РФ) необходимо ввести определение «токен». Однако впоследствии законодатели пришли к выводу, что понятие «цифровые права» шире, чем «токены», которые функционируют в основном на основе технологии Blockchain.

По этому поводу О. В. Лосева пишет: «Отказ законодателя от привязки цифровых прав к распределенному реестру приводит к тому, что цифровые права могут распространяться на любые права, фиксируемые в цифровой форме и действующие по правилам той или иной информационной системы, т. е. цифровые права не сводятся к токенам, при этом некоторые токены (например токены-активы) – это разновидность цифровых прав (цифровые финансовые активы)» [10. С. 46].

Законодатель дифференцирует цифровые права на утилитарные цифровые права [3] (далее – УЦП), цифровые финансовые активы (далее – ЦФА), и цифровые права, включающие ЦФА и иные цифровые права [4, 5, 7–9, 11, 12, 14].

Тем временем юридическим сообществом токены также принято условно подразделять на три группы:

1. Платежные токены, являющиеся средством платежа.

2. Токены – активы, выступающие инструментом инвестирования или финансирования.

3. Уникальные токены, принадлежащие единственному владельцу, например автору какого-то произведения.

Система цифровых прав по своему наполнению объемнее категории токенов, однако последние представляют собой вид УЦП и ЦФА.

«Согласно дефиниции токен представляет собой вид цифрового финансового актива, а цифровой финансовый актив включает в себя, кроме токенов, и криптовалюты» [6. С. 15].

В связи с этим рассмотрим еще один «подкласс» цифровых прав, называемый криптовалютой.

В Федеральном законе от 31 июля 2020 г. № 259-ФЗ «О ЦФА…» [2] дается определение цифровой валюте, которая, хоть и не является денежной единицей РФ, тем не менее может быть принята в качестве средства платежа.

Несмотря на то, что цифровая валюта получила официальный статус, у криптовалюты до настоящего времени нет законодательного определения, однако из названия понятно, что наряду с цифровыми деньгами и виртуальной валютой, она является разновидностью цифровой валюты, особенностью которой является учет ее в децентрализованной платежной системе, так как она в полной мере не узаконена государством.

Учитывая, что статья 140 ГК РФ отождествляет понятия «деньги» и «валюта», можно утверждать, что криптовалюта – это валюта, не имеющая материальной или электронной формы, однако наряду с другими видами цифровых валют может быть использована в качестве платежа за товары и услуги.

Более того, криптовалюта имеет преимущества перед другими средствами платежа, что делать ее привлекательной, особенно для ведения бизнеса, например:

– эту валюту нельзя подделать ввиду наличия уникального кода;

– перевод средств между контрагентами осуществляется без посредников в лице банков и других кредитных организаций, что позволяет избежать излишних комиссионных;

– лицо, владеющее криптовалютой, остается анонимным, что позволяет участникам рынка платить минимальные налоги или не платить их вовсе;

– средства, находящиеся на электронных счетах (кошельках), не могут быть арестованы;

– данные о наличии средств на счетах (кошельках) являются сугубо конфиденциальными.

Зачастую понятия «токен» и «криптовалюта» путают между собой, считая их идентичными средствами платежа, а также функционирования их в распределительном реестре Blockchain, но все же между ними имеется разница:

– эмиссия и проверка подлинности криптовалют, в отличие от токенов, могут осуществляться только децентрализованно;

– цены на криптовалюту полностью регулируются рынком, в отличие от токенов, цена на которые может зависеть от многих других факторов;

– криптовалюты всегда имеют свой блокчейн;

– токены могут выполнять различные функции, в отличие от криптовалют, которые в основном выполняют платежную функцию.

Заключение. Таким образом, токены являются одной из разновидностей цифровых прав, которые относятся к УЦП и ЦФА. Токены по своему предназначению схожи с криптовалютой, однако между ними есть различия. Токен, хотя и является средством платежа, не может полноправно называться криптовалютой, так как не имеет собственного блокчейна, вместе с тем он более прозрачен и централизован. Одновременно с этим установлено, что криптовалюта также является одной из разновидностей цифровых прав, но при этом она относится больше к средствам платежа (деньгам), как платежные токены, чем к праву требования (токены-активы). Авторами исследуются вопросы токенизации других результатов интеллектуальной деятельности [13. С. 125].

В заключение хотелось бы сказать, что целью создания частного бизнеса всегда было извлечение прибыли и получение независимости от государства, «стремление к минимизации временных затрат на покупку и продажу ценных бумаг и финансовых активов, упрощение денежных переводов – все это признаки развития финансовых потоков корпоративного сектора, не нуждающегося в государственном регулировании» [15, 16]. Поэтому «частные деньги» в виде токенов и криптовалют приобретают все большую популярность в предпринимательском обороте.

Список литературы

1. Жарова А. К. Сущность и структура информационного противоборства // Государство и право. 2009. № 2. С. 48–54.

2. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федер. закон от 31 июля 2020 г. № 259-ФЗ (ред. от 8 августа 2024 г.) // КонсультантПлюс.

3. Жарова А. К. О подходе к классификации информационно-технологических услуг // Государство и право. 2014. № 3. С. 32–38.

4. Александрова Н. С. Соотношение понятий «цифровые права», «цифровая валюта» и «цифровой финансовый актив» // Вестник Московского университета МВД России. 2021. № 6. С. 28–31.

5. Василевская Л. Ю., Падузова Е. Б., Тасалов Ф. А. Цифровизация гражданского оборота: проблемы и тенденции развития (цивилистические исследования): монография: в 5 т. Т. 1. М.: Проспект, 2023. 287 с.

6. Демкин В. О. Не токеном единым: сущность токенов и их виды, соотношение с цифровыми правами // Хозяйство и право. 2020. № 10(525). С. 13–19.

7. Денисюк А. Ю. Общая характеристика криптовалюты, использование криптовалюты в нынешних условиях и перспективы // Вопросы устойчивого развития общества. 2022. № 6. С. 195–199.

8. Корчагина К. О. Криптовалюта в России. Влияние криптовалют на экономику РФ // Вестник молодых ученых Самарского государственного экономического университета. 2022. № 1(45). С. 63–66.

9. Кочергин Д. А. Криптоактивы: экономическая природа, классификация и регулирование оборота // Вестник международных организаций: образование, наука, новая экономика. 2022. № 3. С. 75–130.

10. Лосева О. В. Виды и классификация цифровых активов для целей стоимостной оценки // Имущественные отношения в РФ. 2022. № 2(245). С. 45–57.

11. Понкин И. В., Редькина А. И. К вопросу о понятии и онтологии цифровых прав // Пермский юридический альманах. 2021. № 4. С. 340–351.

12. Решетняк С. Р. Классификация цифровых прав // Вестник экспертного совета. 2021. № 1(24). С. 96–105.

13. Самогин А. С. Токены и их правовой статус: проблемы и перспективы регулирования // Образование и право. 2022. № 12. С. 123–126.

14. Фроленко Н. А., Осипова Ю. В. Классификация цифровых прав в нормах действующего российского законодательства // Вестник науки. 2024. № 2(71). С. 174–178.

15. Будник Р. А. Риски и перспективы токенизации творчества // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 587–611.

16. Харуна И. О. Проблемы и перспективы нормативного регулирования системы электронных платежей в Нигерии / И. О. Харуна, П. А. Айдоноджи, О. Д. Бейда // Journal of Digital Technologies and Law. 2024. Т. 2, № 2. С. 372–393.

А. А. Тесленко,
магистрант,
Воронежский государственный университет

МЕТОДИКА РАССЛЕДОВАНИЯ ВЗЯТОЧНИЧЕСТВА И КОММЕРЧЕСКОГО ПОДКУПА С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ВАЛЮТ

Аннотация. В настоящей статье проведен анализ криминалистической характеристики взяточничества и коммерческого подкупа, а также некоторых особенностей производства первоначальных следственных действий при расследовании преступлений коррупционной направленности с использованием криптовалют. Рассматриваются вопросы определения правового статуса цифровых валют как предмета взяточничества и коммерческого подкупа. Затрагиваются проблемы, которые возникают при расследовании рассматриваемых преступлений, а именно глобальный характер, анонимность криптовалют, сложность получения денежной оценки переданных цифровых активов.

Ключевые слова: криминалистическая характеристика, субъект преступления, цифровая валюта, криптовалюта, предмет преступления, тактика следственных действий, следственный осмотр, цифровые следы

METHODOLOGY OF INVESTIGATION OF BRIBERY AND COMMERCIAL BRIBERY USING DIGITAL CURRENCIES

Abstract. This article analyzes the forensic characteristics of bribery and commercial bribery, as well as some features of the production of initial investigative actions in the investigation of corrupt crimes using cryptocurrencies. The issues of determining the legal status of digital currencies as a subject of bribery and commercial bribery are considered. The problems that arise during the investigation of the crimes in question are touched upon, namely the global nature, anonymity of cryptocurrencies, the complexity of obtaining a monetary valuation of the transferred digital assets.

Keywords: forensic characteristics, subject of crime, digital currency, cryptocurrency, subject of crime, investigative tactics, investigative inspection, digital traces

Введение. Бурное внедрение цифровых технологий во все сферы общественных отношений является не только благом, но и несет значительные правовые риски [4, 20]. Новые объекты, возникающие в цифровой среде, могут способствовать развитию более ухищренных способов совершения преступлений [21].

Основная часть. Официальная статистика [16] показывает, что в январе – декабре 2023 года 36 407 криминальных деяний коррупционной направленности выявлено сотрудниками органов внутренних дел – этот показатель на 3 % выше, чем годом ранее. В 2023 году был выявлен 34 271 случай взяточничества, из них в 6 406 – мелкое взяточничество, на втором месте – получение взятки (5 960 дел), а затем дача взятки (5 667 дел). В указанный период было зарегистрировано 2 136 фактов коммерческого подкупа, включая и мелкий коммерческий подкуп.

Взяточничество (коммерческий подкуп) представляет собой трудно раскрываемое преступление. С использованием цифровой валюты сам процесс расследования данных уголовных дел осложняется некоторыми факторами, которые мы рассмотрим ниже.

Переходя к самой методике расследования рассматриваемых преступлений, стоит отметить, что организация расследования – процесс творческий. Аксиоматично, что в первую очередь следует создать реконструкцию события преступления.

В криминалистической литературе механизм совершения преступления рассматривается как некий процесс последовательного взаимодействия всех элементов преступления в ходе формирования и реализации способа преступления [1].

Знание содержания криминалистической характеристики взяточничества и коммерческого подкупа является фундаментом результативного расследования данных преступлений. Ее элементами являются субъекты преступления, а также их личностные характеристики (взяткодатель, взяткополучатель, посредник, соучастники взяткодателя, соучастники взяткополучателя, соучастники посредника), их физическая и психическая деятельность, место и время взяточничества (коммерческого подкупа), предмет рассматриваемых коррупционных преступлений и их следовая картина (рис. 1).

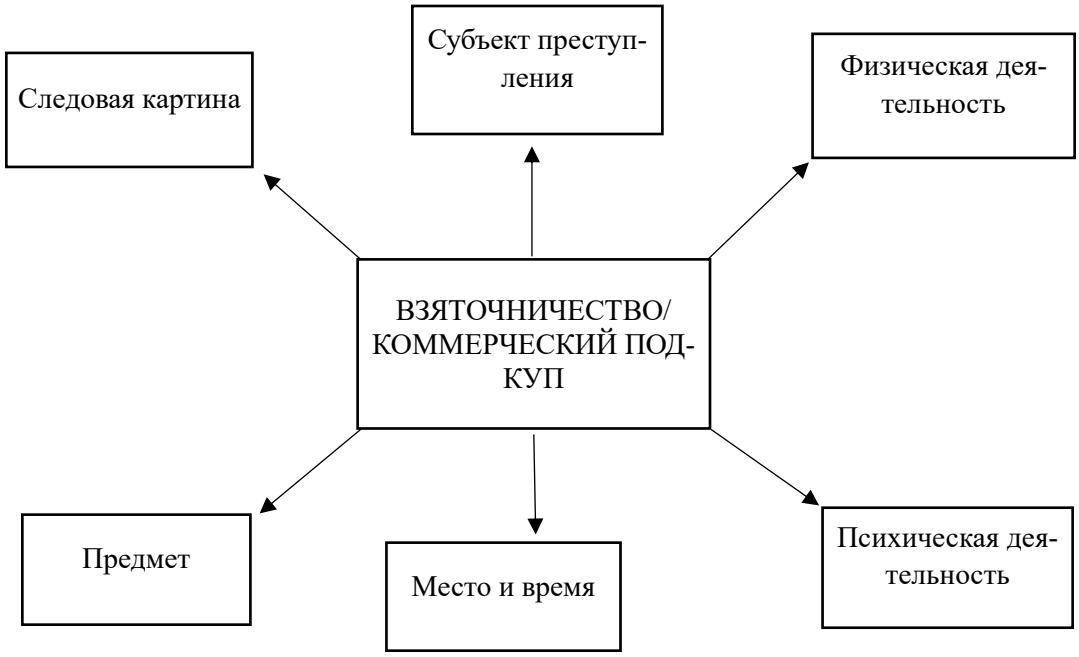

Рис. 1. Схема криминалистической характеристики взяточничества (коммерческого подкупа)

Субъект преступления в коррупционных деяниях. Уголовно-правовая характеристика субъекта (лица, которому передается взятка или незаконное вознаграждение) взяточничества и коммерческого подкупа является основой рассматриваемых коррупционных составов [13]. Для того чтобы понять, совершено ли коррупционное преступление должностным лицом или лицом, выполняющим

управленческие функции в коммерческой или иной организации следует руководствоваться Уголовным кодексом Российской Федерации (далее УК РФ), преимущественно примечаниями 1, 2 и 3 к ст. 285, примечанием 2 к ст. 290, примечанием 1 к ст. 201 УК РФ, учитывая при этом соответствующие разъяснения, которые содержатся в постановлениях Пленума Верховного Суда Российской Федерации (далее – ППВС РФ).

Психологическая деятельность содержит в себе такие понятия, как мотив и цель преступления. При планировании преступления субъект коррупционного деяния непременно действует с прямым умыслом, также сущность коррупционного преступления всегда корыстная.

Пространственно-временными характеристиками, определяющими систему преступления – место и время его совершения. Указанные элементы помогают изобразить реальную картину механизма совершения преступления [6]. Так как информационное развитие общества не стоит на месте, а развивается с каждым годом, то и преступники совершенствуют свои навыки нарушения закона с помощью новых информационных технологий. К настоящему моменту криптовалюту (цифровую валюту) все активнее используют в противозаконной деятельности.

В уголовно-правовой науке «цифровая валюта и цифровые финансовые активы имеют место быть и как средство совершения преступления» [8] и «как предмет преступления» [11], также «рассматриваются вопросы квалификации преступлений, совершенных и связанных с использованием криптовалют», в том числе их классифицируют на те, в которых криптовалюта выступает средством совершения, предметом посягательства, а также на совершаемую для создания (майнинга) криптовалюты [14], при этом отмечаются проблемы определения криптовалюты как предмета преступления [17], ее правовой природы [2], обосновываются предложения по изменению соответствующих положений УК РФ [11, 18].

Единство всех вышеперечисленных элементов криминалистической характеристики предопределяет единство механизма следообразования. Ученые выделяют несколько видов следов коррупционных преступлений. Во-первых, идеальные следы – память лиц. Во-вторых, материальные следы – объекты материального мира (деньги, предметы, услуги имущественного характера, документы) [3]. Как было сказано выше, в ходе совершения преступления используются цифровые технологии, следовательно, образуются цифровые следы [12]. Необходимо указать их особенности: во-первых, зависимость от другого устройства, т. е. цифровой след имеет место быть только на материальном носителе; во-вторых, анонимность, так как не всегда удается идентифицировать владельца или пользователя [5]. Собирание и изъятие таких следов необходимо проводить с участием специалиста в сфере информационных технологий, чтобы не нарушить целостность извлекаемой информации.

Основными следственными действиями при расследовании взяточничества и коммерческого подкупа с использованием цифровых валют являются осмотр, обыск и выемка.

На первоначальном этапе работы следователя основное внимание уделяется обработке информации. Это включает анализ, синтез, восприятие, переработку

и оценку информации, так как именно эта обработка позволяет определить задачи расследования и принимать решения о проведении следственных действий. На предварительном этапе расследования взяточничества и коммерческого подкупа осмотр и обыск являются одними из важных первоначальных следственный действий в ходе расследования рассматриваемых преступлений с использованием цифровых валют. В результате проведения этих следственных действий следует уделить внимание обнаружению различных технических средств, которые дадут доступ к компьютерной информации (в особенности необходимо найти файл wallet.dat, с помощью которого можно установить баланс криптокошелька); бумажные носители информации имеют немаловажную роль, на них могут быть записаны коды доступа, пароли и иная важная информация; необходимо провести осмотр программ-кошельков, используемых для транзакций криптовалюты. Следователь вместе со специалистом должны проанализировать содержимое персонального компьютера, а именно жесткий диск и сетевую карту [9], также необходимо получить информацию из истории браузера (то есть изучить просмотренные веб-страницы). Объектами осмотра являются также помещения, в которых расположена компьютерная техника, оптические и магнитные носители, смартфоны. Стоит обязательно обращать внимание на бумажные носители, какие-либо распечатки, содержащие важные пометки для уголовного дела. Таким образом, основа тактики проведения осмотра или обыска – это привлечение грамотного специалиста, обладающего навыками и знаниями в области информационных технологий. Мы считаем, что следователь должен разбираться в области информационно-коммуникационных технологий, изучать последние события в мире криптовалют, чтобы повышать уровень своих специальных знаний. Но все же ведущую роль в понимании всех тонкостей оставим за специалистами, это связано в первую очередь с нераспространенностью коррупционных преступлений с использованием криптовалют в регионах страны.

Несмотря на всю подготовленность следователя, есть ряд проблем, которые затрудняют расследование взяточничества и коммерческого подкупа. Во взяточничестве и коммерческом подкупе отсутствует потерпевший, обе стороны преступления (взяткодатель и взяткополучатель) заинтересованы в сокрытии фактов совершения коррупции – именно это минимизирует возможности правоохранительных органов выявить общеопасное деяние, а также сокращает сбор доказательств по уголовным делам.

Одной из проблем также является получение денежной оценки предмета взяточничества и коммерческого подкупа, совершенного с использованием криптовалюты. Сложность состоит в том, что нет официального курса, по которому специалист или эксперт должны будут дать заключение. Однако можно использовать курсы криптобирж, какие действовали в момент совершения преступления.

В. А. Михалев выделяет такие проблемы расследования преступлений с криптовалютой, как анонимность операций, проблемы взаимодействия криптовалютных бирж и платформ с правоохранительными органами, необратимость криптовалютных транзакций, отсутствие широко распространенных аналитических инструментов и методов анализа криптовалют [10].

Добавим, что немаловажной проблемой при расследовании взяточничества и коммерческого подкупа с использованием криптовалюты является сложившаяся

внешнеполитическая ситуация в мире, которая делает невозможной координированную работу с правоохранительными органами зарубежных государств. Криптовалюта имеет глобальные масштабы, т. е. нет никаких ограничений по использованию криптокошельков. Однако отсутствие общей правовой базы, регулирующей использование цифровых валют, криптовалют, мешает организованной работе правоохранительных органов.

Заключение. Во-первых, цифровая валюта (она же криптовалюта) может выступать предметом взяточничества и коммерческого подкупа, что вытекает из анализа законодательства, которое устанавливает, в каких случаях цифровая валюта определяется в качестве имущества.

Во-вторых, необходимость совершенствования законодательства в плане применения унифицированного подхода в понимании цифровых валют как предмета совершения преступлений коррупционной направленности.

В-третьих, особое внимание уделить пониманию образования цифровых следов в данной категории преступлений, чтобы безопасно и без изменений изъять компьютерную информацию, имеющую значение для доказательственной базы.

В-четвертых, важность привлечения специалиста при проведении первоначальных следственных действий обуславливается сложностью раскрытия преступлений с использованием цифровых валют.

Список литературы

1. Белкин Р. С. Криминалистика: проблемы, тенденции, перспективы. М., 1987. С. 24–30.

2. Бойкова К. О. Проблемный аспект определения правовой природы цифровых финансовых активов и цифровой валюты при расследовании преступлений, связанных с их оборотом // Криминалистика: вчера, сегодня, завтра. 2022. № 2.

3. Буйнов Д. О. Теория и практика собирания и экспертного исследования цифровых следов по уголовным делам в сфере экономической деятельности: дис. … канд. юрид. наук. М., 2023. 229 с.

4. Ефремов А. А. Оценка правовых рисков проектов цифровой трансформации на основе технологий искусственного интеллекта // Информационное право. 2023. № 3. С. 24–27.

5. Закиян А. А. Цифровые следы в криминалистике // Молодой ученый. 2023. № 23(470). С. 326–328.

6. Захарчук С. Д. Проблемные вопросы определения предмета взяточничества // Юридическая наука и правоохранительная практика. 2019. № 5(50). С. 153–160.

7. Квалификация деяния. Тактика и методика расследования коррупционных преступлений. Настольная книга следователя: учебное пособие для студентов вузов, обучающихся по специальностям «Юриспруденция» и «Правоохранительная деятельность» / Д. И. Аминов, А. М. Багмет, В. В. Бычков, Н. Д. Эриашвили; под ред. Н. Д. Эриашвили. М.: ЮНИТИ-ДАНА, 2017. С. 159–180.

8. Коренная А. А. Цифровая валюта как предмет и средство совершения преступлений // Российско-азиатский правовой журнал. 2021. № 3.

9. Маркарян Э. С. Специфика проведения следственного осмотра при расследовании преступлений, совершенных с использованием криптовалют // Актуальные проблемы российского права. 2018. № 6. С. 146–152.

10. Михалев В. А. Проблемы расследования преступлений, совершенных с использованием криптовалют. – Текст: непосредственный // Молодой ученый. 2024. № 4(503). С. 310–312.

11. Никонов П. В. Цифровые финансовые активы и цифровая валюта, как предмет взяточничества // Искусство правоведения. 2023. № 1(5).

12. Рахимов А. И. Идеальные следы преступления и их классификация // Гуманитарные, социально-экономические и общественные науки. 2022. № 3. С. 150–152.

13. Репин М. Е. Некоторые особенности криминалистической характеристики взяточничества // Актуальные проблемы права: материалы III Междунар. науч. конф. (г. Москва, ноябрь 2014 г.). М.: Буки-Веди, 2014. С. 123.

14. Русскевич Е. А., Малыгин И. И. Преступления, связанные с обращением криптовалют: особенности квалификации // Право. Журнал Высшей школы экономики. 2021. № 3. С. 106–125.

15. Севальнев В. В. Цифровые финансовые активы и цифровые валюты в коррупционном правонарушении // Криминологический журнал. 2022. № 4. С. 151–156.

16. Состояние преступности в России за январь – июль 2022 года // Министерство внутренних дел Российской Федерации.

17. Тарновский А. А., Коваленко Е. В., Мазняк В. К. Проблемы квалификации преступления при даче взятки в криптовалюте // Образование и право. 2022. № 11.

18. Усачева Е. А., Филимонов А. Д. Криптовалюта как предмет взятки и коммерческого подкупа: проблемы регулирования // Искусство правоведения. The art of law. 2023. № 1(5).

19. Sitnikov M. S. Financial and Legal Development of Social Relations Using Digital Currencies in Metaverses // Journal of Digital Technologies and Law. 2024. № 2. Pp. 200–220.

20. Противодействие коррупции: новые вызовы: монография / С. Б. Иванов, Т. Я. Хабриева, Ю. А. Чиханчин [и др.]; отв. ред. Т. Я. Хабриева. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации; ИНФРА-М, 2018.

21. Противодействие коррупции и процессы цифровизации: научно-практическое пособие / Ю. В. Трунцевский, А. М. Цирин, Е. В. Черепанова и др. Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. М.: Инфотропик Медиа, 2023.

Д. В. Усиков,
студент,
Московская академия Следственного комитета
Российской Федерации имени А. Я. Сухарева

ЦИФРОВИЗАЦИЯ «КЛАССИЧЕСКОЙ» ПРЕСТУПНОСТИ: ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

Аннотация. Данная работа обозревает проблему влияния всеобщей цифровизации на изменение криминалистической характеристики так называемых классических преступлений. Анализируются как изменения в механизме преступления на всех его этапах, обусловленные цифровизацией, так и изменения в следах и особенностях работы с ними. Оговаривается, что цифровые следы в условиях цифровизации носят всеобщий характер. Раскрываются такие проблемы, вызванные изменением преступности, как: обилие собираемой различными операторами информации, сложности в ее получении и анализе, отсутствие оперативности, высокая подготовленность злоумышленников в сфере IT, дистанционный характер взаимодействия людей. Предлагаются пути решения указанных проблем, в частности указывается на необходимость развития международного сотрудничества в этой сфере.

Ключевые слова: цифровизация, цифровизация преступности, киберпреступления, дистанционные преступления, цифровые следы, криминалистическая характеристика

DIGITALIZATION OF “CLASSICAL” CRIME: CHALLENGES AND SOLUTIONS

Abstract. This piece reviews the problem of general digitalization impact on a change of so called “classic” crimes characteristics. There are changes of both process of crimes and traces ones leave because of digitalization analyzed. The article specifies general nature of digital traces in conditions of mass digitalization. Article also opens problems caused by digital changes of crime such as: fullness of personal information collected by different operators, difficulty of getting and analyzing it, lack of promptness, high level of criminal digital skills, distant nature of persons interaction. Ways of dealing with it are proposed as well as necessity of developing international cooperation in this field.

Keywords: digitalization, digitalization of crime, cybercrime, distance crime, digital traces, crime characteristics

Введение. Цифровизация криминальной сферы жизни общества [3, 12, 26] как неотъемлемой его части ведет не только к появлению новых форм криминальной деятельности (их принято называть «киберпреступления») аналогично появлению новых форм некриминального взаимодействия людей, но и к тому, что претерпевают значительные изменения старые, уже давно привычные формы преступности: убийства по найму, развратные действия, нарушение неприкосновен-

ности частной жизни, сбыт наркотических средств и т. д. [8]. Таким образом, следует отметить, что вся преступность сейчас становится как бы «киберокрашенной» [15, 23, 25].

Говоря о влиянии всеобщей цифровизации на характер преступлений, следует отметить такую особенность цифровизации, как бурное и неконтролируемое развитие цифровых технологий в условиях, когда отсутствуют институциональные центры развития, либо они сильно размыты. Наличие у огромного количества людей в норме персонального компьютера, базовых навыков работы с ним и доступа в Интернет дает им возможность постоянно самостоятельно совершенствовать свои умения, учиться, делиться опытом и т. д. – для становления специалиста в IT-индустрии теперь важно не столько обучение профессии по специализированной программе в учебном заведении, опыт работы в конкретных организациях, сколько его личная заинтересованность. Новые разработки и современные технологии отныне не концентрируются в ограниченном количестве отдельных центров, они распределены среди энтузиастов, являющихся при этом не любителями, а полноценными профессионалами [11].

Высокая скорость развития цифровых технологий приводит к тому, что отдельные злоумышленники обладают в этой сфере возможностями и знаниями, значительно превышающими уровень правоохранительных органов, что позволяет им избегать ответственности. Помимо общих усилий по повышению мастерства, постоянной актуализации знаний, при раскрытии и расследовании таких преступлений необходимо применять творческий подход, искать нестандартные подходы к поиску доказательственной информации и изобличению виновного. В том числе применяя вместе с логичными в таких случаях тактическими подходами, подразумевающими исследование технических устройств, компьютерной информации, к чему злоумышленник готов и от чего защищен, традиционные приемы, о которых он даже не догадывается. Так, для отождествления лица с неизвестным аккаунтом можно использовать возможности судебного автороведения, путем анализа и сравнения текста переписки в интернет-мессенджере.

В таких условиях получают также распространение различные формы использования лиц для выполнения ими отдельных действий во исполнение более крупной преступной цели иных лиц, организаторов. Приискание таких лиц (так называемые дропы, грибы, номиналы, стрингеры), их наем, координация их действий, оплата осуществляется через Интернет, иногда для этого существуют специальные сервисы, сообщества, куда выкладываются такие объявления. Такие лица используются в качестве подставных при образовании фиктивных юридических лиц (так называемых однодневок), в качестве курьеров наркотических средств, исполнителей диверсий, террористических актов и др. В некотором роде такая работа схожа с фрилансом – она носит кратковременный и часто единичный характер, что также является преимуществом для организаторов и конечных выгодоприобретателей [7, 13].

Однако даже при таких, с одной стороны, благоприятных для них условиях злоумышленники и их сообщники все же существуют и действуют в реальном мире, поэтому в ходе своей преступной деятельности, будучи хорошо защищен-

ными в цифровом отношении, они могут оставлять следы в физическом пространстве, поэтому всегда необходимо также осуществлять тщательный поиск и таких привычных следов, которые могут дать ценную информацию.

Дистанционный характер повседневных взаимодействий в Интернете, оказывающий значительное влияние на криминальную деятельность, проявляется также и в том, что серверы и администрации большого количества интернет-сервисов, которыми активно пользуются в своей повседневной жизни граждане нашей страны, находятся в зарубежных странах. Соответственно, для получения необходимой информации от оператора данных, находящегося в зарубежной юрисдикции, правоохранительным органам необходимо направлять соответствующие международные запросы, процедура подачи которых очень сложна и громоздка. В дополнение к этому такие запросы зачастую не исполняются иностранными организациями, что препятствует раскрытию и расследованию преступлений [6]. Это, а также то, что дистанционный характер преступной деятельности в условиях всеобщей цифровизации приводит к тому, что совершение преступлений и причинение таким путем ущерба возможно лицами, находящимися за пределами России. Также это приводит к тому, что государственная граница и разделение компетенций правоохранительных органов используются криминалитетом в целях уклонения от ответственности или сокрытия следов (например, путем вывода денежных средств в иностранные банки и совершения там с ними операций для их легализации). Все это говорит о необходимости реального развития международного сотрудничества для противодействия развитию современной преступности.

Заключение. Таким образом, видно, как всеобщая цифровизация создает условия, влияющие на характер преступности, видоизменяющие ее во всех проявлениях, затрагивая и существенно изменяя криминалистическую характеристику каждого преступления.

Список литературы

1. Бабихина К. Основные тренды российской преступности в 2021 году: исследование «Если быть точным». Текст: электронный // Если быть точным: [сайт]. URL: https://tochno.st/materials/osnovnye-trendy-rossiyskoy-prestupnosti-v-2021-godu-issledovanie-esli-byt-tochnym (дата обращения: 06.05.2024).

2. Бессонов А. А. Большие данные (big data) в криминалистике // Конституция Российской Федерации и современный правопорядок. 2019. С. 261–265.

3. Бовина И. Б., Дворянчиков Н. В. Поведение онлайн и офлайн: две реальности или одна? // Психологическая наука и образование. 2020. Т. 25, № 3. С. 101–115.

4. Богданов А. В., Ильинский И. И., Хазов Е. Н. Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // Криминологический журнал. 2020. № 1. С. 15–20.

5. Бычков В. В., Вехов В. Б. Электронное следообразование преступной деятельности в сети Интернет // Расследование преступлений: проблемы и пути их решения. 2020. № 1. С. 106–111.

6. Вирясова Н. В., Аванесян А. В. О некоторых проблемах исполнения компетентными органами иностранных государств запросов о правовой помощи по

уголовному делу // Теоретические и прикладные аспекты развития современной науки и образования. 2020. С. 49–51.

7. Зажигалкин В. Е. «Дропы» – инструмент организации и исполнения контрабанды подконтрольных психоактивных веществ с использованием современных телекоммуникационных ресурсов // Наркоконтроль. 2018. № 3. С. 28–30.

8. Земцова С. И. Бесконтактный сбыт наркотических средств с использованием интернет-магазинов: актуальные вопросы // Наркоконтроль. 2019. № 3. С. 17.

9. Значимые утечки данных в 2023 году. URL: https://dfi.kaspersky.ru

10. Капинус О. С. Цифровизация преступности и уголовное право // Baikal Research Journal. 2022. Т. 13, № 1. С. 22–32.

11. Комлев Ю. Ю. Кибердевиантность миллениалов: феноменология и пути противодействия // Профилактика девиантного поведения детей и молодежи: региональные модели и технологии. 2020. С. 77–81.

12. Кудрявцева Т. Ю., Кожина К. С. Основные понятия цифровизации // Вестник Академии знаний. 2021. № 3(44). С. 149–151.

13. Ларичев В. Д. Преступления в сфере экономики, связанные с незаконным образованием юридического лица через подставных лиц, а также незаконным использованием документов // Безопасность бизнеса. 2021. № 2. С. 39–43.

14. Елин В. М., Жарова А. К. Правовые аспекты торговли в сети интернет // Право и государство: теория и практика. 2012. № 10. С. 139–151. EDN: NVSBLB

15. Пырчев С. В. Тенденции организованной преступности в развивающемся цифровом мире // Труды Академии управления МВД России. 2020. № 2(54). С. 142–153.

16. Работа следователя с «цифровыми следами»: учебно-методическое пособие / В. В. Бычков, С. Ю. Скобелин. М.: Московская академия СК России, 2021. 17 с.

17. Расследование преступлений в сфере информационно-телекоммуникационных технологий: учебно-методическое пособие / С. Ю. Скобелин, А. А. Лебедева. М.: Московская академия СК России, 2021. 78 с.

18. Расследование преступлений, совершенных с использованием Интернета и мобильной телефонии: курс лекций / В. В. Бычков, А. А. Лебедева, С. Ю. Скобелин. М.: Московская академия СК России, 2021. 161 с.

19. Сергеев С., Сергеев Н., МВД запросило неотложное. URL: https://www.kommersant.ru

20. Тактика следственного осмотра по делам о киберпреступлениях: учебно-методическое пособие / Э. Б. Хатов, А. Ю. Любавский, С. Ю. Скобелин и др. М.: Московская академия Следственного комитета имени А. Я. Сухарева, 2023. 117 с.

21. Ткаченко А. Л., Сафронов Е. С., Кузнецова В. И. Анализ эффективности защиты персональных данных и проблема cookie файлов // Дневник науки. 2021. № 6.

22. Шайдуллина В. К. Большие данные и защита персональных данных: основные проблемы теории и практики правового регулирования // Общество: политика, экономика, право. 2019. № 1(66). С. 51–55.

23. Шалагин А. Е., Идиятуллов А. Д. Новые тенденции преступности в XXI веке: глобализация, цифровизация, социальный контроль // Modern Science. 2020. № 11–1. С. 131–134.

24. Bruce M. et al. Mapping the global geography of cybercrime with the World Cybercrime Index // Plos one. 2024. Т. 19, №. 4. P. e0297312.

25. Fortier M. READ: Brian Walshe's Shocking Google Searches After His Wife Went Missing. URL: https://www.nbcboston.com/news/local/heres-what-brian-walshes-google-searches-included-after-his-wife-went-missing/294814 (дата обращения: 06.05.2024).

26. Жарова А. К. О подходе к классификации информационно-технологических услуг // Государство и право. 2014. № 3. С. 32–38.

В. В. Федорова,
магистрант,
Поволжский институт управления имени П. А. Столыпина –
филиал Российской академии народного хозяйства
и государственной службы при Президенте Российской Федерации

«ВОЛШЕБНЫЙ КРУГ»: ПРАВОВОЕ РЕГУЛИРОВАНИЕ ВИРТУАЛЬНЫХ МИРОВ КОМПЬЮТЕРНЫХ ИГР

Аннотация. В данной статье анализируются основные особенности правового регулирования общественных отношений, возникающих в ходе игрового процесса между пользователями онлайн компьютерных игр, а также иными лицами. Рассматривается сущность концепции Magic Circle, которая предусматривает, какие правовые последствия для игроков возникают в результате внутриигровых действий, и анализирует суверенно-интерактивный подход к юридическому суверенитету игровых миров и вымышленных реальностей. Сделаны выводы о недостаточной определенности допустимого правового влияния на игровые события с точки зрения современного российского законодательства.

Ключевые слова: компьютерные игры, виртуальная реальность, правовое регулирование, суверенитет, интерактивность, интернет-право, правовая квалификация

“MAGIC CIRCLE”: LEGAL REGULATION OF VIRTUAL WORLDS IN COMPUTER GAMES

Abstract. This article analyzes the main features of the legal regulation of public relations that arise during the gameplay process between users of computer games, as well as other persons. The author examines the essence of the «Magic Circle» concept, explores what legal consequences for players arise as a result of in-game actions and studies a sovereign-interactive approach to the legal sovereignty of game worlds and fictional realities. Conclusions are drawn about the lack of certainty of the permissible legal influence on gaming events from the point of view of modern Russian legislation.

Keywords: computer games, virtual reality, legal regulation, sovereignty, interactivity, legal qualifications

Введение. На сегодняшний день каждому из нас доступно множество форм досуга, большая часть которых так или иначе связана с цифровыми технологиями. Индустрия компьютерных игр стремительно развивается, ежегодно расширяя охват за счет игроков, привлекаемых как инновационными игровыми механиками, так и принципиально новыми моделями социального взаимодействия. Если раньше компьютерные игры могли считаться исключительно индивидуальным развлечением для того пользователя, на чьем устройстве установлена соответствующая игра, то сейчас многие игры эволюционировали в некое подобие отдельного мира, существующего в виртуальной реальности. Очевидно, что, как и в любой другой реальности, в реальности компьютерных игр должны работать свои законы и правила, в том числе юридические, которые необходимы для поддержания порядка и разрешения возникающих конфликтов. В связи с этим возникает закономерный вопрос: в какой части взаимоотношения, возникающие в рамках киберпространства игровых процессов, подлежат правовому регулированию и влекут правовые последствия в реальном мире [9]. Ответ на этот вопрос позволил бы значительно упорядочить огромный массив общественных отношений, имеющих место в связи с активным развитием игровой индустрии.

Целью данного исследования стало выяснение, каким образом осуществляется правовое регулирование общественных отношений, возникающих в рамках многопользовательских видеоигр. Для достижения поставленной цели нами были выполнены следующие задачи: изучить историю формирования правовых взглядов на виртуальную реальность компьютерных игр, выявить основные подходы к допустимости действия законодательных положений в пределах игрового пространства, выяснить, каким образом правовое регулирование данных общественных отношений осуществляется в РФ, сделать выводы, исходя из собранных материалов.

Основная часть. До определенного момента события, происходящие внутри компьютерных игр, не выходили за пределы персональных компьютеров отдельных игроков. В рамках игры пользователь мог быть кем угодно (ассасином, торговцем, воином, фермером и т. д.), и это не оказывало влияния на реальный мир. Однако с повсеместным распространением Интернета и многопользовательских онлайн-игр ситуация значительно изменилась. Сегодня некоторые события виртуального мира порождают реальные последствия даже для тех лиц, которые не принимают непосредственного участия в игровом процессе. Многие игровые механики предусматривают наличие у пользователей имущественной заинтересованности в исходе определенных внутриигровых событий, товарно-денежные отношения, предметом которых становится игровое имущество или аккаунты, имеющие доступ к определенным игровым ресурсам, подразумевают оплату реальной валютой. Игровой мир постепенно начал влиять на реальность [8].

До тех пор, пока влияние игровых миров на реальный оставалось минимальным, государство не было заинтересовано в том, чтобы внедрять в них нормативно-правовое регулирование. В рамках сети Интернет сформировалась так называемая lex informatica (так же, как в свое время была сформирована lex

mercatoria, успешно выполнявшая функции по саморегулированию коммерческой практики) [7]. В случае если бы lex informatica продолжила развиваться в соответствии с базовыми принципами, нашедшими отражение в неофициальной Декларации независимости киберпространства [10] («Поступай с другими так, как хочешь, чтобы поступили с тобой»), государственного вмешательства в данную сферу общественных отношений удалось бы полностью избежать, однако подобное предположение по своей сути является утопическим и, очевидно, не могло бы быть реализовано на практике.

Lex informatica, существующая на данном этапе своего развития, дискриминационна и не направлена на защиту интересов широкого круга лиц, взаимодействующих в цифровом пространстве. Как отмечается в современных исследованиях [4. С. 55], такая система регулирования цифровых отношений не является прозрачной и базируется на навязывании «условий игры» другим пользователям. Именно поэтому государство было вынуждено вмешаться и предпринять попытки по адаптации правовых механизмов к новым реалиям.

Несмотря на значительное расширение сферы влияния государства на виртуальное пространство игр, не все процессы, происходящие в них, представляют интерес, с правовой точки зрения, поскольку сами игры входят в сферу досуга, развлечения, которая не порождает юридически значимых событий и редко подпадает под действие каких-либо правовых норм (так, например, убийства персонажей или кражи внутриигровых объектов, если они предусмотрены игровой механикой, остаются за рамками правового поля, так как не влекут за собой реальных последствий) [3]. Наиболее перспективными направлениями для совершенствования правового регулирования виртуальных игровых миров являются электронная коммерция, отношения, связанные с интеллектуальной собственностью, а также отношения в области защиты чести, достоинства и деловой репутации участников кооперативных игр.

Среди юристов наибольшей популярностью пользуются три основных подхода к возможности регулирования игровых миров средствами действующего права [5. С. 59].

Первый подход полностью оправдывает государственное вмешательство в дела виртуальной игровой реальности тем, что интересы пользователей необходимо защищать, даже если сами пользователи с этим не согласны. Поскольку кооперативные и многопользовательские онлайн-игры действительно в значительной степени затрагивают реальные права и свободы участников (чаще всего имущественные), государство, согласно данному подходу, обязано осуществлять защиту пользователей в отношении разработчиков (как слабой стороны), а также защищать публичные интересы в области налогообложения дохода, который обращается в виртуальной среде. С одной стороны, государство, осуществляющее свою регулятивную деятельность в рамках данного подхода, получает практически неограниченную свободу воздействия на игровую реальность, мотивированную необходимостью поддержания общественной справедливости, но, с другой стороны, на плечи государства ложится обязанность по адаптации существующих правовых механизмов к цифровой среде, что, безусловно, испытывает любое право на гибкость.

В противовес первому подходу вторая точка зрения, имеющая ярко выраженную либертарианскую направленность, провозглашает, что пространство многопользовательских игр (как часть киберпространства) является суверенным и должно быть полностью свободным от действия какого-либо национального права. Сторонники такой точки зрения предполагают, что наиболее оптимальным для современного киберпространства является саморегулирование, основанное на обычаях, традициях, а также правилах, предложенных разработчиком конкретной игры своим пользователям. Обычно такие правила предлагаются пользователям для ознакомления в рамках лицензионного соглашения, доступ к которому предоставляется до начала самой игры [6]. Данная концепция абсолютизирует внутреннюю свободу компьютерных игр, однако полностью лишает как игроков, так и разработчиков возможности рассчитывать на правовые средства защиты в случае возникновения конфликтных ситуаций, в связи с чем ее применение на практике выглядит крайне спорным.

Третья концепция стремится к тому, чтобы в равной степени учесть и суверенитет игровой виртуальной реальности, и ее взаимодействие с настоящей жизнью. Именно поэтому эта концепция именуются в теории цивилистики «суверенно-интерактивной». В рамках данного подхода американскими юристами было разработано «правило волшебного круга» (Magic Circle) [11]. Смысл «волшебного круга» заключается в том, что действия игроков должны иметь правовые последствия только в том случае, если они, даже будучи связанными с игровой механикой, влияют на реальный мир, выходя за рамки цифрового пространства. Во всех остальных случаях действия пользователей юридически безразличны и регулируются исключительно в рамках правил, установленных для конкретной игры разработчиком.

На первый взгляд кажется, что именно такой подход способен учесть все необходимые особенности внутриигровых отношений и дает возможность разграничить механики игры (например, совершаемые виртуальными персонажами хищения) и фактические правонарушения (хищения аккаунтов посредством взлома). Однако в некоторых случаях у правоприменителя могут возникнуть весьма ощутимые трудности в определении круга отношений, подлежащих регулированию правовыми средствами, так как реальные правовые последствия (пусть даже и довольно условные) можно обнаружить практически у любого действия, совершенного игроком (игровое имущество зачастую имеет реальную стоимостную оценку).

Концепция «магического круга» под разными названиями широко применяется в тех государствах, где виртуальная реальность и компьютерные игры уже давно стали частью повседневной жизни (наиболее развито применение данной методики регулирования киберпространства в Южной Корее и Китае) [2]. Как показывает практика, иногда судебная защита прав игроков, нарушенных в рамках многопользовательской игры, может стать эффективным инструментом защиты частных имущественных интересов (особенно в тех случаях, когда возникает вопрос о купле-продаже игровых объектов за реальные деньги).

К сожалению, отечественная правовая действительность еще не готова к тому, чтобы однозначно определиться с механизмом регулирования виртуаль-

ных миров. Для РФ сегодня характерным является отказ от вмешательства государства в дела виртуальных реальностей компьютерных игр, который мотивирован отнесением видеоигр к «игре» для целей применения ст. 1062 ГК РФ к отношениям в рамках игрового процесса [1]. По уже сложившейся традиции игровые правила, которые предусматривают порядок создания, обмена и купли-продажи игровых предметов, устанавливаются и регулируются правообладателем игры, а не законом. Фактически пользователи кооперативных игр вынуждены следовать принципу take it or leave it, что провоцирует формирование теневого сектора игрового взаимодействия, где игроки более гибко налаживают имущественный обмен, но лишаются возможности защитить свои права.

Существующий пробел в нормативно-правовом регулировании создает почву для нарушений интересов пользователей в области имущественного оборота виртуальных объектов. В основном такие нарушения совершаются разработчиками игр, которые допускают необоснованные блокировки аккаунтов или списание игрового баланса, или третьими лицами, заинтересованными в краже аккаунтов.

Поскольку правовое регулирование не всегда способно в достаточной степени обеспечить защиту прав пользователей онлайн-игр, интернет-сообщество предпринимает попытки по выработке новых самостоятельных способов регулирования, одним из которых является lex cryptographica [12], свод правил саморегулирования блокчейн-сообщества. Безусловно, криптографическое шифрование надежно защищает пользователя от кражи игрового имущества, поскольку игровое имущество представлено исключительно в виде токена в криптокошельке, однако масштаб использования криптокошельков в рамках многопользовательских игр по-прежнему крайне невелик, поэтому такой способ регулирования не может быть признан универсальным.

Заключение. Подводя итоги, необходимо в очередной раз отметить, что регулирование виртуальной реальности – крайне перспективное направление для развития современной юриспруденции, поскольку не только сфера развлечений, но и многие другие области повседневной жизни людей постепенно уходят в цифровой формат. Выработав приемлемую стратегию для поддержания порядка в рамках цифровой реальности многопользовательских игр, мы сможем в дальнейшем распространить соответствующую модель на более широкий круг виртуальных реальностей.

Наиболее перспективным подходом к регулированию общественных отношений, возникающих внутри игровых миров, следует считать суверенно-интерактивный подход, который в равной степени учитывает и уникальность игровой реальности как суверенного, фактически независимого слоя реальности, и его неразрывную связь с действительностью за пределами цифрового мира.

В России на сегодняшний день одной из наибольших проблем для формирования эффективного механизма правового регулирования цифровых миров видеоигр является крайне размытая формулировка ст. 1062 ГК РФ, которая затрудняет для правоприменителя определение границ между играми и «игрой», к которой может быть применена данная статья. В связи с этим становится целесообразным внести изменения не только в текст данной статьи, но и в целом весь массив законодательства об азартных играх. В случае если данные изменения будут

предусматривать разработку соответствующих дефиниций с учетом технических особенностей, присущих компьютерным играм, это позволит провести черту между азартными играми, отношения, вытекающие из которых правовой защите не подлежат, и иными играми (в частности, теми, в рамках которых формируются собственные игровые миры), что, безусловно, необходимо в свете повсеместного роста популярности компьютерных игр.

Список литературы

1. Апелляционное определение судебной коллегии по гражданским делам Московского городского суда от 20 мая 2019 г. по делу № 33-21065/19 (в первой инстанции № 02-3433/2018). URL: https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/0de6b77e-95c8-4707-8921-f762e36dd67d?caseNumber=33-21065/19 (дата обращения: 07.09.2024).

2. Бесчастнов Н. Н., Егоров К. Ю. Политика КНР в сфере регулирования рынка компьютерных игр (социальный и культурный аспекты) // Теория и практика общественного развития. 2023. № 5(181).

3. Васильев А. А., Печатнова Ю. В. Реальные правовые проблемы виртуальных миров компьютерных игр // Вестник юридического факультета Южного федерального университета. 2022. № 4.

4. Войниканис Е. А. Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. М.: Юриспруденция, 2013.

5. Григорьев Д. А. Суверенность игровых миров: как право должно регулировать виртуальные игры // Видеоигры, гейминг, киберспорт: правовые вопросы. М.: Развитие правовых систем, 2023. С. 55–65.

6. Жарова А. К. О подходе к классификации информационно-технологических услуг // Государство и право. 2014. № 3. С. 32–38. EDN: SDFIQT

7. Мажорина М. В. Право сообщества (Lex communitas) как современный этап развития Lex mercatoria // Актуальные проблемы российского права. 2023. №6 (151). Перепелкина Я. А. Виртуальное игровое имущество: перспективы правового регулирования [Электронный ресурс] // Журнал Суда по интеллектуальным правам. 2020 URL: http://ipcmagazine.ru/legal-issues/virtual-gaming-property-prospects-for-legal-regulation (дата обращения: 07.09.2024).

8. Семенова И. С. Цифровое общество: новые вызовы // Наука, образование и культура. 2020. № 5(49). URL: https://cyberleninka.ru/article/n/tsifrovoe-obschestvo-novye-vyzovy (дата обращения: 07.09.2024).

9. A Declaration of the Independence of Cyberspace [Электронный ресурс]. URL: https://www.eff.org (дата обращения: 07.09.2024).

10. Duranske B. T. Virtual Law. Navigating Legal Landscape of Virtual Worlds // Chicago: ABA Publishing, 2008. 461 c.

11. Filippi P. de. From Lex Mercatoria to Lex Cryptographica // Dispute Revolution. The Kleros Handbook of Decentralized Justice. URL: https://blog.kleros.io/dispute-revolution-the-kleros-handbook-of-decentralized-justice

12. (дата обращения: 07.09.2024).

З. З. Шайхутдинова,
студент,
Российский государственный университет правосудия,
Казанский филиал

ОСОБЕННОСТИ ПРИМЕНЕНИЯ СОКРАЩЕННОЙ ФОРМЫ ДОЗНАНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. В данной статье рассматривается особенность сокращенной формы дознания как взаимный компромисс между сторонами уголовного процесса, история возникновения, цель создания данного института, а именно снижение нагрузки на правоохранительные органы и сокращение издержек при исследовании обстоятельств преступного деяния, преимущества как для государственных органов, так и для обвиняемого, исследуются трудности осуществления данной процессуальной формы, проводится анализ сущности данного института в условиях цифровизации.

Ключевые слова: предварительное расследование, сущность, дознание, сокращенная форма дознания, институт

FEATURES OF THE USE OF THE ABBREVIATED FORM OF INQUIRY IN THE CONTEXT OF DIGITALIZATION

Abstract. The article examines the peculiarity of the abbreviated form of inquiry, as a mutual compromise between the parties to the criminal process, the history of its origin, the purpose of creating this institution, namely, reducing the burden on law enforcement agencies and reducing costs in investigating the circumstances of a criminal act, advantages for both government agencies and the accused, the difficulties of implementing this procedural form are investigated, The essence of this institution is analyzed.

Keywords: preliminary investigation, essence, inquiry, abbreviated form of inquiry, institute

Введение. Идея упрощения уголовного судопроизводства давно существовала в отечественном праве, однако в современном уголовно-процессуальном кодексе дознание в сокращенной форме появилось относительно недавно, а именно после принятия Федерального закона от 4 марта 2013 г. № 23-ФЗ, которым была введена глава 32.1, посвященная данному институту. Связано это, прежде всего, с необходимостью разгрузить работу органов предварительного расследования, а также сократить затраты на расследование преступлений, как временные, так и материальные. Все это позволяет по-новому взглянуть на проблему в условиях цифровизации.

Основная часть. По своей сути данная форма дознания является неким взаимным компромиссом между сторонами уголовного процесса. Со стороны обвиняемого – признание своей вины в полном объеме и согласие с правовой оценкой своего деяния, со стороны потерпевшего – согласие с данной формой дознания. Тем самым обвиняемому назначается наказание меньшее, нежели предусмотрено санкцией нормы, а именно, согласно ст. 229.6 Уголовно-процессуального кодекса

[1], оно не может превышать одну вторую максимального срока или размера наиболее строгого вида наказания. Однако в ряде случаев упрощенная форма дознания применяться не может [2. С. 368].

Потерпевший, в свою очередь, в ускоренном порядке может реализовать свое право на судебную защиту, восстановить нарушенные права и облегчить свои моральные терзания благодаря приближению момента возмещения вреда от преступного посягательства лица, момента восстановления социальной справедливости путем назначения наказания обвиняемому. Также потерпевший может получить копии процессуальных документов [3. С. 341].

Необходимо отметить, что в рамках производства дознания в сокращенной форме, реализуется непосредственная цель создания данного института, а именно снижение нагрузки на правоохранительные органы и сокращение издержек при исследовании обстоятельств преступного деяния, когда дело не представляет фактической сложности. Не стоит забывать и про то, что по делам, дознание по которым проводилось в сокращенной форме, судебное разбирательство проводится в упрощенном, т. е. в особом порядке, что также способствует разгрузке судебной системы, в частности, сокращает время рассмотрения дела [4. С. 42]. Связано это, прежде всего, с тем, что отсутствует необходимость проведения судебного следствия, так как обвиняемый согласен с фактическими обстоятельствами дела и предъявленным обвинением. Все вышеперечисленное способствует созданию быстрого судопроизводства, что является необходимым в современных реалиях при условиях огромной нагрузки как на суды, так и на органы предварительного расследования.

К сожалению, и в данном случае могут возникать определенные процессуальные трудности. Связано это с тем, что, согласно части 3 ст. 226.3 Уголовно-процессуального кодекса, участники уголовного судопроизводства на любом этапе дела до удаления суда в совещательную комнату могут заявить ходатайство о переходе к общему порядку производства дознания. Одним из мотивов со стороны потерпевшего может быть положение ч. 10 ст. 316 УПК РФ, согласно которой подсудимым не будут возмещаться процессуальные издержки, возникшие в ходе осуществления правосудия. К ходатайству о прекращении дознания в особом порядке подозреваемого может подтолкнуть желание намеренно затянуть рассмотрение дела из личной заинтересованности. В данных случаях может иметь место злоупотребление правом. И это будет огромным шагом назад, возврат к новому расследованию, производимому в общем порядке, и в данном случае не может идти и речи о сокращении сроков и упрощении судопроизводства [5. С. 152]. Но, с другой стороны, данное право дает гарантию достижения объективной истины по делу. Тем не менее думается, что существует потребность в урегулировании данного вопроса и закрепления закрытого перечня оснований для прекращения производства дознания в сокращенной форме.

Заключение. Таким образом, в условиях цифровизации особенностями сокращенной формы дознания являются, прежде всего:

– сжатые сроки досудебного производства, а именно 15 суток со дня вынесения постановления о производстве дознания в сокращенной форме;

– закрытый перечень преступлений, по которым может проводиться дознание в данной форме, установленный п. 1 ч. 3 ст. 150 УПК РФ;

– то, что подозреваемый полностью признает вину в совершенном деянии;

– основанием производства дознания в сокращенной форме является непосредственно ходатайство подозреваемого.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (УПК РФ) // СЗ РФ. 2001 № 52 (ч. 1). Ст. 4921.

2. Гончарова Н. Н., Латыпова Э. Ю., Гончаров Н. А. Проблемы проведения уголовно-процессуальных действий с участием иностранных граждан, на российской территории, также в зданиях посольств и консульств России // Пробелы в российском законодательстве. 2021. Т. 14, № 3. С. 366–372.

3. Латыпова Э. Ю., Гильманов Э. М. Кирпичников Д. В. Роль прокурора в обеспечении права потерпевшего на получение копий процессуальных документов // Актуальные проблемы уголовного права, криминологии, уголовного процесса и уголовно-исполнительного права: теория и практика. материалы IX Международной научно-практической конференции / ред.: Э. Ю. Кузьменко [и др.]. Тамбов: Державинский, 2020. С. 339–347.

4. Закирова Э. Ф. Систем источников (видов) доказательств в уголовном процессе // Доказывание в уголовном процессе: проблемы нормативного регулирования и правоприменения: материалы Международной научно-практической конференции. Н. Новгород, 2023. С. 40–44.

5. Земскова А. В., Ильяшевич Т. А. Заявление ходатайства подозреваемым и потерпевшим при производстве дознания в сокращенной форме // Вестник экономической безопасности. 2021. № 2. С. 152–154.