



ЦИФРОВЫЕ
ТЕХНОЛОГИИ
И ПРАВО

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

СБОРНИК НАУЧНЫХ ТРУДОВ
I МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ
КОНФЕРЕНЦИИ

В шести томах

Том 4

КИУ

ИЗДАТЕЛЬСТВО
«ПОЗНАНИЕ»



ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

I Международная научно-практическая
конференция

Как цитировать: Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегешева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 4. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. – 412 с. EDN: KSNIFB. DOI: http://dx.doi.org/10.21202/978-5-8399-0770-6_2022_4_412

For citation: Digital Technologies and Law: collection of scientific articles of the I International Scientific and Practical Conference (Kazan, September 23, 2022) / eds.: I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova. In 6 vol. Vol. 4. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2022. – 412 p. EDN: KSNIFB. DOI: http://dx.doi.org/10.21202/978-5-8399-0770-6_2022_4_412



Казанский
инновационный
университет имени
В. Г. Тимирязова



Министерство цифрового развития
государственного управления,
информационных технологий
и связи Республики Татарстан

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
I Международной научно-практической конференции

23 сентября 2022 г.
г. Казань

В шести томах
Том 4



Kazan
Innovative University
named after
V. G. Timiryasov



Ministry of Digitalization of Public
Administration, Information
Technologies and Communications
of the Republic of Tatarstan

DIGITAL TECHNOLOGIES AND LAW

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

September 23, 2022

Kazan

In 6 volumes

Volume 4

УДК 004:34(063)

ББК 67с51я43

Ц75

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

Редакторы:

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

Е. А. Громова, кандидат юридических наук, доцент, заместитель директора Юридического института по международной деятельности, доцент кафедры предпринимательского, конкурентного и экологического права Южно-Уральского государственного университета;

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

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

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

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»;

А. В. Минбалева, доктор юридических наук, доцент, заведующий кафедрой информационного права и цифровых технологий Московского государственного юридического университета имени О. Е. Кутафина;

Э. В. Талапина, доктор юридических наук, доктор права (Франция), ведущий научный сотрудник Центра технологий государственного управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации;

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 I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегишева, Е. А. Громова, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 4. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. – 412 с. EDN: KSNIFB. DOI: http://dx.doi.org/10.21202/978-5-8399-0770-6_2022_4_412

ISBN 978-5-8399-0767-6

ISBN 978-5-8399-0770-6 (Том 4)

Вошедшие в сборник научные труды приурочены к Международной научно-практической конференции «Цифровые технологии и право», состоявшейся 23 сентября в Казани в рамках Международного форума Kazan Digital Week 2022, организуемого Кабинетом Министров Республики Татарстан под эгидой Правительства Российской Федерации.

Широкий круг рассмотренных на конференции теоретико-методологических и практикоориентированных, междисциплинарных и отраслевых вопросов связан с приоритетами правового развития цифровых технологий, перспективами правового регулирования цифрового профилирования, экспериментальными и специальными правовыми режимом в сфере создания цифровых инноваций, интеллектуальными правами, трудовыми и связанными с ними отношениями, блокчейн-технологиями, криптовалютой, децентрализованными финансами в правовых реалиях, искусственным интеллектом, робототехникой и др.

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 этом и иных томах сборника 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, молодым исследователям-студентам, магистрантам и аспирантам, всем интересующимся вопросами взаимовлияния цифровых технологий и права.

УДК 004:34(063)

ББК 67с51я43

ISBN 978-5-8399-0767-6

ISBN 978-5-8399-0770-6 (Том 4)

© Авторы, 2022

© Казанский инновационный университет
имени В. Г. Тимирязова, 2022

UDC 004:34(063)
LBC 67c51я43

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

Editors:

Ildar R. Begishev, Doctor of Law, Honored Lawyer of the Republic of Tatarstan, Chief Researcher of Scientific-Research Institute of Digital Technologies and Law, Professor of the Department of Criminal Law and Procedure, Kazan Innovative University named after V. G. Timiryasov;

Elizaveta A. Gromova, PhD (Law), Associate Professor, Deputy Director of the Law Institute on international activity, Associate Professor of the Department of Entrepreneurial, Competition and Environmental Law, South Ural State University;

Maksim V. Zaloilo, PhD (Law), Leading Researcher, Department of the Theory of Law and Interdisciplinary Research of Legislation, Institute of Legislation and Comparative Law under the Government of the Russian Federation;

Irina A. Filipova, PhD (Law), Associate Professor, Associate Professor of the Department of Labor Law and Environmental Law, National Research Lobachevsky State University of Nizhny Novgorod;

Albina A. Shutova, PhD (Law), Senior Researcher of Scientific-Research Institute of Digital Technologies and Law, Associate Professor, Department of Criminal Law and Procedure, Kazan Innovative University named after V. G. Timiryasov

Reviewers:

Anna K. Zharova, Doctor of Law, Associate Professor, Director of the Center for Cyberspace Research, Associate member of the International scientific-educational Center “UNESCO Chair on Copyright, Neighboring, Cultural and Information Rights”, National Research University Higher School of Economics;

Aleksey V. Minbaleev, Doctor of Law, Associate Professor, Head of the Department of Informational Law and Digital Technologies, Kutafin Moscow State Law University;

Elvira V. Talapina, Doctor of Law, Doctor of Law (France), Chief Researcher of the Institute of State and Law of the Russian Academy of Sciences, Leading Researcher of the Center for Public Governance Technologies, Russian Presidential Academy of National Economy and Public Administration;

Yuliya S. Kharitonova, Doctor of Law, Professor, Head of the Center for Legal Research of Artificial Intelligence and Digital Economy, Professor of the Department of Entrepreneurial Law, Lomonosov Moscow State University

Digital Technologies and Law: collection of scientific articles of the I International Scientific and Practical Conference (Kazan, September 23, 2022) / eds.: I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova. In 6 vol. Vol. 4. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2022. – 412 p. EDN: KSNIFB. DOI: http://dx.doi.org/10.21202/978-5-8399-0770-6_2022_4_412

ISBN 978-5-8399-0767-6

ISBN 978-5-8399-0770-6 (Volume 4)

The research works included into the collection are correlated with International Scientific and Practical Conference “Digital Technologies and Law” which took place on September 23 in Kazan during the International Forum Kazan Digital Week 2022, organized by the Cabinet of Ministers of the Republic of Tatarstan under the aegis of the Government of the Russian Federation.

The broad range of theoretical and methodological, practice-oriented, interdisciplinary and sectoral issues is related to the priorities of juridical development of digital technologies, prospects of legal regulation of digital profiling, experimental and special legal regimes in the sphere of digital innovations, intellectual rights, labor and adjacent relations, blockchain technologies, cryptocurrency, decentralized finance in legal realities, artificial intelligence, robotics, etc.

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

The ideas and proposals reflected in this and other volumes are, taken integrally, a key to understanding the intellectual map of meanings, which would be interesting for legal scientists and experts in the sphere of digital technologies, practicing lawyers, representatives of law-making and law-enforcement agencies, state servants and participants of the real economy sector, young researchers – students, graduates and post-graduates, to all those interested in the issues of mutual influence of digital technologies and law.

UDC 004:34(063)
LBC 67c51я43

© Authors, 2022

© Kazan Innovative University named after V.G. Timiryasov, 2022

ISBN 978-5-8399-0767-6

ISBN 978-5-8399-0770-6 (Volume 4)

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ПРАВОВЫХ ОТНОШЕНИЙ (МОЛОДЕЖНОЕ ПРОСТРАНСТВО НАУКИ)

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

МЕСТО ЦИФРОВОЙ ВАЛЮТЫ В СИСТЕМЕ ОБЪЕКТОВ ГРАЖДАНСКИХ ПРАВ

Аннотация. В статье предлагается анализ места цифровой валюты в системе объектов гражданских прав, аргументируется позиция об отсутствии необходимости внесения изменений в Гражданский кодекс Российской Федерации и целесообразности рассмотрения криптовалюты как разновидности имущества, право собственности на которое подтверждается записью, внесенной в публичный реестр, прекращается в случае совершения лицом коррупционного правонарушения.

Ключевые слова: цифровая валюта, криптовалюта, коррупция, коррупционные риски, имущество, объект гражданских прав, блокчейн

THE PLACE OF DIGITAL CURRENCY IN THE SYSTEM OF OBJECTS OF CIVIL LAW RIGHTS

Abstract. The article offers an analysis of the place of digital currency in the system of objects of civil law rights, argues for the position that there is no need to the Civil Code of the Russian Federation and the expediency of considering cryptocurrencies as a type of property, the ownership of which is confirmed by an entry entered in the public register, is terminated if a person commits a corruption offense.

Keywords: Digital currency, Cryptocurrency, Corruption, Corruption risks, Property, Object of civil law rights, Blockchain

В современном мире совершается немалое количество коррупционных правонарушений с использованием цифровой валюты, актуальным вопросом юридической науки на протяжении длительного периода времени являлся вопрос о возможности обращения взыскания на цифровую валюту, применения к ней нормы пп. 8 п. 2 ст. 235 Гражданского кодекса Российской Федерации (далее – ГК РФ). Согласно положениям Закона «О цифровых финансовых активах», вступившего в силу 1 января 2021 г., криптовалюта признается имуществом для целей антикоррупционного законодательства. В случае приобретения цифровой валюты лицом, замещающим государственную или муниципальную должности, на сумму, превышающую его доход за три года, ему необходимо сообщить сведения об источниках доходов, на которые им было приобретено данное имущество. Таким образом, на лиц, замещающих должности, возлагается обязанность представлять в декларации цифровую валюту наряду с прочим имуществом. В целях сокращения числа коррупционных

правонарушений, совершаемых в цифровом пространстве, представляется необходимым введение Центральным банком новой валюты – цифрового рубля. Такой вариант решения проблемы может значительно сократить коррупционные риски, сделать более прозрачными операции с цифровой валютой. 1 апреля 2022 г. было внесено изменение в ст. 17 ФЗ «О контроле за соответствием расходов лиц, замещающих государственные должности, их доходам», в соответствии с которым цифровая валюта признана имуществом, которое можно обратить в собственность государства в случае совершения лицом коррупционного правонарушения. Однако в ст. 128 ГК РФ изменение не было внесено, и правовой режим криптовалюты с позиции гражданского законодательства остается полемическим вопросом. Следует ли признавать криптовалюту отдельным объектом гражданских прав и вносить изменение в ст. 128 ГК или же нужно определять цифровую валюту как иное имущество, которое закреплено в ст. 128 ГК в качестве объекта гражданских прав?

Длительное время в РФ ключевыми проблемами выступали отсутствие правового регулирования цифровой валюты, определение ее правовой сущности, решение вопроса о целесообразности ее рассмотрения как электронных денег или как денежного суррогата. Невозможно отождествлять понятия «виртуальная валюта» и «электронные деньги», поскольку электронные деньги представляют собой лишь цифровое выражение, механизм перевода в электронную форму фиатной валюты, являются законным платежным средством. Исходя из смысла документа, представленного пресс-службой Центрального банка РФ в январе 2014 г., посвященного вопросу совершения сделок с использованием цифровой валюты, оказание юридическими лицами услуг по обмену цифровой валюты на рубль или иностранную валюту можно рассматривать как потенциальное вовлечение субъектов в совершение операций, связанных с легализацией доходов, полученных преступным путем, использование ее в качестве инструмента теневой экономики, что становится возможным ввиду анонимности криптовалюты. Поэтому важным вопросом в части регулирования обращения цифровой валюты является вопрос о предоставлении государственным органам возможности идентификации клиентов, обеспечения прозрачности транзакций. Специфическим признаком цифровой валюты, который может быть использован в целях противодействия совершения с ее использованием правонарушений, является открытость сети, что позволяет при установлении номера счета владельца посмотреть все его транзакции за определенный период.

Центральный банк однажды признал цифровую валюту денежным суррогатом, который не должен использоваться субъектами, функционировать в качестве счетной единицы и включаться в денежное обращение. Не рассматриваются как денежные суррогаты формирующиеся в процессе исполнения сторонами обязательств по гражданско-правовому договору объекты имущественных прав, стимулирующие приобретение товаров, услуг, работ. Исходя из точки зрения, нашедшей отражение в законопроекте об официальном запрете биткоинов, криптовалюту следует признавать денежным суррогатом, поскольку она может быть использована субъектами гражданского оборота в качестве платежного средства, а также может выступать средством обмена, не урегулирована действующим законодательством.

Но проведя сравнительный анализ между данными категориями, можно прийти к выводу о невозможности рассмотрения криптовалюты как денежного суррогата. В приведенном выше законопроекте денежный суррогат определяется как применяемый в качестве средства платежа и средства обмена на деньги объект имущественных прав, не урегулированный законодательством, однако невозможно рассматривать денежный суррогат, имеющий противоправный характер, в качестве объекта имущественных прав, выступающего в гражданском обороте легальным понятием, к тому же в данной редакции законопроекта не учитываются функции цифровой валюты как средства накопления, сбережения, что и объясняет невозможность рассмотрения цифровой валюты в качестве денежного суррогата. Кроме того, криптовалюту в отличие от денежного суррогата достаточно просто трансформировать в денежные средства по номинальной стоимости (цифровой валюте присущ признак мгновенной ликвидности), что нехарактерно для денежного суррогата. Денежному суррогату свойственно установление высоких дисконтов при вторичном обращении, в то время как криптовалюте не присущ такой признак [3. С. 81–91].

В соответствии с законом «О цифровых финансовых активах» криптовалюту следует признавать имуществом в отношении определенных нормативных актов, в частности Федерального закона от 25.12.2008 № 273-ФЗ «О противодействии коррупции», вследствие этого многие цивилисты видят необходимость внесения изменений в ст. 128 ГК, закрепляющую перечень объектов гражданских прав в целях регламентации правового режима цифровой валюты, включения ее в норму в качестве отдельного объекта гражданских прав. ГК РФ называет наличные деньги вещами, в то время как безналичное денежное средство является правом требования, такие расчеты представляют собой передачу определенности об осуществляемых платежах. Если таким образом трактовать безналичные деньги, к ним можно отнести и криптовалюту. Однако безналичные деньги могут выступать не только платежным средством, но и средством сбережения, и лицо может потребовать у банка выдачи ему наличных, что невозможно произвести с криптовалютой. Клиент не может заявить право требования к банку о выдаче ему цифровой валюты, следовательно, невозможно отождествление операций с криптовалютой и безналичных расчетов.

Цифровую валюту нельзя рассматривать как определенное действие, результат работ ввиду отсутствия в отношении по ее созданию и использованию обязательственной природы. Не может выступать она и охраняемым законом результатом творческой деятельности, нематериальным благом, которому свойственна прочная связь с личностью, неотчуждаемость. Кроме того, правоотношения, объектом которых выступает нематериальное благо, носят абсолютный неимущественный характер, что совершенно не применимо к правовому режиму цифровой валюты [1. С. 455–468]. Некоторые авторы полагают, что криптовалюте следует относить к бездокументарным ценным бумагам, но данную позицию можно опровергнуть, проанализировав статью 142 ГК и характерные черты криптовалюты. Выпуск ценной бумаги оформляется соответствующим актом, возлагающим ответственность на определенных лиц за ее исполнение, в то время

как введение в оборот криптовалюты не требует документального оформления и правовой регламентации ответственности определенных субъектов. Кроме того, лицо, осуществляющее учет операций с ценными бумагами, несет ответственность за достоверность сведений, в то время как технология блокчейн не позволяет осуществление контроля и учета операций с криптовалютой одним оператором, следовательно, их точность обеспечивается самими участниками [2. С. 179–192]. Сделки по передаче права на цифровую валюту осуществляются анонимно, чему не препятствует положение ст. 19 ГК, передача валюты другому лицу не порождает обязательственные права. В отличие от криптовалюты, обладающей свойством бесконечного деления, пакет ценных бумаг можно разбить только на строго определенное количество, не подвергая его дальнейшему делению. В настоящей статье приводятся аргументы, подтверждающие целесообразность рассмотрения цифровой валюты как иного имущества, вследствие чего становится возможным обращение на нее взыскания в случае совершения коррупционного правонарушения.

Согласно немецкой доктрине, криптовалюту следует рассматривать как «некодифицированный объект права» в силу того, что она представляет собой определенную имущественную ценность, может выступать объектом относительных правоотношений, предметом сделок ввиду обладания субъектом правами пользования и распоряжения цифровой валютой. По мнению немецких цивилистов, правовой режим криптовалюты нужно рассматривать по аналогии с вещно-правовым режимом животных, нашедшим отражение в Германском гражданском уложении, что не свидетельствует о необходимости их отождествления с юридической природой вещей [5. С. 694–695]. Применяя немецкую концепцию к российской правовой действительности, можно сделать вывод об отсутствии необходимости включения в ст. 128 ГК цифровой валюты в качестве отдельного объекта гражданских прав, целесообразности ее определения как иного имущества, нуждающегося в специальном механизме правового регулирования. Такая точка зрения находит отражение в российской судебной практике, в частности, рассматривая дело о включении содержимого крипто-кошелька в конкурсную массу при реализации процедуры банкротства в апелляционном порядке, суд опроверг позицию суда первой инстанции, пришедшего к выводу о нахождении криптовалюты вне правового поля, о невозможности ее рассмотрения через призму объектов гражданских прав ввиду неприменения к операциям с цифровой валютой механизма государственного регулирования, принудительной силы. Суд апелляционной инстанции аргументировал свою позицию о необходимости рассмотрения криптовалюты в качестве иного имущества путем обоснования ее имущественной ценности и возможности расширительного толкования нормы ст. 128 ГК в части определения понятия «иное имущество». Также суд указал на необходимость применения положения ст. 6 ГК РФ, обуславливающей применение аналогии права при определении прав и обязанностей сторон в случае невозможности использования аналогии закона. Таким образом, криптовалюта представляет собой разновидность цифрового финансового актива, выступает имуществом, выраженном в электронной форме.

Безусловно, криптовалюта может выступать и объектом права собственности лица, но не в классическом понимании данного понятия с точки зрения вещно-правовой конструкции. Содержание юридической категории «право собственности» определяется свойствами вещи, владение которой представляет собой физическое господство над ней. Поскольку цифровая валюта не является вещью, она не выступает объектом права собственности с точки зрения субъективного права. Создание и учет криптовалюты осуществляются в распределенном реестре, представляющем собой базу цифровых транзакций, которые на основе алгоритмов одновременно создаются, хранятся, обновляются на носителях всех пользователей данного реестра, в чем и заключается сущность технологии блокчейн. Поскольку все действия, процессы, связанные со внесением, хранением транзакций, производятся одновременно на всех носителях, можно говорить о публичном характере распределенного реестра. Участники обладают информацией обо всех совершенных транзакциях, контролируют друг друга, проверяют действительность операций, не допускают внесение недостоверной информации другими лицами, в чем и заключается децентрализованный характер данной системы [4. С. 16–23].

Таким образом, цифровая валюта с позиции Закона «О цифровых финансовых активах» выступает имуществом, право собственности на которое подтверждается записью, внесенной в публичный распределенный реестр. Поскольку криптовалюта представляет собой имущество, находящееся на праве собственности у лица, на него может быть обращено взыскание в случае совершения субъектом коррупционного правонарушения.

Список литературы

1. Андрюшин С. А. Криптовалюты: выпуск, обращение и проблемы регулирования // Актуальные проблемы экономики и права. 2020. Т. 14, № 3. С. 455–468.
2. Гонгало Б. М., Новоселова Л. А. Есть ли место «цифровым правам» в системе объектов гражданского права // Пермский юридический альманах. 2019. № 2. С. 179–192.
3. Егорова М. А., Кожевина О. В. Место криптовалюты в системе объектов гражданских прав // Актуальные проблемы российского права. 2020. Т. 15, № 1. С. 81–91.
4. Цинделиани И. А., Нигматулина Л. Б. Криптовалюта как объект гражданско-правового и финансово-правового регулирования // Финансовое право. 2018. № 7. С. 16–23.
5. Kuhlmann N. Bitcoins – Funktionsweise und rechtliche Einordnung der digitalen // CR. 2014. S. 694–695.

Е. В. Авдеева,
руководитель экспертного центра
Общероссийской общественной организации «Деловая Россия»
по уголовно-правовой политике и исполнению судебных актов; доцент,
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации,
А. Ф. Мелик-Оганджян,
студент,
Национальный исследовательский университет
«Высшая школа экономики»

ЦИФРОВИЗАЦИЯ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ПРАВ СУБЪЕКТОВ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Статья посвящена исследованию цифровизации производства по обращениям, уголовного судопроизводства, исполнительного производства и контрольной (надзорной) деятельности для защиты прав субъектов предпринимательской деятельности. Исследовано текущее состояние обозначенных сфер общественных отношений, предложены возможные и перспективные меры по их цифровизации. Сделаны выводы о применимости механизмов цифровизации для формирования системы отслеживания действия сотрудников органов публичной власти со стороны их руководства и надзирающих органов; существенного повышения законности в сфере уголовного судопроизводства; значительной экономии средств федерального бюджета при осуществлении цифровизации; о превентивном действии цифровизации в отношении процессуальных нарушений сотрудников правоохранительных органов; об экономическом значении цифровизации и автоматизации исполнительного производства; о возможностях цифрового противодействия недобросовестного использования контрольных (надзорных) органов как способа хозяйственной конкуренции; необходимости повышения защищенности персональных данных участников цифровых отношений с помощью разработки понятных правил обработки персональных данных лиц, передающих их государственным информационным системам.

Ключевые слова: право, цифровые технологии, цифровое производство по обращениям, электронное уголовное дело, цифровое уголовное судопроизводство, цифровое исполнительное производство, контрольная (надзорная) деятельность

DIGITALIZATION TO IMPROVE THE EFFICIENCY OF THE PROTECTION OF THE RIGHTS OF BUSINESS ENTITIES

Abstract. This article is focused on the research of digitization of reporting proceedings, criminal proceedings, enforcement proceedings and control (supervisory) activities to protect the rights of businessmen. The article examines the current state of the designated areas of social relationships, and proposes possible and promising measures for their digitalization. The following conclusions are drawn about: the applicability of digitalization mechanisms for the formation of a system to monitor the actions

of employees of public authorities by their management and supervisory bodies; a significant increase in the legality of criminal proceedings; significant savings of the federal budget when implementing digitalization; the preventive effect of digitalization to procedural violations of law enforcement officers; the economic significance of digitalization and automation of enforcement proceedings; the possibilities of digital counteraction against unfair use of control (supervisory) bodies as a way of economic competition; the need to improve the protection of personal data of participants in digital relations through the development of clear rules for processing personal data of persons transferring them to state information systems.

Keywords: Law, Digital technologies, Digital appeal proceedings, Electronic criminal proceedings, Digital criminal proceedings, Digital enforcement proceedings, Control (supervisory) activities

Введение. Использование новых цифровых технологий имеет большое значение для развития экономики. Цифровизация прямо положительно влияет на экономический рост, динамику ВВП, а также на производительность во всех отраслях экономики и деятельности человека, включая отправление правосудия и даже ведение боевых действий [13. С. 1, 49]. В настоящее время степень цифровизации экономики показывает положение страны на мировой арене. Вместе с тем вопрос совершенствования политики цифровизации в первую очередь смещен в сферу хозяйственной деятельности и государственных услуг [10. С. 107]. Учитывая успешную цифровизацию экономических процессов и процессов оказания государственных услуг, со временем становится все более актуальной цифровизация процессов по организации защиты прав субъектов предпринимательской деятельности в сфере уголовного преследования, контрольно-надзорной деятельности и исполнительного производства.

В настоящей статье рассматривается проблема использования цифровизации для повышения эффективности защиты прав именно субъектов предпринимательской деятельности по причине специализации Экспертного центра по уголовно-правовой политике и исполнению судебных актов Общероссийской общественной организации «Деловая Россия», но существенная часть выводов и механизмов может быть применена и к иным категориям граждан.

Цифровизация зарекомендовала себя как способ повышения конкурентоспособности, эффективности и производительности процессов. Однако остаются недостаточно разработанными практические вопросы по реализации цифровых технологий в сфере судопроизводства и производства по обращениям. На данном этапе развития правовой культуры среди теоретиков и практиков формируется консенсус по делегированию цифровым технологиям операционных функций с сохранением аналитических и контрольных обязанностей непосредственно за сотрудниками уполномоченных органов и организаций в сфере судопроизводства и производства по обращениям субъектов предпринимательской деятельности.

Производство по обращениям. Одним из ключевых потенциалов цифровизации является возможность повышения прозрачности и контролируемости цифровизируемых процессов. Так, с введением института электронных обращений

существенно облегчается контроль сроков производства по указанным обращениям, т. е. сроков выполнения предусмотренных действий органом власти и направлению заявителю ответов.

Прозрачность сроков совершения предусмотренных законом действий зарекомендовала себя с положительной стороны. Особенную роль цифровизация играет в организации взаимодействия предпринимателей, чьи права были нарушены, и органов публичной власти. Принципиальная важность отраслевых интернет-приемных, особенно относящихся к вопросам предпринимателей, связана с целым комплексом обязательных государственных процедур, в которых предприниматели обязаны участвовать в рамках разрешительной и иной контрольно-надзорной деятельности государства.

В настоящий момент действует прямая линия Генеральной прокуратуры РФ для предпринимателей. Другие интернет-приемные предпринимателей существуют лишь в специализированных государственных и негосударственных органах и организациях, прямо специализирующихся на субъектах предпринимательской деятельности (Уполномоченный при Президенте РФ и уполномоченные в субъектах РФ по защите прав предпринимателей, АНО «Платформа для работы с обращениями предпринимателей» и др.). В органах публичной власти не разрабатываются специализированные интернет-приемные для предпринимателей или других отдельных категорий граждан, за обращениями которых необходимо осуществление повышенного контроля и надзора.

С появлением цифровых механизмов подачи обращений и производства по ним заметно возросла эффективность защиты прав субъектов предпринимательской деятельности и других лиц, в связи с чем необходима дальнейшая работа в направлении внедрения механизмов цифровизации [5. С. 101–102]. В частности, поступление обращения на цифровые платформы позволяет точно отследить момент подачи и регистрация жалобы, а также момент отправки и даже получения ответа. За счет исключения бумажного документооборота возможно существенное снижение расходов на бумагу, а также почтовых расходов в связи с возможностью предоставления ответов посредством сервиса «Госпочта», расположенным в разделе «Уведомления» федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (далее – ЕСИА). При этом достоверность реквизитов документа и ее источника гарантируется специальными техническими методами, именуемыми подписанием электронной цифровой подписью [14. С. 183].

Отслеживание сроков представления ответов гарантирует отсутствие нарушений прав предпринимателей, в случае с которыми каждый лишний день рассмотрения обращения может стоить значительных финансовых затрат, например в случае с незаконным затягиванием срока получения или продления действия соответствующего разрешения. Разумеется, такое нарушение прав влияет не только на частные интересы конкретных лиц, но и на публичные интересы – снижаются

поступления в бюджет, перед сотрудниками организаций возникают риски увольнения, что в совокупности ослабляет экономическую безопасность государства.

Цифровизация производства по обращениям существенно повысит эффективность деятельности и самих органов публичной власти. Механизмы цифрового производства сформируют своего рода CRM-систему (систему управления взаимоотношениями с клиентами, только в данном случае речь идет о широком круге заявителей. – Прим. авт.). Такая CRM-система поможет руководству органа публичной власти отслеживать в режиме реального времени ситуацию с производством по обращениям, в том числе: общее количество обращений в работе, количество обращений в работе на конкретный отдел органа и даже на сотрудника, количество обращений по которым нарушен срок принятия решения или уведомления заявителя о принятом решении, содержание конкретного решения или уведомления заявителя и др. Увеличение контроля за деятельностью сотрудников органа публичной власти позволит руководству указанных органов оперативнее выявлять и реагировать на возможные проявления халатности или коррупциогенных факторов.

Уголовное судопроизводство. Существует обоснованная позиция сторонников цифрового уголовного судопроизводства, в том числе председателя Верховного Суда РФ, который на Совете судей в мае 2022 г. заявил, что проектируемые изменения в УПК РФ позволят подавать процессуальные документы и направлять повестки и уведомления через «Госуслуги». За 2021 г., по словам председателя ВС, судебная система потратила 7,9 млрд руб. на почтовые услуги [3, 12]. Поддерживает введение электронного уголовного дела с помощью разработки специального федерального закона уполномоченный по правам человека – Татьяна Москалькова [7].

Цифровизация уголовного судопроизводства может включать: внедрение электронного документооборота, в том числе межведомственного, с полным или преимущественным вытеснением бумажного документооборота; формирование электронного уголовного дела с хранением в информационной системе уполномоченного органа и обеспечением доступа к нему заинтересованных сторон (в других странах эту функцию на себя принимает Министерство юстиции [15. С. 15]); формирование цифровых площадок хранения аудио- и видеопротоколов процессуальных действий и судебных заседаний с доступом для сторон или зарегистрированных пользователей.

Среди положительных эффектов цифровизации уголовного судопроизводства можно выделить:

1. Точное отслеживание процессуальных сроков рассмотрения ходатайств и заявлений участников уголовного судопроизводства. Так, например, в соответствии с ч. 1 ст. 124 УПК РФ прокурор, руководитель следственного органа рассматривает жалобу в течение трех суток со дня ее получения. В исключительных случаях допускается рассмотрение жалобы в срок до 10 суток, о чем извещается заявитель. Вместе с тем указанный срок практически всегда продлевается до 30 суток и рассмотрение жалобы происходит в общем порядке, установленном ч. 1 ст. 12 Федерального закона от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

2. Автоматическое фиксирование в материалах уголовного дела содержания всех ходатайств и обращений к следователю или дознавателю. Цифровые механизмы позволят исключить физическую возможность следователей и дознавателей по «исключению» из материалов дела ходатайства и заявления участника уголовного судопроизводства, а также приобщенных к ходатайству и заявлению материалов, что играет ключевую роль в достижении объективности и полноты предварительного расследования, соблюдения предусмотренного ст. 15 УПК РФ принципа состязательности сторон [6. С. 82]. Нередко предпринимателям следствие отказывает в приобщении экспертиз в материалы уголовного дела, в такой ситуации при отсутствии экспертизы как приложения к ходатайству или при ее исключении из материалов уголовного дела прокуратура как надзирающий орган при рассмотрении обвинительного заключения в порядке ч. 1 ст. 221 УПК РФ лишается возможности установить все существенные для конкретного дела обстоятельства и принять законное и обоснованное процессуальное решение [1. С. 199–200].

3. Укрепление ведомственного контроля и прокурорского надзора за деятельностью следователей и дознавателей. В условиях цифровизации уголовного судопроизводства соблюдение сроков и содержание процессуальных решений будет находиться в более оперативном контроле со стороны руководства следственных органов и прокуратуры. Более того, наличие системы, которая сигнализирует о наличии нарушений, прямо способствует росту ответственности соответствующих контролируемых и надзирающих лиц, что в свою очередь приведет к общему укреплению законности в ходе предварительного расследования.

4. Существенная экономия средств федерального бюджета. Согласно приложению 11 к Федеральному закону от 6 декабря 2021 г. № 390-ФЗ «О федеральном бюджете на 2022 год и на плановый период 2023 и 2024 годов» стоимость закупки товаров в рамках осуществления предварительного следствия составила 393,16 млн для СК РФ и 7,2 млрд для МВД РФ, существенная часть указанных расходов связана с бумажным документооборотом: непосредственно бумага (о значительных объемах которой можно судить по одному лишь количеству зарегистрированных преступлений в 2021 г. – 2 004 404 [11]), канцелярские товары, почтовые расходы, расходы по транспортировке материалов в рамках межведомственного взаимодействия. Все указанные расходы буквально исчезают в случае цифровизации уголовного судопроизводства.

5. Устраняются возможности оформления процессуальных документов после осуществления процессуальных действий, а также производство процессуальных действий задним числом, т. е. за рамками установленного законом срока.

Отдельно важно указать, что выдвинутые предложения не являются смелыми предположениями, но постепенно становятся объективной реальностью и даже потребностью общества. Со временем все больше стран осуществляет цифровую трансформацию правосудия с помощью перехода на электронный документооборот и внедрения цифровых систем [2. С. 38–39].

Интересным примером выступает суд бразильского города Сан-Пауло (по численности населения сопоставим с Москвой), который в рамках эксперимента «100 % Digital» внедрил цифровую систему электронного документооборота в формате PDF без первоисточника на бумажном носителе, а также систему

по ознакомлению с материалами дела участниками процесса. Итогом реализации эксперимента стало:

1. Сокращение на 70 % времени, осуществления процессуальных действий в сравнении с бумажным процессом, который предполагал физическое создание, перемещение, хранение и извлечение бумаги.

2. Рост производительности судей на 50 % за счет быстрого получения удаленного доступа к информации, на основании которой принимается решение.

3. Рассмотрение новых дел ускорилось на 87 %.

4. За год было сэкономлено 3 миллиона рабочих часов (почти 400 лет), после того как ранее бумажные процессы стали цифровыми [15. С. 8, 12].

5. За 5 лет осуществления эксперимента сэкономлено около 5 тысяч тонн бумаги.

6. За 5 лет осуществления эксперимента удалось избежать 13 507 тонн выбросов CO₂ [15. С. 8].

В Великобритании цифровизация уголовного судопроизводства движется по нескольким направлениям:

- полная цифровизация документооборота между правоохранительными органами и судом, которая значительно ускоряет движение уголовного дела;

- оцифровка и автоматическая сортировка письменных доказательств, которая упрощает их оценку судом [15. С. 15–16].

Существенным эффектом цифровизации уголовного судопроизводства, включающим указанные нами в начале настоящего раздела статьи меры, является повышение доверия предпринимательского сообщества к уголовному судопроизводству и правоохранительной системе в целом. Открытость судебных процессов и доступность ознакомления с ними (в частности, с протоколами судебных заседаний) выведет сферу уголовного судопроизводства из существующего образа закрытости и непредсказуемости.

Разумеется, изложенная в настоящем разделе позиция не является бесспорной и подвергается критике отдельными представителями зарубежной науки. Среди интересных недочетов цифровизации уголовного судопроизводства отмечают:

- существенные единовременные затраты государства на создание цифровых платформ и сервисов вместе с необходимостью обучения персонала по взаимодействию с ним;

- деградация правовой культуры населения с переходом в «пассивных» наблюдателей процесса отправления правосудия [16. С. 508–509];

- формирование физического барьера между властью и гражданами.

В отечественной науке споры в основном направлены на определение необходимой степени цифровизации уголовного судопроизводства. Наряду с положительными эффектами, учеными, исследующими реализацию электронного уголовного судопроизводства в зарубежных странах, признаются и инструментальные издержки ведения электронных уголовных дел:

- 1) отсутствие в действующем уголовно-процессуальном законодательстве специальных норм, регламентирующих процедуру ведения электронного уголовного дела;

- 2) недостаточность ведомственных нормативных актов, конкретизирующих правила пользования цифровыми сервисами;
- 3) неготовность сотрудников низовых звеньев правоохранительных органов к практической реализации нововведений закона в данной сфере деятельности;
- 4) слабая техническая оснащенность рабочих мест должностных лиц, осуществляющих уголовное преследование;
- 5) неосведомленность населения о возможности ведения электронного формата досудебного расследования.

Следует согласиться с профессором О. А. Зайцевым и доцентом О. И. Андреевой, что правовое регулирование применения современных информационно-цифровых технологий в уголовном процессе должно носить централизованный и системный характер, обеспечивающий как публичные, так и частные интересы [2. С. 38–39].

Исполнительное производство. Исполнительное производство является одной из самых цифровизируемых сфер отечественной системы права. С 2020 г. происходит активная интеграция информационных систем ФССП России и ЕСИА, что позволяет реализовать цифровые решения в работе ФССП: на официальном сайте ФССП функционирует сервис «Банк данных исполнительных производств»; должники и взыскатели через «Банк данных исполнительных производств» получают подробную информацию по исполнительным производствам; с помощью ЕСИА должники и взыскатели могут записаться на прием к судебному приставу-исполнителю, а также подавать необходимые заявления и обращения [8].

Дальнейшее развитие цифрового исполнительного производства необходимо осуществлять с помощью внедрения механизмов автоматического наложения при возбуждении исполнительного производства и автоматического снятия в случае погашения задолженности арестов на имущество и счета. Автоматизация этих процессов имеет большое значение для исключения человеческого фактора, с которым связывают в том числе и злоупотребления по срокам совершения тех или иных действий со стороны приставов-исполнителей, что оказывает достаточно серьезное воздействие на хозяйственную деятельность. Так, например, сотрудник ФССП может отправить требование о списании денежных средств со всех счетов физических и юридических лиц, а в случае наличия на всех счетах достаточной суммы списание произойдет неоднократно. Возврат излишне взысканных денежных средств на счета происходит в течение значительного времени, которое исчисляется неделями. Для юридических и физических лиц такие сроки, очевидно, могут быть критичными, а в случае смены судебного пристава-исполнителя или ухода его в отпуск срок возврата может составлять и несколько месяцев. С 2020 г. функционирует сервис «Банк данных исполнительных производств», что открыло возможности для получения через портал подробной информации по исполнительным производствам, включая основание возбуждения, размер задолженности, обо всех действиях судебного пристава-исполнителя, а также наложенных ограничениях. Также была реализована возможность через портал госуслуг подавать ходатайства, заявления, жалобы. Но практика, к сожалению, свидетельствует, что не всегда все происходит без сбоев и в немалом количестве случаев приходится записываться на личный прием.

Также автоматизации подлежит ограничение лиц на выезд за пределы государства. Автоматизация процессов устранил человеческий фактор в осуществле-

нии операционной деятельности и существенно снизит коррупционные риски, в частности в случаях, когда после оплаты задолженности счета компаний продолжают находиться под арестом на протяжении нескольких недель, что особенно критично в части исполнения обязательств по государственным контрактам, тем более в такое время, когда из-за задолженности выпуск критически важной для государства продукции может быть остановлен на недели.

Досудебное обжалование решений контрольных (надзорных) органов. Цифровизация досудебного обжалования решений контрольных (надзорных) органов проходит в достаточно уверенном режиме, что существенно повышает защищенность субъектов предпринимательской деятельности в рамках контрольной (надзорной) деятельности. 1 июля 2021 г., когда вступил в силу Федеральный закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» вместе с нормами об обязательном досудебном порядке обжалования по определенным Правительством РФ видам контроля, с 2023 г. обязательный досудебный порядок будет обязателен в рамках всех видов контроля (надзора). С 1 июля 2021 г. также начал свою работу сервис по подаче жалоб в порядке ст. 40 248-ФЗ с помощью ЕСИА. Сервис позволяет обжаловать решения 31 федерального уполномоченного органа, региональных и муниципальных уполномоченных органов.

До 2024 г. планируется полный перевод всех видов взаимодействий контролируемых субъектов с административными органами исключительно в электронный формат, что, однако, встречает неоднозначную оценку научного сообщества. В первую очередь ученые отмечают малую долю взаимодействия граждан и коммерческих организаций с государственными (муниципальными) органами и бюджетными учреждениями в цифровом виде – 30 % на 2020 г. В связи с чем предлагается оставить возможность сохранения нецифровых форм коммуникации с государственными (муниципальными) органами [4. С. 42].

На наш взгляд, коммуникация с государственными (муниципальными) органами, если и может сохранить диспозитивность форм, то только с дифференциацией требований. Так, например, считаем целесообразной практику предоставления скидок по уплате госпошлин за обращение именно посредством цифровых платформ, а также иных преимуществ, способствующих постепенному полному переходу на цифровую коммуникацию бизнеса и власти. Указанный подход обоснован не только с правовой точки зрения, но и экономической: осложнение контроля и работы с представленными бумажными материалами предполагает дополнительные затраты со стороны государственных (муниципальных) органов, что должно быть компенсировано заявителем, также такие меры будут способствовать добровольному переходу заявителей и контролируемых лиц на цифровые формы коммуникации, которые повышают защищенность прав контролируемых лиц – субъектов предпринимательской деятельности.

На данный момент функционирует ФГИС «Единый реестр контрольных (надзорных) мероприятий» оператором системы является Генеральная прокуратура Российской Федерации, реестр позволяет по идентификаторам организации или контрольного (надзорного) мероприятия выяснить вид государственного контроля

(надзора), класс опасности (категории опасности) деятельности проверяемого лица, даты начала и окончания проведения контрольного (надзорного) мероприятия, цели, задачи, предмет, а также основание проведения контрольного (надзорного) мероприятия, в том числе с указанием заявителей. Также реестр содержит такую важную информацию как результат контрольного (надзорного) мероприятия.

Существенным образом реестр мог быть усовершенствован путем внесения в него информации о наличии или отсутствии его обжалования, в том числе досудебного, и результатов такого обжалования. Следовало бы отдельно сформировать работу с информацией о заявителях, по заявлению которых проводятся внеплановые проверки, чтобы своевременно отслеживать недобросовестную конкуренцию субъектов предпринимательской деятельности, в которую стремятся включить уполномоченные контрольные (надзорные) органы. Соответствующая информация могла бы даже стать основанием для проведения проверки на предмет наличия в действиях лиц правонарушений. Указанный комплекс мер позволил бы снизить недобросовестную конкуренцию субъектов предпринимательской деятельности, что приведет к определенному экономическому росту в высококонкурентных отраслях.

Политика в сфере персональных данных для цифровизации. В сфере цифровизации производства по обращениям, уголовного судопроизводства, исполнительного производства и досудебного обжалования решения контрольных (надзорных) органов принципиальную важность имеет защита персональных данных граждан.

Рост неотвратимости ответственности за нарушение правил обработки персональных данных должен корреспондировать с совместной выработкой государством, предпринимательским сообществом и гражданским обществом понятных правил обработки персональных данных лиц, передающих их государственным информационным системам [9. С. 175]. Только участие всех заинтересованных сторон взаимодействия позволит избежать не только технических, но и политических рисков органов государственной власти, реализующих функции в сфере цифровизации общественных отношений.

В заключение следует отметить, что цифровизация правовой системы стала неотъемлемой частью ее развития, перспективные отрасли регулярно попадают в соответствующие акты стратегического планирования. С учетом необходимости реализации последних научное сообщество в связке с общественными профильными организациями должно выработать устойчивую позицию и комплексный подход по повышению эффективности защиты прав субъектов предпринимательской деятельности с помощью и в процессе цифровизации правовой системы Российской Федерации.

Рассмотренные аспекты цифровизации отдельных отраслей права нуждаются в дальнейшей научной разработке с учетом конкретных механизмов по защите прав субъектов предпринимательской деятельности и обеспечению должного баланса частных и публичных интересов в сфере цифровизации.

Список литературы

1. Александров А. С., Андреева О. И., Зайцев О. А. О перспективах развития российского уголовного судопроизводства в условиях цифровизации // Вестник Томского государственного университета. 2019. № 448. С. 199–207.

2. Андреева О. И., Зайцев О. А. Электронный формат уголовного судопроизводства в Республике Казахстан // Юридический вестник Кубанского государственного университета. 2019. № 1. С. 34–40.
3. Без бумажных протоколов и оглашения полных приговоров: что предложили на Совете судей // Официальный сайт Верховного Суда Российской Федерации. URL: https://www.vsrfr.ru/press_center/mass_media/31154/?ysclid=l84y8dez7n868291924 (дата обращения: 15.09.2022).
4. Гриценко Е. В., Курындин П. А. Цифровизация контрольно-надзорной деятельности: опыт России и Франции // Правоприменение. 2020. Т. 4, № 3. С. 25–45.
5. Горошко И. В. Цифровизация – современный тренд развития правоохранительных органов // Обозреватель. 2022. № 2 (385). С. 98–110.
6. Долгов А. М. Реализация принципа состязательности сторон в условиях цифровизации уголовного процесса // Теория и практика общественного развития. 2020. № 11 (153). С. 80–82.
7. Москалькова выступает за расширение применения цифровых технологий в уголовном процессе // Российское агентство правовой и судебной информации. URL: https://rapsinews.ru/human_rights_protection_news/20220606/307998753.html?ysclid=l8772dxzk5694941029 (дата обращения: 10.09.2022).
8. О реализации суперсервиса цифровое исполнительное производство // Официальный сайт ФССП России. URL: <https://fssp.gov.ru/pressreleases/document28754817/> (дата обращения: 01.03.2022).
9. Саушкин С. О., Синцов Г. В. К вопросу о соотношения институтов защиты персональных данных и защиты неприкосновенности частной жизни // Гуманитарный научный вестник. 2020. № 2. С. 172–177.
10. Скляр М. А., Кудрявцева К. В. Цифровизация: основные направления, преимущества и риски // Экономическое возрождение России. 2019. № 3 (61). С. 103–114.
11. Состояние преступности в Российской Федерации за январь – декабрь 2021 года // ГИАЦ МВД России. URL: <https://мвд.рф/reports/item/28021552/> (дата обращения: 09.09.2022).
12. Уголовный процесс будут оформлять и вести в электронном виде // Российская газета. URL: <https://rg.ru/2022/02/15/ugolovnyj-process-budut-oformliat-i-vesti-v-elektronnom-vide.html?ysclid=l84ygljzt832090617> (дата обращения: 14.09.2022).
13. Харченко Е. Б., Иванов В. Г., Лукьянчик В. Н. Научно-теоретические положения по построению технической основы системы управления Вооруженными Силами Российской Федерации // Военная мысль. 2018. № 8. С. 46–53.
14. Яценко И. И. Понятие, признаки и функции электронного документа в российском законодательстве, науке и уголовно-процессуальной деятельности // Вестник Восточно-Сибирского института МВД России. 2022. № 1 (100). С. 174–186.
15. Finucan L., Sierra E. B., Rajesh N. Smart Courts: Roadmap for Digital Transformation of Justice in Africa. Access Partnership. 2018. 26 p.
16. Moore S. Digital government, public participation and service transformation: the impact of virtual courts // Policy & Politics. 2019. Т. 47, № 3. Pp. 495–509.

М. В. Автомонова,

кандидат юридических наук, доцент,
Ставропольский филиал Российской академии народного хозяйства
и государственной службы при Президенте Российской Федерации

А. Е. Блинкова,

студент,
Ставропольский филиал Российской академии народного хозяйства
и государственной службы при Президенте Российской Федерации

ПРАВОВАЯ ДЕЙСТВИТЕЛЬНОСТЬ ВОСПИТАНИЯ МОЛОДЕЖИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. В статье освещается правовая действительность воспитательной составляющей нашего общества. Идет построение открытой системы, в которой будет существовать, развиваться наша молодежь. Молодежь в нынешних реалиях неразрывно связана с цифровой эпохой, имея практически неограниченный доступ ко всему тому, что есть в мире. Цифровые информационные технологии в процессе правового образования и воспитания подрастающего поколения играют важную роль, поскольку помогают интегрироваться в современное цифровое общество в качестве полноценной личности.

Ключевые слова: общество, право, цифровизация, система, действительность, молодежь

LEGAL VALIDITY OF YOUTH EDUCATION IN CONDITIONS OF DIGITALIZATION

Abstract. The article highlights the legal reality of the educational component of our society. We are building an open system in which our youth will exist and develop. Young people in the current realities are inextricably linked with the digital age, having almost unlimited access to everything that is in the world. Digital information technologies play an important role in the process of legal education and upbringing of the younger generation, as they help to integrate into the modern digital society as a full-fledged personality.

Keywords: Society, Law, Digitalization System, Reality, Youth

Правовое воспитание личности играет огромную роль как на первоначальных этапах ее становления, так и в дальнейшем. Современная образовательная политика Российской Федерации направлена на воспитание нравственно зрелой личности, способной занимать активную гражданскую позицию, жить в соответствии с нормами права [1. С. 143–148].

В современном обществе все большую роль приобретает процесс цифровизации. Популярность гаджетов стремительно набирает обороты. Они охватывают практически все сферы жизни человека. Это влияние, конечно, не обходит стороной обучение, воспитание и развитие подрастающего поколения. Правовое воспитание молодежи необходимо для того, чтобы в будущем предупреждать рост развития преступности, исключать девиантное поведение как отдельных личностей, так и всего поколения в целом. Однако сейчас, при отсутствии должного

контроля за действиями и времяпрепровождением детей в сети Интернет, уровень преступности, наоборот, растет. При использовании интернет-сетей новое поколение не только просматривает, распространяет негативную информацию, вовлекается в преступные действия, но и само становится жертвой негативного влияния. Предотвратить пагубное влияние Сети на правовое развитие возможно в том случае, если будет осуществлен четкий контроль над потоком информации, получаемой молодежью. Ведь если не контролировать огромный объем информации, поступаемый извне, то нельзя предположить, какие будут результаты и последствия влияния на сознание, а тем более на правовое воспитание юного поколения. В этой сфере, безусловно, необходим родительский контроль.

Однако мы считаем, что нельзя однозначно критично относиться к современным технологиям, ведь в их применении, безусловно, есть и свои плюсы. Изначально их внедрение имело своей целью просвещение молодежи, развитие правовой культуры подрастающего поколения. С помощью информационных ресурсов дети, подростки и т. д. формируют и воспитывают себя как личность, обозначают свое «я», свою гражданскую позицию, реализуют свои амбиции. Гражданская позиция – это система позитивных ценностных установок личности на государство, право, гражданское общество, на самого себя как активного гражданина, осуществляющего социально значимую деятельность, ориентированную на общественное благо [2. С. 218–226]. Только стоит делать это на проверенных интернет-порталах и площадках, ведь грань добра и зла очень тонка, особенно если это касается одного клика мышью. Необходимо лишь просто уметь систематизировать, разделять и воспринимать ту информацию, которую ты получаешь. Если в силу отсутствия опыта, юного возраста, некомпетентности индивид не в силах этого сделать, то на помощь ему всегда придут педагоги, родители и преподаватели.

Стоит отметить, что во время обучения в школе учителя очень часто использовали видеоматериалы, презентации и т. д., взятые из медиaprостранства. Большинство из них были весьма интересными и познавательными.

В современных реалиях формирование личности как раз и происходит в основном в информационном пространстве. В этом пространстве он впервые проявляет себя, ищет мечты, цели и стремления, формирует свою правовую культуру. Проявляет себя как с положительной стороны, так иногда и с отрицательной, иногда демонстрирует черты отклоняющегося поведения. Будь то негативные комментарии в социальных сетях или СМС личного характера, оскорбляющие собеседника. Эти действия – показатель того, что необходимо четко и грамотно дозировать то, какие действия ты совершаешь в Сети и какую информацию берешь оттуда. Ведь то, что попало в информационные сети, остается там навсегда.

Список литературы

1. Вестник Костромского государственного университета. Серия: Педагогика. Психология. Социокенетика. 2021. Т. 27, № 1. С. 224.
2. Плотникова Е. Ю. Понятие и сущность гражданской позиции в педагогике и психологии // Научно-педагогическое обозрение (Pedagogical Review). 2019. Вып. 6 (28). С. 218–226.

В. С. Акифьева,

магистрант,

Новосибирский государственный университет экономики и управления

А. И. Рау,

магистрант,

Новосибирский государственный университет экономики и управления

А. И. Сметанина,

магистрант,

Новосибирский государственный университет экономики и управления

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ ЦИФРОВИЗАЦИИ В ПРАВОВОЙ СИСТЕМЕ

Аннотация. Исследование посвящено анализу преимуществ и недостатков цифровизации в правовой системе на примере правового регулирования закупочной деятельности для государственных и муниципальных нужд, сферы исполнительного производства, а также само воздействие цифровизации на гражданско-правовые отношения. На основе совокупного анализа изменений законодательства в ряде сфер сделан вывод относительно перспектив дальнейшей цифровизации и решения существующих проблем.

Ключевые слова: закупки для государственных и муниципальных нужд, исполнительное производство, цифровизация, правовое регулирование, цифровые технологии, исполнительное производство, судебные приставы

BENEFITS AND DISADVANTAGES OF DIGITALIZATION IN THE LEGAL SYSTEM

Abstract. The study analyzes the advantages and disadvantages of digitalization in the legal system on the example of legal regulation of procurement activities for state and municipal needs, the sphere of enforcement proceedings, as well as the very impact of digitalization on civil law relations. Based on a cumulative analysis of changes in legislation in a number of areas, a conclusion is made about the prospects for further digitalization and solutions to existing problems.

Keywords: Purchases for state and municipal needs, Enforcement proceedings, Digitalization, Legal regulation, Digital technologies, Enforcement proceedings, Bailiffs

Отношения в обществе в современных условиях постоянно трансформируются. Правоотношения также претерпевают изменения. Одной из причин изменения правового регулирования ряда сфер общественных отношений является цифровизация. Появление новых процессов и возможностей неизбежно порождает потребность в упорядочении правоотношений, в том числе за счет трансформации правовых норм.

Российское законодательство, в связи с активной цифровизацией, также претерпело ряд изменений. Не претендуя на исследование всех аспектов изменений норм права, хотелось бы уделить внимание отдельным и наиболее значимым.

Первое – это изменение правового регулирования сферы закупок для государственных и муниципальных нужд. Цифровизация данную сферу затронула доста-

точно давно, уже с появления электронных площадок для проведения торгов в целях повышения прозрачности закупок. В 2021 г. были внесены новые изменения [7], в результате которых процесс документа был упрощен и ускорен. В частности, речь идет о введении единых форм электронных документов, об освобождении участников закупочной процедуры от предоставления выписки из ЕГРЮЛ, о сокращении срока с момента подачи заявки и до момента вскрытия конвертов.

Законодательное изменение процедуры закупок, отмеченное выше, имеет определенные преимущества, позволяя сделать саму процедуру более прозрачной, снизить риски злоупотреблений и нагрузку на участников закупок за счет того, что ряд документов организаторы закупки получают из открытых источников.

Следует отметить и еще одно изменение – это необходимость размещения сведений о закупке только ЕИС. Подобное изменение можно расценить как положительное в силу того, что уменьшение объема разрабатываемых документов способствует снижению количества ошибок, в том числе ошибок технического характера, когда на практике одни размещенные документы противоречили другим.

В целом цифровизация сферы закупок имеет ряд достоинств и ряд недостатков. В числе достоинств можно выделить следующие:

- минимизация сговора организаторов и заказчиков с участниками, в том числе в аспекте уменьшения коррупционных рисков;
- уменьшение объема документации, предоставляемой участниками, что в итоге упрощает процедуру закупки и расширяет доступ к ней для участников;
- постепенное достижение целей повышения прозрачности закупок, их единообразия.

При этом есть и недостатки, а именно:

- расходы, которые необходимо нести для организации и содержания электронных площадок, так или иначе должны окупаться. В итоге повышаются риски увеличения затрат для участников, что в итоге уменьшит возможности доступа к закупочным процедурам;
- повышение потребности в специалистах для проведения закупочных процедур, то есть, опять же, увеличение затрат. Помимо этого – расширение круга лиц, имеющих доступ к сведениям о закупках, что потенцирует коррупциогенные риски.

Вторая сфера, где реализуется активная цифровизация и, соответственно, изменяется правовое регулирование, – это сфера исполнительного производства, которую можно определить как одну из наиболее сложных и проблематичных, а также, низкоэффективных. Система исполнительного производства на протяжении многих лет подвергается критике, в том числе по причине сложности и неудобства документооборота, что порождает множество нарушений и судебных разбирательств.

В 2021 г. законодательство об исполнительном производстве было изменено. В числе значимых изменений следует выделить нормативное закрепление возможности принятия ряда решений в форме электронного документа [10]. Участники исполнительного производства (как взыскатели, так и должники) также получили возможность подачи документов в электронном виде через портал Госуслуг. Важным новшеством, уже реализованным в настоящее время, является возможность полу-

чения юридически значимых уведомлений в рамках исполнительного производства в электронном виде, что также реализовано через портал Госуслуг.

Дальнейшая реализация цифровых технологий позволит принимать ряд решений в автоматическом режиме. Например, в автоматическом режиме могут быть приняты решения о возбуждении и о прекращении исполнительного производства. Фактически речь идет об ускорении исполнительного производства, снижения объема документов, которые излагаются на бумажных носителях, а также об ускорении процесса оповещения, который ранее был существенно затруднен вследствие того, что документооборот осуществлялся через «Почту России». Проблем было много – начиная от утраты документов, несвоевременности вручения или возникновения ситуаций невозможности вручения получателю. В комплексе подобные проблемы решались на правовом уровне за счет того, что само по себе направление документов и уведомления о поступлении их получателю приравнивались к получению, что на самом деле не идентично. С одной стороны, минимизировались риски злоупотреблений, а, с другой стороны, нарушались права добросовестных лиц, которые вынуждены были за их восстановлением обращаться в суд.

Как отмечает в своем исследовании А. О. Гамалей, для решения проблем исполнительного производства, разрабатываются различные варианты решений, но большинство из них связано с возможностями цифровизации. В числе подобных вариантов специалист видит построение электронного взаимодействия между рядом государственных органов, имеющих право принятия решений о наложении штрафов, а также органами и организациями, наделенными полномочиями по исполнению таких решений, в том числе за счет исключения из процесса судебных приставов-исполнителей [2. С. 579].

Сама идея интересна, но речь идет исключительно о снижении нагрузки на судебных приставов-исполнителей, а не о повышении качества исполнительного производства. Действующее законодательство России предусматривает возможность исполнения ряда требований о взыскании денежных средств за счет непосредственного обращения взыскателя в банки и иные кредитные организации, минуя службу судебных приставов [6]. Представляется, что полностью исключать судебных приставов-исполнителей из процесса исполнения, в том числе связанного со взысканием денежных средств, не стоит, так как фактически это будет равноценно полному упразднению данной государственной службы. Построение же цифрового взаимодействия необходимо, в том числе в аспекте взаимодействия банков и иных кредитных организаций со службами судебных приставов, а также с иными государственными органами и другими участниками правоотношений.

Можно согласиться с мнением Т. Б. Добриной, которая полагает, что в современных условиях целесообразно развивать систему цифрового взаимодействия службы судебных приставов с разного рода организациями устанавливая при этом максимально краткие сроки исполнения запросов судебных приставов-исполнителей – один рабочий день с момента получения запроса [3. С. 355]. Данные изменения должны быть нормативно закреплены, но перед этим нужно создать материальную базу, т. е. обеспечить наличие у всех участников правоотношений ресурсов для взаимодействия.

Например, далеко не все юридические лица в настоящее время имеют личный кабинет на портале Госуслуг. Как следствие, взаимодействие с ними через данную систему невозможно, что увеличивает срок исполнения запросов и негативно отражается на построении самого процесса исполнения. Поэтому можно утверждать, что цифровизация предполагает изначальное создание условий для внедрения технологий, а уже после этого формировать правовые основы и регламентировать соответствующие общественные отношения.

Основная проблема реализации процесса цифровизации во всех сферах – это проблема построения его через портал Госуслуг. Безусловно, подобный портал удобен, но значительная часть населения России ограничена в возможности пользоваться сетью Интернет и, как следствие, порталом Госуслуг. Определенная часть населения так и не овладела навыками пользования порталами.

Обязанность пользоваться порталом Госуслуг либо иными системами, законодательно не закреплена. Представляется, что и вводить подобную обязанность на уровень законов не следует, потому что в итоге часть населения нашей страны окажется в ситуации невозможности разрешения ряда вопросов.

Подобная проблема не связана с недостатками правового регулирования. Она имеет практический характер, будучи обусловленной отсутствием доступа в сеть Интернет, отсутствием необходимого оборудования (в том числе по причине бедности), отсутствием навыков. Следовательно, максимальная цифровизация многих процессов взаимодействия в обществе будет возможна только при условии обеспечения обучения и повышения уровня доходов населения, когда каждый гражданин будет располагать необходимым оборудованием и средствами на оплату доступа в сеть Интернет.

И еще один аспект, связанный с цифровизацией и ее правовым регулированием, которому хотелось уделить внимание, – это гражданско-правовая модель регулирования цифровых технологий.

Цифровизация уже достаточно давно затронула сферу гражданских правоотношений. Появление цифровых активов, возможности учета ценных бумаг на цифровых носителях, а также многое иное не осталось без внимания законодателя. Как следствие правовое регулирование подверглось изменению, также, как и процесс взаимодействия, предполагающий все более активное внедрение современных технологий.

Вопрос о цифровых правах и их регулировании нормами гражданского права становится все более актуальным. При этом регламентация подобного рода отношений еще только начинает развиваться, концептуальной модели, которая была бы принята всеми исследователями, пока не существует. В плане определения сущности гражданско-правовой модели регулирования анализируемой сферы, заслуживает внимания работа А. А. Карцихия, в которой данный автор предлагает собственное определение. При характеристике гражданско-правовой модели регулирования цифровых прав автор делает акцент на том, что правовое регулирование должно затрагивать не только возникновение указанных прав, но и определение субъектного состава участников правоотношений, а также способа распоряжения данными правами [4. С. 13].

Мнение А. А. Карцихия представляется правильным. Цифровой гражданский оборот специфичен, он не может быть идентичен в полной мере обороту иных

объектов гражданских прав уже в силу того, что сам по себе объект радикально отличается от иных объектов, которые ранее были включены в нормы ГК РФ [5]. Фиксация цифровых прав, совершение сделок в отношении объектов цифровых прав имеет свою специфику. Сам по себе факт нематериальности объекта правоотношений в настоящее время уже не является новшеством, с учетом совершенствования норм права, однако в остальном применительно к сфере регулирования цифровых прав присутствуют свои особенности, отдельные аспекты еще недостаточно проработаны и являются дискуссионными.

В числе наиболее дискуссионных вопросов последних лет можно выявить вопрос о криптовалюте, ее признании и возможности использования. Д. Ю. Вяжев и О. В. Тищенко отмечают, что технологии блокчейн и возможности криптовалюты в современных условиях можно рассматривать как один из способов решения «дефицита долгосрочного финансирования», как способов решения ряда государственных проблем [1. С. 35].

Безусловно, в свете популярности криптовалюты утверждение Д. Ю. Вяжева и О. В. Тищенко допустимо рассматривать как правильное, однако стоит учитывать следующие моменты. При всех преимуществах – высокая стоимость, доступность и прочее, криптовалюта еще не признана в качестве альтернативной существующим денежным системам. Она не является официальной валютой какого-либо государства, вследствие чего вопрос обеспеченности становится спорным. Если, например, рубль обеспечен за счет золотовалютного запаса, гарантирован со стороны государства, то у криптовалюты подобных гарантий нет.

Во-вторых, система блокчейн не предполагает персонификации владельца, вследствие чего сложным становится вопрос о возможности защиты собственных прав в ситуации посягательств.

Российское законодательство, признавая допустимость существования цифровой валюты, а также использования ее в качестве средства платежа, существенно ограничивает подобные правоотношения. В частности, в настоящее время установлен запрет для российских юридических и физических лиц – резидентов России по смыслу, придаваемому этому термину налоговым законодательством, принимать цифровую валюту в качестве встречного представления по сделкам [7]. Возможность защиты прав для данной категории лиц применительно к цифровой валюте также ограничена, будучи поставленной под условие, а именно: если данные лица информировали об обладании цифровой валютой, а сделки в отношении нее совершали в соответствии с нормами права России.

Иными словами, российский законодатель, признавая объективный факт существования криптовалюты и потребности в регламентации правоотношений, связанных с ее оборотом, устанавливает максимальные ограничения. Представляется, что причиной служит именно необеспеченность валюты и анонимность. Условие о сообщении о себе, как о владельце криптовалюты, делает более прозрачным построение дальнейших правоотношений. Полная анонимность может стать причиной невозможности защиты права, потому что как таковое право сложно установить, доказать его принадлежность.

Проиллюстрировать современную проблематику правоотношений, связанных с оборотом криптовалюты на территории России и возможностью защиты право-

обладателей, можно на примере дела, которое было рассмотрено Арбитражным судом Поволжского округа [9].

Предметом спора по указанному делу стало взыскание убытков в виде упущенной выгоды, возникших вследствие повреждения оборудования в результате аварии в системе электросетей. В удовлетворении иска было отказано и суд кассационной инстанции счел правовую позицию нижестоящих истцов, правомерной.

Обосновывая собственные выводы, Арбитражный суд Поволжского округа заострил внимание на следующих моментах. Во-первых, правоотношения возникли до момента принятия федерального закона, регламентирующего вопросы оборота цифровой валюты, а по аналогии законодательство в данном случае неприменимо. Во-вторых, никаких допустимых доказательств тому, что в случае исправности оборудования истец получил бы доход, не представлено. В-третьих, криптовалюта бесконтрольна и может рассматриваться как суррогат денежных средств, не имеющий обеспечения. Акцент Арбитражный суд Поволжского округа сделал и на том, что операции, связанные с криптовалютой, носят «спекулятивный характер», сопряжены с риском потери стоимости при игре на бирже. Неограниченность круга анонимных субъектов, выпускающих криптовалюту, также имеет значение в аспекте возможности защиты права, особенно с учетом отсутствия специальной документации.

Приведенный пример наглядно демонстрирует тот факт, что даже при наличии федерального закона, определяющего сущность криптовалюты, она до настоящего времени не может быть определена как полноценный объект гражданского оборота. Цифровые права, подлежащие защите на территории России, имеют иной характер. Они связаны преимущественно с ценными бумагами и цифровыми права, которые регистрируемы, предполагают конкретизацию субъекта права. Следовательно, в данной части правовое регулирование еще недостаточно.

Важным является и момент «спекулятивности» сделок с криптовалютой, как определяют это суды. Здесь просматривается определенное сходство с защитой прав применительно к играм и пари, где защита предоставляется только в той части, в какой присутствует государственное участие. Отделенность криптовалюты от признанных валют становится причиной непредоставления ее владельцам правовой защиты.

Что касается взыскания упущенной выгоды применительно к криптовалюте, то здесь ситуация практически равнозначна иным, связанным с доказыванием упущенной выгоды, т. е. присутствует проблема, которая в целом еще не нашла своего разрешения в правоприменительной практике нашего государства. Как следствие доказать, что выгоды действительно могла быть получена, но упущена по вине того или иного лица, крайне сложно.

Поэтому можно утверждать, что гражданско-правовое регулирование цифровых технологий в России практически не развито, но оно необходимо. Само по себе существование таких технологий предопределяет потребность признания и защиты прав. Можно предположить, что в обозримом будущем цифровые технологии будут приоритетны, особенно в свете тотальной цифровизации и стремления государства максимально внедрить их. Однако оборот и правовое регулирование полностью зависит от того, насколько контролируемыми будут цифровые технологии, будут ли созданы средства идентификации владельцев, средства защиты от нарушения права.

Подводя итог, можно утверждать, что цифровизация в целом и ее правовая регламентация, необходимы. В сферах государственных и муниципальных закупок, в сфере исполнительного производства, а также в плане использования цифровых технологий применительно к гражданско-правовым отношениям, присутствует немало достоинств, что свидетельствует о необходимости сохранения и развития цифровизации, а также дальнейшей проработки правового регулирования. Выявленные проблемы и недостатки, отчасти обусловлены несовершенством правовой регламентации, и могут быть устранены за счет совершенствования норм права, а отчасти, обусловлены низким уровнем правосознания, в результате чего, возникают разного рода злоупотребления и правонарушения той или иной степени опасности для общества.

Список литературы

1. Вяжев, Д. Ю. Криптовалюта как объект гражданско-правового регулирования / Д. Ю. Вяжев, О. В. Тищенко // Проблемы социально-экономического развития Сибири. 2022. № 2 (48). С. 35–38.
2. Гамалей, А. О. К вопросу о направлениях цифровизации исполнительного производства / А. О. Гамалей // Охрана и защита прав и законных интересов в современном праве: сборник статей по результатам Международной научно-практ. конф. В 2 т. Симферополь, 2022. С. 576–581.
3. Добрина, Т. Б. Цифровизация исполнительного производства в России. Обращение взыскания на цифровые активы / Т. Б. Добрина // Скиф. Вопросы студенческой науки. 2021. № 4 (56). С. 353–359.
4. Карцихия, А. А. Гражданско-правовая модель регулирования цифровых технологий: автореф. дис. ... д-ра юрид. наук / Карцихия Александр Амиранович. Москва, 2019. 44 с.
5. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Собрание законодательства РФ. 1994. № 32. Ст. 3301.
6. Федеральный закон от 02.10.2007 № 229-ФЗ «Об исполнительном производстве» // Собрание законодательства РФ. 2007. № 41. Ст. 4849.
7. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. URL: www.pravo.gov.ru. 31.07.2021.
8. Федеральный закон от 02.07.2021 № 360-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. URL: www.pravo.gov.ru. 02.07.2021.
9. Постановление Арбитражного суда Поволжского округа от 08.10.2021 № Ф06-9272/2021 по делу № А57-15876/2020 // Справочно-правовая система «КонсультантПлюс».
10. Федеральный закон от 21.12.2021 № 417-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. URL: www.pravo.gov.ru. 21.12.2021.

Д. О. Александров,

студент,

Российский государственный университет
нефти и газа имени И. М. Губкина

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ СУДОСТРОЕНИЯ

Аннотация. В связи с активным развитием технологии искусственного интеллекта и ее внедрением в судостроительную и другие отрасли растет потребность в упорядочивании этих отношений посредством правового регулирования. Целью данного исследования является проведение анализа юридических средств и методов, регулирующих положения искусственного интеллекта в сфере судостроения. Анализ проводится на основе национального и международного права.

Ключевые слова: право, цифровые технологии, искусственный интеллект, беспилотные суда, автономность, морское право, международная морская организация

PROBLEMS OF LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE IN SHIPBUILDING

Abstract. Due to active development of artificial intelligence technology and its implementation in shipbuilding and other industries, there is a growing need to streamline these relationships through legal regulation. The purpose of this research is to analyze the legal means and methods that regulate the provisions of artificial intelligence in shipbuilding. The analysis is carried out on the basis of national and international law.

Keywords: Law, Digital technology, Artificial intelligence, Unmanned ships, Automation, Maritime law, International Maritime Organisation

На сегодняшний день транспортировка грузов по морю является одним из самых перспективных направлений. Морские перевозки, во-первых, универсальны, так как можно перевозить различные виды грузов. Во-вторых, они более безопасны по сравнению с автомобильными грузоперевозками. В-третьих, стоимость такой перевозки значительно ниже, чем авиационная перевозка. Стоит отметить, что сегодня также активно развивается и такая технология, как искусственный интеллект. Ввиду того, что законодательное регулирование различных стран не успевает за темпами развития искусственного интеллекта, многие отрасли не спешат внедрять такие технологии в свои процессы ввиду отсутствия нормативной базы для них.

На данный момент между государствами нет согласованного определения термина «искусственный интеллект», хотя в Европейском союзе уже принят Законопроект об искусственном интеллекте Artificial Intelligence Act, где под искусственным интеллектом (далее – ИИ) понимается «программное обеспечение, которое может для заданного набора задач, определяемого человеком, генерировать выходные данные, такие как контент, прогнозы, рекомендации или решения, влияющие на среду,

с которыми оно взаимодействует» [8]. Такую технологию относят к машинному обучению: она совершенствуется благодаря анализу новых данных и их применению.

В сфере судостроения данное технологическое решение позволит на порядок улучшить анализ данных для принятия решений, оптимизировать маршруты, повысить безопасность и эффективность. ИИ также улучшает систему навигации, тем самым устраняя вероятность столкновения судов в открытом море. Помимо этого, ИИ обеспечивает высокий уровень безопасности на судах, поскольку 70–95 % аварий вызваны ошибками человека. Таким образом, благодаря искусственному интеллекту можно повысить необходимые показатели и спрогнозировать потенциальные риски.

Однако интеграция ИИ – процесс небыстрый, поэтому компании и страны, которые уже разрабатывают необходимые условия для ИИ, в конечном счете будут в выигрышном положении. При этом необходима определенная стратегия по внедрению ИИ в систему государства или в конкретные отрасли. Несмотря на то, что ИИ ассоциируется с автономностью, полной независимостью от человека он обладать не сможет: ИИ зависит от данных, которые поступают к нему от человека, поэтому искусственный интеллект лишь дополняет его работу, тем самым человек может заниматься решением более масштабных задач.

На сегодняшний день нет четко выработанной нормативно-правовой базы для ИИ. Однако в различных странах уже приняты национальные стратегии развития технологий ИИ. В России Указом Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» утверждена национальная стратегия развития искусственного интеллекта на период до 2030 года. Среди основных принципов развития и использования технологий ИИ, соблюдение которых обязательно при реализации данной стратегии, выделяют: защиту прав и свобод человека, безопасность, прозрачность, технологический суверенитет, целостность инновационного цикла, поддержку конкуренции и разумную бережливость [5].

Кроме того, в 2021 г. Межотраслевой альянс в сфере искусственного интеллекта совместно с Аналитическим центром при Правительстве РФ и Министерством экономического развития России разработал «Кодекс этики искусственного интеллекта». Данный документ носит рекомендательный характер, следовательно, нарушение его принципов не будет влечь юридическую ответственность. Среди основных принципов внедрения ИИ, изложенных в кодексе, выделяют: прозрачность, правдивость, ответственность, надежность, инклюзивность, беспристрастность, безопасность и конфиденциальность [1]. Для обеспечения безопасной работы с данными акторы, лица, принимающие участие в функционировании ИИ, должны соблюдать и обеспечивать охрану и защиту персональных данных в соответствии с законодательством РФ о персональных данных и охраняемых законом тайн. Как мы видим, законодательное регулирование в области ИИ находится в разработке.

С учетом внедрения ИИ в отрасль судостроения необходимы будут отдельные нормы, учитывающие ее специфику. В частности, нужно будет определить отношения ИИ с морским правом, поскольку уже сегодня в гаванях появляются автономные беспилотные суда, которыми управляет искусственный интеллект. У таких судов международная морская организация выделяет четыре вида автономности:

- 1) судно с автоматизированными процессами, при этом экипаж на борту осуществляет контроль судовых систем и функций;
- 2) судно с дистанционным контролем и экипажем. Судно контролируется дистанционно, при этом на борту экипаж контролирует и эксплуатирует системы и функции судна;
- 3) судно с дистанционным контролем без экипажа. При таком виде автономности судно может контролироваться из любой точки мира;
- 4) полностью автономное судно. Операционная система такого судна способна функционировать самостоятельно [6].

На данный момент проходят испытания морских автономных надводных судов (МАНС), которые относятся ко 2-й и 3-й группам вышеприведенной классификации. Они перевозят грузы практически без участия человека. Их автономность достигается путем мониторинга и дистанционного контроля с близлежащего пилотируемого судна, берегового центра управления, а также при помощи искусственного интеллекта, который функционирует самостоятельно.

Проблема правового регулирования ИИ в сфере судостроения также заключается в том, что морское право, международные конвенции и коммерческое право регулируют только деятельность, связанную с пилотируемыми судами. Так, согласно ст. 94 Конвенции Организации Объединенных Наций по морскому праву (UNCLOS) (заключена в г. Монтего-Бее 10.12.1982), суда государств флага обязаны находиться под командованием капитана и офицеров, обладающих соответствующей квалификацией, а экипаж по квалификации и численности должен соответствовать типу, размерам, механизмам и оборудованию судна [4]. Для государств, подписавших конвенции международной морской организации (ИМО) и ООН, эти конвенции имеют силу только в рамках их национального законодательства. Следовательно, каждая страна, которую опросила МКК, имела свое мнение на счет капитана и экипажа, но при этом вопрос их нахождения на беспилотном судне остается открытым.

Конвенция о Международных правилах предупреждения столкновений судов в море (МППСС-72) (с изменениями на 29 ноября 2001 г.) – первый документ ИМО, который изучают начинающие палубные офицеры. В правиле 2а говорится: «Ничто в настоящих Правилах не может освободить ни судно, ни его владельца, ни капитана, ни экипаж от ответственности за последствия, могущие произойти от невыполнения этих Правил или от пренебрежения какой-либо предосторожностью, соблюдение которой требуется обычной морской практикой или особыми обстоятельствами данного случая» [2]. С учетом данного правила при использовании автономного судна, непонятно кто будет нести ответственность, и кто будет считаться капитаном, что вызывает трудности в соответствии с действующими конвенциями.

Юридический комитет ИМО стремится выработать определенные нормативные положения, которые бы устанавливали правила и для беспилотных судов. Международный морской комитет (МКК) в 2018 г. начал рассматривать вопрос международной нормативной базы для беспилотных судов в рамках следующих конвенций: SOLAS (Международная конвенция по охране человеческой жизни на море), Полярный кодекс, MARPOL (Международная конвенция по предотвращению

загрязнения с судов), COLREGs (Международные правила предупреждения столкновения судов в море), STCW (Международная конвенция о подготовке и дипломировании моряков и несении вахты) и др.

Как и в случае с международными конвенциями, отсутствие соглашений о регулировании ИИ является ключевой проблемой. Основные соглашения, регулирующие морские перевозки грузов (Гаагские, Гаагско-Висбийские, Гамбургские и Роттердамские правила), возлагают на перевозчика обязанность обеспечить мореходность судна и проявить должную осмотрительность для предотвращения инцидентов [3]. В случае предъявления иска суды должны будут решить, работают ли системы поддержки ИИ или автономные суда в пользу перевозчика или против него.

В 2018 г. Международным союзом морского страхования было отмечено, что в связи с ростом автоматизации процессов и внедрением МАНС снизится уровень рисков и потерь в судоходстве, но в то же время появятся риски, которые ранее не были количественно оценены или застрахованы. МКК было установлено, что в большинстве юрисдикций принята ответственность за столкновение судов на основе вины. Таким образом, судовладелец и производитель программного обеспечения могут нести ответственность за столкновение, вызванное полностью автономным судом [7]. Решением в данной ситуации может послужить введение строгой ответственности как запасного варианта для ситуаций, когда вина не очевидна. Но это противоречит действующим международным конвенциям об ответственности и распределении вины.

Таким образом, мы убедились, что проблема правового регулирования ИИ в области судостроения сегодня недостаточно изучена, к тому же сегодня в мире нет утвержденных нормативно-правовых баз для автономных судов с ИИ, поскольку данная технология появилась относительно недавно. При этом многие страны уже разрабатывают законодательство, которое бы регулировало эти отношения. А в некоторых странах уже приняты конкретные стратегии на пути внедрения ИИ в различные отрасли.

Список литературы

1. Кодекс этики искусственного интеллекта от 26.10.2021. URL: <https://bit.ly/3VcSOBA> (дата обращения: 11.09.2022).
2. Конвенция о Международных правилах предупреждения столкновений судов в море (МППСС-72) (с изменениями на 29 ноября 2001 г.). URL: https://sailme.eu/wp-content/uploads/2018/10/sailme.eu_mppss72.pdf (дата обращения: 11.09.2022).
3. Конвенция Организации Объединенных Наций о договорах полностью или частичной морской международной перевозки грузов (Нью-Йорк, 2008 г.) (Роттердамские правила). URL: <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ru/rotterdam-rules-r.pdf> (дата обращения: 11.09.2022).
4. Конвенция Организации Объединенных Наций по морскому праву (UNCLOS) (заключена в г. Монтего-Бее 10.12.1982) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_121270/559d2de5eff5d39a33139e0fe14c0427f4644b2a/ (дата обращения: 11.09.2022).

5. Указ Президента Российской Федерации «О развитии искусственного интеллекта в Российской Федерации» от 10.10.2019 № 490. URL: <http://static.kremlin.ru/media/events/files/ru/АН4x6HgKWANwVtMOfPDhcbRpvd1HCCsv.pdf> (дата обращения: 11.09.2022).

6. Autonomous shipping of 14.11.2016. URL: <https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx> (дата обращения: 11.09.2022).

7. How will AI impact Maritime Law of 18.06.2021. URL: <https://thetius.com/how-will-ai-impact-maritime-law/> (дата обращения: 11.09.2022)

8. The Artificial Intelligence Act of 21.04.2021. URL: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF (дата обращения: 11.09.2022).

Л. И. Антонова,

студент,

Дальневосточный федеральный университет

К. А. Корнева,

студент,

Дальневосточный федеральный университет

К ВОПРОСУ О «МЯГКОМ ПРАВЕ» И САМОРЕГУЛИРОВАНИИ В КОДЕКСАХ ЭТИКИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. В современном мире взаимосвязь между законом и этикой становится все более очевидной. В статье рассматриваются этические вопросы регулирования искусственного интеллекта (ИИ), возможности регулирования ИИ с помощью мягкого права и саморегулирования. Проанализирована правовая природа кодексов этики. По данному вопросу приводится зарубежный и отечественный опыт.

Ключевые слова: искусственный интеллект, право, законодательство, мягкое право, интеллектуальные технологии, правовое регулирование, этика

ON SOFT LAW AND SELF-REGULATION IN CODES OF ETHICS FOR ARTIFICIAL INTELLIGENCE

Abstract. In the modern world, the interconnection between law and ethics is becoming more and more obvious. The article deals with ethical issues of artificial intelligence regulation. The possibilities of regulation through soft law and self-regulation are considered. The authors analyzed the legal nature of codes of ethics, reviewed the foreign experience in comparison with the domestic reality.

Keywords: Artificial intelligence, Law, Legislation, Soft law, Smart technology, Legal regulation, Ethics

В современном мире стало все очевиднее смешение права и этики. При этом их связь оказалась настолько прочной, что многие правовые решения теперь вытекают из интерпретации различных этических вопросов. Некоторые из этих вопросов касаются непосредственно искусственного интеллекта (далее – ИИ).

Применение ИИ в любой сфере имеет огромные перспективы, так как повышает комфорт людей, оптимизирует производство, развивает науки. При этом использование систем ИИ также создает этические проблемы, например, не стоит забывать о «проблеме вагонетки», которую применительно к ИИ упоминают все чаще. И это не удивительно. Как правильно отмечается, большинство людей недооценивают реальный уровень автономности этих систем, «разумность» и способность оказывать влияние на человека [3. С. 178].

Поэтому необходимо подчеркнуть важность наличия прочной этической базы для использования этой технологии, учитывая реальное влияние, которое она оказывает на жизнь людей уже в наши дни. Когда мы говорим об этических принципах, мы имеем в виду прозрачность, безопасность, равенство, инклюзивность, конфиденциальность. Важно, чтобы при использовании ИИ, лица, ответственные за разработку этих систем и введение их в эксплуатацию, делали это с соблюдением выше представленных принципов. Поскольку никто не учится без входных данных, тем более ИИ, его необходимо снабжать информацией и данными, которые соответствуют этическим принципам.

Чтобы полностью реализовать потенциал ИИ, необходимо зафиксировать основные этические принципы в едином документе, доступном для каждого. Такие документы активно создаются как на международном, так и национальном уровне, и называются Кодексами этики ИИ. Кодекс этики ИИ призван вдохновлять и направлять этическое поведение всех специалистов по ИИ, включая нынешних и начинающих практиков, инструкторов, студентов, влиятельных лиц и всех, кто эффективно использует технологии ИИ, и, в частности, он должен действовать в качестве этического стандарта. Кроме того, Кодекс служит основой для устранения нарушений в случае их возникновения.

Руководящие принципы, помимо рекомендации «надежности и безопасности систем», сосредоточены в первую очередь на центральной роли людей в их отношениях с искусственным интеллектом: человеческое достоинство и свобода должны стоять на первом месте.

Так, в России потребность в Национальном кодексе этики ИИ была зафиксирована в Указе Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», Распоряжении Правительства РФ от 19 августа 2020 г. № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г.».

В результате был создан Национальный кодекс этики в сфере ИИ, авторами которого выступают Альянс в сфере искусственного интеллекта РФ, Аналитический центр при Правительстве РФ и Минэкономразвития.

Созданию Кодекса, очевидно, предшествовал возникший всеобъемлющий вопрос: «Достаточно ли существующей нормативно-правовой базы или необходимы инновационные формы регулирования»? И, как видно из пояснений авторов Российского кодекса этики, выбор был сделан в пользу так называемого мягкого права, когда нормы представляют собой рекомендации для государственных органов и компаний, использующих системы искусственного интеллекта.

Учитывая традиционную потребность российского законодателя «все строго, четко, нормативно зарегулировать или запретить», ставка на «мягкое право» была сделана не случайно. Как правильно отмечают исследователи, излишняя урегулированность потенциальных рисков может быть неэффективной. Регулирующие органы и государство должны способствовать объективному устойчивому, но в то же время осторожному развитию ИИ [2. С. 32–46].

Изначально концепция мягкого права была разработана в рамках науки международного права, которая представляет собой совокупность формализованных общих положений (норм, принципов, критериев, стандартов), которые не имеют юридически обязательного характера, не обеспечены официальными санкциями и соблюдаются добровольно в силу авторитетности их создателей, заинтересованности адресатов и целенаправленного социального «давления», которое оказывает на потенциальных (и фактических) нарушителей соответствующее сообщество [1. С. 28].

Однако проблематика «мягкого права» с некоторого момента уже не ограничивается международно-правовым уровнем. Мягко-правовая концепция начинает активно использоваться при характеристике многочисленных внутригосударственных актов, которые формально не вписываются в систему традиционных источников права, но имеют важное значение для правотворчества и правоприменения [1. С. 50].

В российской практике уже много примеров актов, формально не относящихся к законодательству, но вместе с тем содержащих общие стандарты и правила, которые можно называть мягким правом. Это самые разные документы – от концепций и стратегий развития до актов локального саморегулирования негосударственных сообществ и ассоциаций.

Так, например, Кодекс профессиональной деятельности адвоката, хотя и является актом, выработанным, изменяемым и поддерживаемым представителями профессионального сообщества – адвокатами, обеспечивается также и государством, что достигается благодаря наличию в специализированном законодательстве федерального уровня указаний на обязательность применения такого акта.

В любом случае перенос мягко-правовой концепции на уровень национальных правовых систем позволяет включить в правовой дискурс разнообразные (подчас – довольно неоднородные) документы, примером которых служит как раз Национальный кодекс этики ИИ. Он не относится к официальным источникам права, формально не является юридически обязательными, но прямо или косвенно задействуются в сложной и многоуровневой системе правового регулирования.

Справедливо отмечается, что традиционное законодательное регулирование может содержать в себе элементы мягкого права, когда этические принципы включаются в текст закона, что придает им необходимую обязательность исполнения [5. С. 91].

В данном контексте важно рассмотреть опыт других стран. Так, в Китае пока не существует универсального законодательства по регулированию ИИ. Однако в соответствии с их Планом по развитию ИИ нового поколения, «зонтичные» нормативно-правовые акты в этой сфере должны быть приняты к 2025 году [4. С. 197–204].

«Зонтичная» конструкция характеризуется провозглашением основной идеи в актах «мягкого права» и возможной последующей реализацией через официально закрепленные нормы права. В данном случае мы понимаем, что власти Китая идут по пути первоначального провозглашения концептуальных идей в сфере ИИ, только затем на их основе принятия отраслевых законов. Эти решения свидетельствуют о широкой распространенности мягко-правовой концепции в правотворчестве КНР в вопросах ИИ.

Важным событием для Китая в сфере ИИ стало представление в 2021 году Министерством науки и техники Китая правил этического взаимодействия с ИИ. Этот кодекс в большей степени обращен к бизнесу, работающему с высокими технологиями ИИ, для того чтобы в последующем каждая корпорация разработала собственные этические кодексы. Такая практика довольно распространена в КНР, так, интернет-компании Baidu и Tencent, работающая в сфере распознавания голоса Megvii, телекоммуникационная компания Huawei и финансовая корпорация Ping An, утвердили документы, в которых затрагиваются этические принципы их работы с ИИ [4. С. 197–204].

Саморегулирование также способствует принятию мягкого права. Это значит, что компании и потребители зачастую могут принимать определенное участие в формулировании правил и контроле за их соблюдением. В некоторых случаях уполномоченные государственные органы могут контролировать соблюдение предусмотренных законодательством процедур, относящихся в той или иной степени к мягкому праву.

В преамбуле отечественного кодекса этики в сфере ИИ также закреплена возможность саморегулирования, в частности, указано следующее: «Положения Кодекса могут быть расширены и/или конкретизированы для отдельных групп Акторов ИИ в отраслевых или локальных документах по этике в сфере ИИ с учетом развития технологий, особенностей решаемых задач, класса и назначения СИИ, уровня возможных рисков, а также специфического контекста и среды, в которой применяются СИИ».

Индустрия ИИ имеет огромный общемировой потенциал для будущего развития, поэтому вопросу его правового регулирования с точки зрения информационной безопасности и гарантиям реализации прав человека и гражданина нужно уделять все большее значение. На примере опыта КНР мы формулируем вывод о важности участия непосредственно тех компаний, которые работают с технологиями ИИ, в работе по формулированию этических правил и принципов посредством саморегулирования в корпоративных кодексах этики ИИ. Этот вывод базируется на отсутствии у законодателя специфического опыта непосредственно такого обращения с технологиями ИИ, которое сумеет выявить потенциальные риски нарушения прав граждан и создания угроз обществу, что входит в компетенцию конкретных специалистов в этой сфере.

Таким образом, использование «мягкого права» в сфере ИИ является объективно необходимым для того, чтобы государство определяло общую направленность и основные тенденции внедрения ИИ, а разработчики помогали государству и всему обществу безопасно преодолевать издержки и недостатки технологий ИИ. У многих граждан по-прежнему имеется недоверие к ИИ, поэтому необходимо саморегулирование корпораций, т. е. носители специальных знаний помогут адаптировать норма-

тивное регулирование в этой сфере. Мы считаем, что «мягкая сила права» способна стать инструментом в обретении согласия и доверия между ИИ и гражданами.

Список литературы

1. Демин А. В. «Мягкое право»: практика применения в контексте российского и международного права. 2018. // СПС «КонсультантПлюс». URL: http://www.consultant.ru/edu/student/download_books/book/myagkoe_pravo_praktika_primeneniya_v_kontekste_rossijskogo_i_mezhdunarodnogo_prava/ (дата обращения: 16.09.2022).
2. Ивлиев Г. П., Егорова М. А. Юридическая проблематика правового статуса искусственного интеллекта и продуктов, созданных системами искусственного интеллекта // Журнал российского права. 2022. № 6. С. 32–46.
3. Лизикова М. С. Этические и правовые вопросы развития искусственного интеллекта // Труды Института государства и права РАН. 2022. № 1. URL: <https://cyberleninka.ru/article/n/eticheskie-i-pravovye-voprosy-razvitiya-iskusstvennogo-intellekta> (дата обращения: 16.09.2022).
4. Незнамов А. В. Глобальный атлас регулирования искусственного интеллекта. Восточный вектор / под ред. А. В. Незнамова. Москва: Альпина ПРО, 2022.
5. Попова А. В. Мягкое право как структурная часть комплексной отрасли российского законодательства в сфере правовой регламентации искусственного интеллекта // Вестник Московского городского педагогического университета. Серия: Юридические науки. 2021. № 4 (44). С. 86–93.

Д. А. Артамонова,
студент,

Уральский государственный юридический университет
имени В. Ф. Яковлева

А. М. Киселев,
студент,

Уральский государственный юридический университет
имени В. Ф. Яковлева

О ВОПРОСЕ ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ТРУДОВОМ ПРАВЕ

Аннотация. Цифровые технологии в настоящее время проникают во все сферы жизни человека. Юриспруденция, и в частности трудовое право, не стала исключением. Новейшие технологии изменяют не только сами правоотношения, но и процесс их правового регулирования. Теперь для того, чтобы подписать трудовой договор или же передать отчетность в госинспекцию труда, не обязательно взаимодействовать лично, так как появляются новые сервисы, позволяющие оперативно решать данные вопросы даже на расстоянии. Такие возможности создают благоприятную среду для работников и работодателей, способствуют ускорению процесса поиска работы, упрощают процесс увольнения по инициативе работника, упрощают получение пособия по безработице и т. д. Однако не все изменения и нововведения приводят к глобальным изменениям, некоторые проекты в области

модернизации трудовых отношений не оправдывают надежду, которую возлагали на них разработчики. Данные изменения и их последствия анализируются в настоящем исследовании.

Ключевые слова: трудовое право, цифровизация, работа, работодатель, работник, интернет-портал, технологии

ON THE ISSUE OF THE USE OF DIGITAL TECHNOLOGIES IN LABOR LAW

Abstract. Digital technologies are currently penetrating into all spheres of human life. Jurisprudence and, in particular, labor law are no exception. The latest technologies change not only the legal relations themselves, but also the process of their legal regulation. Now, in order to sign an employment contract or submit reports to the State Labor Inspectorate, it is not necessary to interact personally, as new services are emerging that allow you to quickly resolve these issues even at a distance. Such opportunities create a favorable environment for employees and employers, accelerate the job search process, simplify the process of dismissal on the initiative of an employee, simplify the receipt of unemployment benefits, etc. However, not all changes and innovations lead to global changes, some projects in the field of modernization of labor relations do not justify all the hopes that were pinned on them by developers. We will try to analyze these changes and their consequences in our.

Keywords: Labor law, Digitalization, Work, Employer, Employee, Web portal, Technologies

Проблема безработицы является довольно актуальной и остросоциальной в Российской Федерации, тысячи людей находятся в постоянном поиске достойной работы, хорошего заработка и социальных гарантий. Прежние методы поиска работы устаревают и уже не дают должных результатов. Изменения, которые происходят в современных реалиях в трудовом пространстве [3. С. 2], способствуют созданию новых систем для упрощения поиска вакансий и соответствующих кадров, взаимодействия работодателей с работниками, службами и инспекциями. Одним из таких ресурсов является «Работа в России», который в законодательстве определяется как информационно-аналитическая система [2].

Данный ресурс задумывался как некий цифровой помощник для граждан и работодателей, который помогал бы эффективно и безопасно выстраивать отношения между ними. Однако даже нормативное закрепление портала как государственной информационно-аналитической системы, не помогло избежать проблем и рисков, которые возникают у аналогов негосударственного характера.

Во-первых, из-за недостаточного освещения в средствах массовой информации и иных источниках, ресурс не стал востребован у большого количества пользователей, что привело к снижению эффективности выполнения его первоначальных задач по упрощению поиска работы и электронному взаимодействию между субъектами трудовых отношений.

Во-вторых, данный ресурс не подлежит постоянному и всеобъемлющему контролю и надзору со стороны органов охраны труда, что приводит к появлению

со стороны недобросовестных работодателей вакансий, которые не соответствуют действительности или каком-либо аспекте нарушают права потенциального работника. Не ведется наблюдение за действиями работодателя после закрытия вакансии и направления кандидату уведомления о том, что он прошел отбор.

В-третьих, несмотря на закрепление данного ресурса в Законе Российской Федерации от 19 апреля 1991 г. № 1032-1 «О занятости населения в Российской Федерации», описание всех его возможностей, целей и задач, он не получает отклика среди работодателей. На данный момент не существует никаких мер поощрения за использование платформы, которая поддерживается и развивается государством. Хотя для развития данного проекта необходима стимуляция работодателей, донесение до них информации обо всех плюсах данного способа поиска новых работников.

В данный момент продолжаются дискуссии о передаче данной платформе части функций, которые выполняют центры занятости. Конечно, это бы привело к популяризации и развитию сервиса, однако без должного регулирования мы не можем говорить о возможности полной замены привычных нам способов содействия гражданам в поиске работы [1. С. 118].

В настоящее время мы можем судить об этом сервисе как об эффективном цифровом инструменте по содействию в трудоустройстве граждан. Проведенное исследование позволило сделать вывод, что данный портал нуждается в совершенствовании с целью построения эффективного взаимодействия между соискателями и работодателями, а также между работодателями и государственными органами власти, работниками. Как одну из основных проблем неэффективности созданной системы можно определить отсутствие контроля и надзора в отношении ее функционирования. Возможно, данные функции было бы разумно возложить на органы федеральной инспекции труда, так как подобный функционал вне онлайн среды относится к их компетенции.

Измененный портал был бы оптимальным средством в борьбе с безработицей и содействовал гражданам в поиске подходящих вакансий, что положительно бы сказалась на поддержании экономического благополучия населения Российской Федерации, а также развитии бизнеса и экономики страны.

Список литературы

1. Ивочкин И. В. Методы и способы поиска работы в современной России // Сборник статей V Международной научно-практической конференции. Пенза, 12 ноября 2021 года. – Пенза: Наука и просвещение, 2021. С. 117–120. EDN: ZLLULO
2. О занятости населения в Российской Федерации: Закон РФ от 19.04.1991 № 1032-1 // Собрание законодательства РФ. 1996. № 17. Ст. 1915
3. Dokuchaev V. A. Digital transformation: New drivers and new risks // International Conference on Engineering Management of Communication and Technology, EMCTECH 2020 – Proceedings, Vienna, 20–22 October, 2020. Vienna, 2020. P. 9261544. DOI: 10.1109/EMCTECH49634.2020.9261544

Е. С. Астрякова,

студент,

Белорусский государственный университет транспорта

А. В. Шевцова,

студент,

Белорусский государственный университет транспорта

К ПРОБЛЕМЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОТДЕЛЬНЫХ ОБЪЕКТОВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Аннотация. Необходимость адаптации правовых институтов, в том числе института гражданского права, к новым вызовам в регулировании гражданского оборота, обусловлена тем, что на данный момент цифровые технологии оказывают воздействие на экономические, политические, социальные и другие процессы в обществе. Цель исследования заключается в рассмотрении объектов цифрового и виртуального имущества для определения их принадлежности относительно норм права.

Ключевые слова: право, цифровые технологии, виртуальное имущество, цифровое имущество, правовые акты, указы

ON THE PROBLEM OF LEGAL REGULATION OF THE SEPARATION OF INTELLECTUAL PROPERTY OBJECTS

Abstract. The need to adapt legal institutions, including the institution of civil law, to new challenges in the regulation of civil circulation is due to the fact that at the moment digital technologies have an impact on economic, political, social and other processes in society. The purpose of the study is to consider the objects of digital and virtual property to determine their ownership in relation to the rule of law.

Keywords: Law, Digital technologies, Virtual property, Digital property, Legal acts, Decrees

Не так давно общество стало информационным, тем самым на данный момент наибольшую ценность представляет информация, выражаемая в виде технологий, научных открытий, другими словами, в виде «неосязаемых объектов». Для таких объектов создано понятие «интеллектуальной собственности». В то же время существуют объекты, которые, не имея материальной формы, в полной мере не относятся и к интеллектуальной собственности, обладая при этом значительной ценностью для субъектов права. По отношению к таким объектам применяют различную терминологию, например, «цифровое имущество (активы)», «виртуальное имущество». В современном мире каждый из нас ежедневно взаимодействует с цифровыми технологиями, поэтому вопрос о защите информации на данный момент стоит на первом месте.

К «виртуальному имуществу» относятся объекты, не имеющие материальной формы и существующие исключительно в виртуальном мире. Как правило, их применение ограничено определенной средой (виртуальной системой), например, онлайн-игры, приложения, социальные сети и др. У данных объектов отсутствуют

признаки объектов интеллектуальной собственности, так как они являются частью компьютерного кода.

Понятие «цифровое имущество» является более обширным и включает в себя цифровую форму других объектов гражданских прав, например, электронные файлы (нематериальные активы торговой фирмы, учетных записей по счетам), аккаунты в социальных сетях, блоги на видеоплатформах, платформы для краудфандинга, трехмерные модели, денежные вклады в криптовалюте, «виртуальное имущество» и т. п.

В свою очередь понятие цифровых активов является наиболее широким из всех рассматриваемых. Оно включает как цифровое имущество, так и объекты, которые не относятся к имуществу или в целом к объектам гражданских прав, но которые имеют цифровую форму.

Обратимся к национальному законодательству в сфере рассматриваемых правовых отношений. Среди источников нормативно правового регулирования цифровой экономики в Республике Беларусь самым значимым считается Декрет Президента Республики Беларусь «О развитии цифровой экономики», который является основным правовым актом и содержит определения для таких понятий, как: майнинг, криптовалюта, оператор криптоплатформы и обмена криптовалют, виртуальный кошелек, владелец токена (цифрового знака), размещение токенов (цифровых знаков), смарт-контракт, токен (цифровой знак). Декрет является основанием правового для создания необходимых условий внедрения в экономику технологии блокчейн и других технологий, которые основываются на принципах децентрализации с целью гарантии безопасного использования данных операций. Немаловажным является то, что данный Декрет закрепляет ряд льгот, мер и правомочий для участников отношений, которые связаны с применением современных технологий. Что позволяет четко определять области возможностей и ограничений в отношении применения данных информационных технологий. Применение современных финансовых технологий дает опыт, необходимый для усовершенствования старых и создания новых институтов правового регулирования в гражданское законодательство Республики Беларусь.

Основой для нормативно правового регулирования цифровой экономики являются следующие указы и законы Президента Республики Беларусь:

- Указ Президента Республики Беларусь от 30.09.2010 № 515 «О некоторых мерах по развитию сети передачи данных в Республике Беларусь»;
- Указ Президента Республики Беларусь от 21.06.2011 № 260 «О навигационной деятельности». Он устанавливает правовые и организационные основы для обеспечения навигационной деятельности в спектре национальной экономики, а также обеспечения защиты и безопасности Беларуси, в том числе цифровую картографическую основу, навигационную и дополнительную информацию;
- Указ Президента Республики Беларусь от 18.04.2019 № 148 «О цифровых банковских технологиях». Он определяет правовой принцип использования информационных систем при совершении банковских, других финансовых операций и иной деятельности;
- Закон Республики Беларусь от 28 декабря 2009 г. «Об электронном документе и электронной цифровой подписи». Он регулирует правовой базис для применения электронных документов и электронной цифровой подписи.

Содержание данных нормативных актов свидетельствует об официальном признании правосубъектности в цифровой среде и выступает фундаментальной основой их защиты на законодательном уровне. В то же время, стоит отметить, что в рамках правовых норм необходимо конкретизировать принадлежность каждого из объектов цифрового имущества к определенной группе объектов гражданских прав в целях более эффективного и единообразного их включения в гражданский оборот. В настоящий момент данный вопрос требует четкого и своевременного решения, в связи со стремительным развитием цифровых технологий.

Список литературы

1. Зубарев А. Е. Цифровая экономика как форма проявления закономерностей развития новой экономики // Вестник Тихоокеанского государственного университета. 2017. С. 177–184.
2. Ли Д.-Д., Баэк Ч., Малипхол С., Йеон Д.-И. Ловушка среднего уровня инноваций. Форсайт. 2019.
3. Салимьянова И. Г., Погорельцев А. С. Цифровая трансформация экономики: анализ трендов в контексте институциональных экономических теорий (Часть 1) // Известия Санкт-Петербургского государственного экономического университета. 2018. С. 7–14.
4. Салимьянова И. Г., Погорельцев А. С. Цифровая трансформация экономики: анализ трендов в контексте институциональных экономических теорий (Часть 2) // Известия Санкт-Петербургского государственного экономического университета. 2019. С. 11–17.
5. Славянов А. С., Хрусталева О. Е. Технологические уклады в инновационном развитии экономики // Научный журнал КубГАУ. 2017. С. 386–402.
6. Markey-Towler B. The competition and evolution of ideas in the public sphere: A new foundation institutional theory // Journal of Institutional Economics. 2019. С. 27–48.
7. Vivarelli M. The middle-income trap: A way out based on technological and structural change // Economic Change and Restructuring. 2016. С. 159–193.

А. М. Ахатова,
студент,

Удмуртский государственный университет

ОБОСНОВАННЫЙ РИСК И КРАЙНЯЯ НЕОБХОДИМОСТЬ КАК ИНСТИТУТЫ УГОЛОВНОГО ПРАВА В СФЕРЕ ДЕЙСТВИЯ «РЕГУЛЯТОРНЫХ ПЕСОЧНИЦ» (ЭКСПЕРИМЕНТАЛЬНЫХ ПРАВОВЫХ РЕЖИМОВ В ОБЛАСТИ ЦИФРОВЫХ ИННОВАЦИЙ)

Аннотация. Информационные технологии в жизни общества приобрели значение ключевого системообразующего фактора. Вместе с тем на фоне высокой потребности в регулировании данной сферы общественных отношений российское законодательство не всегда соответствует требованиям времени. Остается неразрешенным

вопрос относительно определения статуса «сильного искусственного интеллекта», способного к самостоятельному принятию решений на основе заданных алгоритмов. Правовая неопределенность информационной среды ведет к формированию новых рисков, связанных с непредсказуемым характером развития техники и технологии. Особое внимание в работе уделено выработке механизма применения уголовного закона в рамках действия «регуляторных песочниц» в соответствии с Федеральным законом от 31.07.2020 № 258 «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации». Негативные последствия такого эксперимента предлагается рассматривать как обстоятельства, исключающие преступность деяния (обоснованный риск или крайняя необходимость).

Ключевые слова: «регуляторные песочницы», экспериментальные правовые режимы, цифровизация, инновационные технологии, искусственный интеллект, обстоятельства, исключающие преступность деяния, правовые риски, обоснованный риск, крайняя необходимость

JUSTIFIED RISK AND EXTREME NEED AS INSTITUTIONS OF CRIMINAL LAW IN THE SPHERE OF “REGULATORY SANDBOXES” (EXPERIMENTAL LEGAL REGIMES IN THE FIELD OF DIGITAL INNOVATION)

Abstract. Information technologies in the life of society have acquired the importance of a key system-forming factor. At the same time, against the backdrop of a high need to regulate this sphere of public relations, Russian legislation does not always meet the requirements of the time. The question remains unresolved regarding the definition of the status of Artificial general intelligence (AGI) capable of independent decision-making based on given algorithms. The legal uncertainty of the information sphere leads to the formation of new risks associated with the unpredictable nature of technology development. Special attention is paid to the development of a mechanism for the application of criminal law. The author makes a suggestion that the negative consequences of the “experiment” can be considered within the framework of the institute of criminal law – “Circumstances precluding the criminality of the act”: justified risk or extreme need.

Keywords: Regulatory sandboxes, Experimental legal regimes, Information law, Innovation technology, Artificial intelligence, Circumstances excluding criminal element of the act, Legal risk, Justified risk, Extreme need

Динамика развития инновационных технологий свидетельствует об их революционном развитии [19]. Однако необходимо понимать, что перспективы научно-технического прогресса, оказываются двойственными. Наряду с большими возможностями цифровых технологий следует обратить внимание на потенциальную угрозу всей системе общественных отношений, которые нуждаются в уголовно-правовой охране.

Писатель-фантаст А. Азимов сформулировал три закона робототехники, первый из которых гласил, что «робот не способен причинить вред человеку». Данные правила не получили закрепления в юридической практике [15]. Примером может служить следующая ситуация.

Одно из дорожно-транспортных происшествий с участием беспилотного автомобиля Volvo XC 90 компании Uber произошло 19 марта 2018 г. В результате аварии погибла 49-летняя Элейн Херцберг, передвигавшаяся на велосипеде в неположенном месте, в 110 метрах от ближайшего пешеходного перехода во время совершения наезда. В салоне на момент происшествия находился водитель, но транспортное средство функционировало в режиме автопилота. В рамках расследования аварии Национальным советом по безопасности на транспорте (National Transportation Safety Board, NTSB) было выявлено, что за 1,3 секунды до столкновения автомобиль смог определить неопознанный объект и был способен использовать аварийные тормоза. Однако данная система была отключена инженерами данной компании, поскольку нередко случались ложные срабатывания, при которых искусственный интеллект (далее – ИИ, Artificial intelligence, AI) обнаруживал опасные объекты [17].

В последнее время среди ученых-правоведов ведется дискуссия о присвоении ИИ статуса «электронных лиц» (субъекта уголовно-правовых отношений) [4. С. 382–388]. В частности, М. А. Фелипе отмечает, что самостоятельной ответственностью могут быть наделены только «самоосознающие» машины, или, по-иному, «сильный ИИ» (далее – СИИ, Artificial general intelligence, AGI) [18]. Их механизм действий основывается на достаточно строгих правилах поведения, созданных человеком, которые служат базой для дальнейшего самообучения и поиска решений при выполнении конкретных задач. Вместе с тем в основе любого алгоритма лежит целая система допущений (рисков), или, по-другому, отклонений от заданных параметров работы [11. С. 10–12].

К основным причинам неблагоприятных последствий в сфере цифровых инноваций можно отнести следующие факторы:

1) технико-технологические: непредсказуемость поведения, выход из-под контроля человека СИИ, способного к самостоятельному принятию решений на основании полученных базовых алгоритмов. По прогнозам шведского философа профессора Оксфордского университета Ника Бострома, мыслительные процессы искусственного интеллекта к 2075 г. будут неотличимы от человеческого разума [16]. И. Р. Бегишев отмечает, что даже незначительный риск способен перерасти в реальное событие и повлечь общественно-опасные последствия, если не принять необходимых мер для его предотвращения [1. С. 59–76]. В данную группу также можно отнести неправомерный доступ к системе искусственного интеллекта, перепрограммирование объекта, повреждение или модификацию ее функций. [2. С. 564–574];

2) организационно-управленческие, в основе которых выступает человеческий фактор: некомпетентность субъектов и (или) лиц, выполняющих поручение или приказ, выраженное в просчетах и ошибках при принятии решений; противоречия интересов, мнений, взглядов субъектов взаимодействия по поводу выбора стратегии и средств достижения желаемого результата, связанные с рисками;

3) природно-климатические и экологические: связанные с проявлением стихийных сил природы; влияние природно-климатических факторов местности.

По мнению российского ученого-правоведа О. С. Капинус: «Системы ИИ при принятии решений, затрагивающих судьбу человека, не должны основываться на предубеждении и неточности» [3. С. 76–85]. В подтверждении данной позиции,

отмечу, что высшей ценностью любого правового государства является человек. Программируя систему ИИ необходимо исходить из этических соображений, не допуская причинения вреда, прежде всего, человеку. Однако научно-технический прогресс невозможен без принятия решений, не связанных с риском. При этом развитие инновационных технологий – это бизнес, который не заинтересован в необходимости обеспечения безопасности общества в силу дополнительного финансирования [10. С. 74–92].

Согласно доктринальному толкованию, выделяются технический, медицинский, научный, профессиональный, хозяйственный и иные риски, каждый из которых делится на подвиды [8. С. 276–300].

На сегодняшний день урегулирование общественных отношений, возникающих в сфере инновационных технологий, сводится к установлению экспериментальных правовых режимов (далее – ЭПР, «регуляторных песочниц»), в соответствии с Федеральным законом от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (в ред. Федерального закона от 02.07.2021 № 331-ФЗ), применяемых в целях установления механизмов тестирования в реальных правоотношениях технологий, которые на данный момент запрещено использовать повсеместно в силу различных причин [13]. Механизм правового регулирования отличается от общеустановленного и предполагает ограничение по применению определенных норм законодательства, действующих в пределах территории, определяемым ФЗ № 258 в целях ускорения внедрения новых продуктов и услуг в сфере цифровых инноваций.

Негативные последствия такого эксперимента могут рассматриваться в рамках института уголовного права «Обстоятельств, исключаящих преступность деяния»: обоснованного риска (ст. 41 УК РФ) или крайней необходимости (ст. 39 УК РФ). С одной стороны, это даст возможность снять уголовно-правовые запреты на пути развития достижений науки и техники, а с другой, оградить общество от потенциальных угроз.

Федеральный закон № 258 (в ред. от 02.07.2021 № 331-ФЗ) в ст. 1 содержит восемь основных направлений разработки, апробации и внедрения цифровых инноваций:

- 1) медицинская деятельность;
- 2) проектирование;
- 3) сельское хозяйство;
- 4) финансовый рынок;
- 5) продажа товаров, работ, услуг дистанционным способом;
- 6) архитектурно-строительное проектирование;
- 7) предоставление государственных и муниципальных услуг и осуществление государственного контроля (надзора) и муниципального контроля;
- 8) промышленное производство (промышленность);
- 9) иные направления [13].

К иным направлениям, согласно Постановлению Правительства Российской Федерации от 18.12.2020 № 2149 (ред. от 24.06.2022) «Об установлении направлений разработки, апробации и внедрения цифровых инноваций, по которым может уста-

навливаться экспериментальной правовой режим в сфере цифровых инноваций», относятся направления разработки, апробации и внедрения цифровых инноваций «Связь» и «Электроэнергетика» [7].

Таким образом, экспериментальные правовые режимы создаются только под новые продукты и услуги, не имеющие аналогов. Зачастую с этим отсутствует и законодательство, регулирующее данные виды деятельности. Для испытания новых инновационных технологий в соответствии с ФЗ № 258 создаются наиболее благоприятные условия:

- определяются правила для конкретного круга лиц (субъектов ЭПР и иных лиц, принимающие непосредственное участие в проведении эксперимента),
- на определенное время (как правило, срок ЭПР не может превышать трех лет, если Правительством РФ не принято решение о продлении еще на один год),
- на определенной территории (если применимо) [13].

В п. 2 ст. 9 ФЗ № 258 (в ред. от 02.07.2021 № 331-ФЗ) закона инициатор предложения обязан стремиться к «минимизации рисков причинения вреда жизни, здоровью или имуществу человека...», при этом п. 6 ст. 5 данного ФЗ гласит, что «предметом специального регулирования не могут быть правоотношения, возникшие при осуществлении деятельности, связанной с высоким риском нанесения ущерба жизненно важным интересам личности, общества и государства...» [13]. Указанное в законе понятие «высокий риск» носит оценочный характер. Возникает возможность для его широкого и неоднозначного толкования. А это, в свою очередь, влечет нарушение принципов уголовного законодательства вследствие чрезмерного усмотрения правоприменителя. В ее основе лежит не совсем точное понимание сущности экспериментальной деятельности, которая невозможна без риска ввиду информационной неопределенности. Иными словами, субъект экспериментального правового режима порой действует «вслепую», что и может породить неблагоприятные последствия. В оценке оправданности ошибки необходимо исходить из баланса высокой цели и ее реальной достижимости в конкретных условиях [9. С. 55]. При масштабном исследовании и негативный результат также может быть полезен с точки зрения дальнейшей перспективы развития науки.

Необходимо конкретизировать в Федеральном законе № 258 (в ред. от 02.07.2021 № 331-ФЗ) указанное понятие («высокий риск») или заменить на «необоснованный риск» в соответствии со ст. 41 УК РФ. Таким образом, логическая структура соответствующей нормы будет выглядеть следующим образом: «Предметом специального регулирования не могут быть правоотношения, возникшие при осуществлении деятельности, связанной с необоснованным риском нанесения ущерба жизненно важным интересам личности, общества и государства».

Нормативное определение «обоснованного риска», данное ст. 41 УК РФ, является универсальным и применимым в различных ситуациях. Исходя из положений нормы закона, умышленное причинение вреда субъектом ЭПР исключается, так как лицо, предпринимая необходимые меры предосторожности, рассчитывает на благоприятный исход, отсутствует осознание «неизбежности причинения вреда». А главной движимой целью является достижение общественно полезного итогового результата.

Тогда как предоставление субъектом ЭПР заведомо недостоверных сведений при приобретении им соответствующего статуса, согласно п. «б» ст. 12 Федерального закона № 258 (в ред. от 02.07.2021 № 331-ФЗ) должно являться не только основанием для прекращения его деятельности, но и подпадать под нормы уголовного законодательства. Содеянное следует квалифицировать по статьям Особенной части (ст. 159, 201, 285 УК РФ) и по наступившим последствиям в совокупности.

В Федеральном законе № 258 (в ред. от 02.07.2021 № 331-ФЗ) и сопутствующих проектах внедрения цифровых инноваций отсутствует норма, указывающая на обязательность субъекта ЭПР осуществлять необходимые меры для защиты персональных данных от иных неправомерных действий, влекущих угрозу как человеку, так и государству в целом. Так, большие данные (Big Data), с одной стороны, открывают новые технологические перспективы в ряде сфер деятельности: медицине, производстве, торговле и множестве других, а с другой – требует решения ряд взаимосвязанных правовых вопросов. Использование возможностей цифровых технологий гражданами, на территории которого будет задействован экспериментальный правовой режим, будет порождать оставление информационных следов, содержащих информацию о конкретном человеке, что может стать объектом не только анализа, но и манипуляций.

В рамках действия «регуляторных песочниц» возникает проблематика применения ч. 3 ст. 41 УК РФ: «Риск не признается обоснованным, если он заведомо был сопряжен с угрозой для жизни многих людей...» [12]. При этом совершенствование мер безопасности «регуляторных песочниц» («regulatory sandboxes») возможно лишь методом проб и ошибок, поэтому полностью исключить вероятность причинения вреда двум или более лиц является невозможным. Может возникнуть ситуация, когда изначально общественно опасное деяние подпадает под нормы обоснованного риска, но затем лицо, в силу сложившихся обстоятельств, для предотвращения большего ущерба причиняет меньший вред охраняемым уголовным законом интересам. Такие действия должны подпадать под норму ст. 39 УК РФ и рассматриваться как крайняя необходимость.

В рамках действия «регуляторных песочниц» данное обстоятельство может усматриваться, в частности, когда субъект ЭПР, в целях поддержания бесперебойного электричества, не имеет возможности уплатить налоги, поскольку остановка деятельности «искусственной машины», вызванная неуплатой электроэнергии, могла привести к техногенной аварии [6]. Однако если субъект ЭПР осознает, что в дальнейшем он будет неспособен выплатить задолженность либо вернуться к платежеспособности, то в данном случае следует говорить о наличии в его действиях состава преступления, предусмотренного ст. 199.2 УК РФ [14].

Применительно к рассматриваемому вопросу «проблему вагонетки» поднял английский философ Филиппа Фут в 1967 г. Его этический эксперимент заключался в том, что вагонетка носится в неисправном состоянии со сломанными тормозами и движется в сторону пятерых людей, привязанных к рельсам. Есть возможность изменить направление вагонетки с помощью стрелки, но тогда погибнет другой человек, привязанный на втором пути. Решение данной ситуации не является однозначным и исходит из умозаключения конкретного лица. В ситуации крайней

необходимости возникает конфликт «более ценного охраняемого блага и менее ценного интереса», когда объектам уголовно-правовых отношений причиняется заведомо меньший вред для спасения большего блага [5]. Проецируя данную ситуацию на систему искусственного интеллекта, можно сказать, что трудным остается вопрос относительно программирования беспилотных транспортных средств, когда на основе заданных алгоритмов он должен будет безошибочно принять решение, рискуя меньшим ради спасения большего.

Таким образом, риск порождается не только процессами субъективного характера, но и такими, существование которых не зависит от сознания человека [10. С. 74–92].

Сильный искусственный интеллект является разумом «особого рода», поэтому юридическая наука и законодательство сталкиваются с проблемой природы и характера возникающих правоотношений. Иными словами, происходящие новые технологические сдвиги настолько концептуальны, что требуют обособленного рассмотрения. Российская Федерация мобилизует свои ресурсы, чтобы занять достойное место в информационном обществе, демонстрируя высокие темпы внедрения цифровых технологий. Однако правовая природа возникающих общественных отношений и их воздействие на общественные процессы требует взвешенного и обоснованного подхода к развитию правового регулирования. Одним из вариантов решения регулирования процесса создания и внедрения новых, малоизученных цифровых технологий явилось введение законодателем экспериментальных правовых режимов, действующих на определенной территории в отношении ее субъектов. Особенность данного правового режима в том, что он «блокирует» отдельные нормы законодательства. В рамках такого эксперимента субъект действует обоснованно, ради достижения общественно полезной цели, и в случае причинения вреда охраняемым уголовным законам интересам его действия не будут являться уголовно наказуемым. Данную ситуацию необходимо рассматривать в рамках гл. 8 УК РФ «Обстоятельства, исключющие преступность деяния»: обоснованного риска (ст. 41 УК РФ) или крайней необходимости (ст. 39 УК РФ). Однако не следует вовсе исключать ответственность за совершенное общественно опасное деяние. В случаях, когда последствия охватывались умыслом субъекта ЭПР, содеянное следует квалифицировать по статьям Особенной части Уголовного кодекса.

Для единообразного применения Федерального закона от 31.07.2020 № 258-ФЗ и эффективной реализации правовой политики в области действия «регуляторных песочниц» необходимо исключить указанное в п. 6 ст. 5 № 258-ФЗ понятие «высокий риск», заменив его на «необоснованный риск» в соответствии со ст. 41 УК РФ.

Список литературы

1. Бегишев, И. Р. Уголовно-правовая охрана общественных отношений, связанных с робототехникой: монография / И. Р. Бегишев. Москва: Проспект, 2022. 384 с.
2. Бегишев, И. Р. Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты / З. И. Хисамова, И. Р. Бегишев // Всероссийский криминологический журнал. 2019. Т. 13, № 4. С. 564–574.

3. Капинус, О. С. Право и технологии: анализ взаимосвязи в новых цифровых реалиях: [анализ соотношения права и технологий в цифровую эпоху] / О. С. Капинус // Обозреватель – Observer. 2021. № 6. С. 76–85.
4. Камалова Г. Г. Некоторые вопросы уголовно-правовой ответственности в сфере применения систем искусственного интеллекта и робототехники // Вестник Удмуртского университета. Серия: Экономика и право. 2020. С. 382–388. URL: <https://www.elibrary.ru/item.asp?id=43153241>
5. Комментарий к Уголовному кодексу РФ в 4 т. Т. 1. Общая часть / В. М. Лебедев [и др.]; отв. ред. В. М. Лебедев. – Москва: Юрайт, 2022. 316 с. (Профессиональные комментарии). ISBN 978–5–534–00044–3 // Образовательная платформа Юрайт [сайт]. URL: <https://urait.ru/bcode/490816> (дата обращения: 07.09.2022).
6. Обзор практики применения судами положений главы 8 Уголовного кодекса Российской Федерации об обстоятельствах, исключающих преступность деяния (утв. Президиумом Верховного Суда РФ 22 мая 2019 г.) URL: http://www.consultant.ru/document/cons_doc_LAW_328041/
7. Постановление Правительства РФ от 18.12.2020 № 2149 «Об установлении направлений разработки, апробации и внедрения цифровых инноваций, по которым может устанавливаться экспериментальный правовой режим в сфере цифровых инноваций») // СПС «КонсультантПлюс».
8. Подройкина И. А. Уголовное право. Общая часть. В 2 т. Т. 1: учебник для вузов / отв. ред.: И. А. Подройкина, Е. В. Серегина, С. И. Улезько. 5-е изд., перераб. и доп. Москва: Юрайт, 2022. 299 с. (Высшее образование). ISBN 978–5–534–12766–9 // Образовательная платформа Юрайт [сайт]. URL: <https://urait.ru/bcode/470468>
9. Рарог, А. И. Медицинское уголовное право: монография / А. И. Рарог, Т. Г. Понятовская, А. А. Бимбинов, В. Н. Воронин, А. И. Рарог. Москва: Проспект, 2022. 576 с. ISBN 978–5–392–36148–9
10. Ровнейко В. В. Обоснованный риск в уголовном праве // Риски в праве: пути решения / Д.Д. Барамидзе, З. З. Зинатуллин, Н. В. Кузнецова [и др.]; под ред. Л. Г. Татьяниной. Москва: Юрлитинформ, 2020. 155 с. ISBN 978–5–4396–2114–9
11. Трофимов, В. В. Информатика. В 2 т. Т. 1: учебник для вузов / В. В. Трофимов, М. И. Барабанова; отв. ред. В. В. Трофимов. 3-е изд., перераб. и доп. Москва: Юрайт, 2022. 553 с. (Высшее образование). ISBN 978–5–534–02613–9 // Образовательная платформа Юрайт [сайт]. URL: <https://urait.ru/bcode/470744>
12. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 07.09.2022).
13. Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // СПС «КонсультантПлюс». от 31.07.2020 № 258-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_358738/ (дата обращения: 07.09.2022).
14. Яни П. С. Уголовная ответственность за сокрытие имущества с целью уклонения от взыскания недоимки // Законность. 2020. № 3.
15. Asimov I. Runaround // Astounding Science Fiction. New York, 1942. 180 p.
16. Bostrom, N. Superintelligence: Paths, Dangers, Strategies / N. Bostrom. Oxford: Oxford Univ. Press, 2014.

17. Uber Finds Deadly Accident Likely Caused By Software Set to Ignore Objects On Road. URL: <https://www.theinformation.com/articles/uber-finds-deadly-accident-likely-caused-by-software-set-to-ignore-objects-on-road?shared=56c9f0114b0bb781>

18. Filipe, M. A. The Legal Status of Artificially Intelligent Robots: Personhood, Taxation and Control / M. A. Filipe // SSRN. Electronic Journal. 2017. Pp. 1–68. URL: <http://dx.doi.org/10.2139/ssrn.2985466>

19. PropTech 2020: The future of real estate // University of Oxford Research. Oxford: Saïd Business School; University of Oxford, 2020. P. 5. URL: <https://www.sbs.ox.ac.uk/sites/default/files/2020-02/proptech2020.pdf>

В. В. Базака,

студент,

Донецкий национальный университет

И. П. Ковалев,

кандидат юридических наук, доцент,

Донецкий национальный университет

К ВОПРОСУ О ЦИФРОВИЗАЦИИ ГРАЖДАНСКОГО ПРОЦЕССА В ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКЕ

Аннотация. В XXI веке, веке технического прогресса, особое внимание следует уделить развитию цифровизации судопроизводства. В теоретическом аспекте одной из основных проблем является классификация цифровых технологий в гражданском судопроизводстве. Автором была предпринята попытка классификации. Поднимается вопрос о необходимости изучения практики Российской Федерации. Уточняются риски при использовании цифрового правосудия.

Ключевые слова: цифровизация гражданского процесса, гражданский процесс, классификация, технологии, доктрина, цифровые технологии, группы

ON THE ISSUE OF DIGITALIZATION OF THE CIVIL PROCESS IN THE DONETSK PEOPLE'S REPUBLIC

Abstract. In the XXI century – the century of technological progress, special attention should be paid to the development of digitalization of legal proceedings. In the theoretical aspect, one of the main problems is the classification of digital technologies in civil proceedings. The author attempted classification. The question of the need to study the practice of the Russian Federation is raised. The risks of using digital justice are clarified.

Keywords: Digitalization of the civil process, Civil process, Classification, Technologies, Doctrine, Digital technologies, Groups

Перспективы дальнейшего развития и внедрения цифровых технологий в различные отрасли юриспруденции обязывают научное сообщество исследовать объект и теоретически осмысливать данное явление. В Донецкой Народной Республике в гражданском судопроизводстве используются различные цифровые технологии, которые различны по своему функциональному и процессуальному назначению.

В период COVID-19, когда были введены ограничения Указом Главы Донецкой Народной Республики от 14 марта 2020 г. № 57 «О введении режима повышенной готовности» цифровизация гражданского процесса активно начала развиваться, о чем свидетельствует постановление Президиума Верховного Суда Донецкой Народной Республики от 17 апреля 2020 г. «Об ограничительных мерах, связанных с работой судов Донецкой Народной Республики, введенных с 21 апреля 2020 года по 30 апреля 2020 года (включительно)».

Затем внедрение цифровых технологий продолжилось в период вооруженного конфликта и по сей день процесс сохраняется. Цифровое правосудие в целом и цифровые технологии в частности имеют преимущество перед «классическим правосудием».

Например, судебное разбирательство с применением различных цифровых технологий происходит быстрее, в данном случае мы подразумеваем сокращение сроков рассмотрения дел. Еще одно из преимуществ цифровизации – бюджетность, благодаря диджитализации судебных документов государство сможет снизить уровень государственной пошлины и иных расходов для судопроизводства, исходя из вышеупомянутых преимуществ, можно сделать вывод о том, что цифровизация судебной системы ведет к доступности правосудия, что также является плюсом.

Актуальность данной работы вызвана необходимостью выработки классификации цифровых технологий с целью улучшения понимания используемых цифровых технологий в гражданском судопроизводстве.

Квалифицировать информационные технологии, используемые в гражданском судопроизводстве, можно на три группы:

- технологии, используемые для передачи информации;
- технологии, используемые для хранения, фиксации и воспроизведения информации;
- технологии, предназначены для переработки информации [3. С. 170].

В первую группу технологий нами были выделены аппаратные и физические средства передачи информации. В данную категорию необходимо отнести различные телекоммуникационные технологии (смартфоны, компьютеры, сервисы для текстовых сообщений (Яндекс.Почта, Gmail и другие)).

Первая категория мало распространена на данный момент в гражданском судопроизводстве. В силу требований к процессуальной форме, распространяющихся также на процессуальную коммуникацию, процесс внедрения средств передачи информации усложняется и требует большего времени.

Для лучшего и быстрого внедрения первой категории цифровых технологий необходимо изменить правовую базу. На наш взгляд, стоит прописать в Гражданско-процессуальном кодексе Донецкой Народной Республики возможность использовать различные телекоммуникационные технологии, но необходимо ослабить процессуальную форму для удобного использования первой группы цифровых технологий.

Но развитие второй группы технологий наблюдается, например, активное использование СМС-сообщений для оповещения участников гражданского судопроизводства, использование почты для передачи файлов в суд, перечисленные возможности, на наш взгляд, можно оценивать как положительное развитие в сфере цифровизации гражданского судопроизводства.

Ко второй группе нами были отнесены технологии, которые выполняют вспомогательную функцию во время гражданского судопроизводства – сбор и представление доказательств. Данные технологии используются, когда появляется необходимость фиксации, хранения и передачи информации о фактах, которые следует рассмотреть суду.

На данный момент категория технологии второй группы наиболее распространены в гражданском судопроизводстве. Примером этому может послужить признание за аудио- и видеозаписями, а также электронными документами доказательственной силы (ч. 1 ст. 56 ГПК ДНР, ч. 2 ст. 60 АПК ДНР, ч. 2 ст. 60 КАС ДНР). Отметим еще один пример – применение технологий аудио- и видеозаписи для ведения протокола (ч. 1 ст. 243 ГПК ДНР, ч. 1 ст. 156 АПК ДНР, ч. 1 ст. 223 КАС ДНР) [1. С. 80; 2. С. 85; 4. С. 56].

При анализе второй группы необходимо отметить причины быстрого внедрения в гражданский процесс. Первая причина – данный вид технологий используется в быту, в связи с чем использование аналогичной техники в гражданском процессе является вполне логичным. Вторая причина – отсутствие затруднений в использовании у различных поколений.

В последнюю, третью, группу цифровых технологий, применяемых в гражданском процессе, нами были выделены аппаратные и физические средства для переработки информации. К ним относятся различные программные обеспечения, предназначенные для оценки информации.

Отметим, что на данный момент в Донецкой Народной Республике третья группа не используется в судебной практике. Нам представляется необходимым для развития третьей группы цифровых технологий разработка аналогов специализированных систем анализа судебной статистики. Например, разработать аналог подсистемы «Судебное делопроизводство и статистика», которая будет выполнять схожие задачи – обеспечивать автоматизированное системное производство, документооборот и систематизацию электронного архива. Также следует разработать аналог подборки судебной практики, например, аналогом подсистемы «Банк судебных решений» может стать «Судебная практика Донецкой Народной Республики», если выкладывать на данную платформу не только ППВС ДНР, но и судебные решения судов общей юрисдикции.

Таким образом, при попытке квалификации цифровых технологий мы пришли к выводу о том, что внедрение данных технологий происходит медленно. Необходимо увеличить темп развития первой и третьей групп в гражданское судопроизводство для улучшения качества защиты прав и интересов личности.

На наш взгляд, также необходимо обратить внимание на доктрину Российской Федерации в сфере цифровых технологий. Нам представляется полезным и необходимым для нашего гражданского судопроизводства перенять федеральную целевую программу «Развитие судебной системы России на 2013–2020 годы», которая была утверждена Постановлением Правительства Российской Федерации от 27.12.2012 № 1406 (ред. от 24.12.2018). Данная программа предусматривает необходимость внедрения в судебную систему, систему принудительного исполнения судебных актов и судебно-экспертную деятельность современных информационно-коммуни-

кационных технологий, позволяющих сформировать инновационный подход к их развитию, а также улучшить качество и сроки осуществления правосудия, качество и оперативность проводимых судебно-экспертными учреждениями экспертиз и обеспечить эффективное исполнение судебных решений [5. С. 13].

Несмотря на преимущества «цифрового правосудия», у перечисленных технологий имеется и ряд минусов. В юридической литературе выделяют: утечку персональных данных лиц, участвующих в деле, легкодоступность изменения документов, что в разы повышает риск недостоверности информации, трудности с опознанием личностей, участвующих в судебном заседании [7. С. 10].

В связи с перечисленными рисками, на наш взгляд, разумным считается создание кибернетических отделов в судебной системе. Задачами данных отделов должно являться:

- выявление лиц, проникнувших незаконно в компьютерную сеть;
- выявление лиц, незаконно распространяющих персональную информацию об участниках судопроизводства;
- борьба с лицами, распространяющими вредоносные программы [6. С. 8].

В заключение отметим, что проведенное исследование и предложенная классификация позволяют сделать вывод о том, что, в условиях активного технического прогресса используемый спектр технологий необходимо увеличивать. Несмотря на очевидную необходимость усовершенствования цифровых технологий, на данном этапе задача имеет ряд трудностей, мы выработали несколько рекомендаций для решения проблем. Во-первых, для внедрения новых цифровых технологий необходимы реформы в законодательстве гражданского процесса Донецкой Народной Республике. Во-вторых, необходимо разработать систему безопасности во избежание рисков связанных с цифровым правосудием, для этого стоит создать кибернетических отделов в судебной системе. В-третьих, мы предлагаем использовать практику нашего ближайшего соседа – Российской Федерации. Например, обратить внимание на доктрину в сфере цифровых технологий, а также разработать аналог аппаратных и физических средств для переработки информации, используемых в ходе гражданского судопроизводства.

Отметим, что в цифровую эпоху использование цифровых технологий в судебном производстве вполне органично и логично, но для качественного и безопасного их внедрения необходимо решить перечисленные проблемы.

Список литературы

1. Арбитражный процессуальный кодекс Донецкой Народной Республики: Закон Донецкой Народной Республики от 30.04.2021 № 277-ІІНС. URL: <https://dnrsovet.su/zakonodatelnaya-deyatelnost/prinyatye/zakony/arbitrazhnyj-protsessualnyj-kodeks-donetskoj-narodnoj-respubliki/>
2. Гражданский процессуальный Кодекс Донецкой Народной Республики: Закон Донецкой Народной Республики от 30.04.2021 № 278-ІІНС. URL: <https://dnrsovet.su/zakonodatelnaya-deyatelnost/prinyatye/zakony/grazhdanskiy-protsessualnyj-kodeks-donetskoj-narodnoj-respubliki/>
3. Девятова С. В., Казарян В. П. Многомерность проблемы коммуникации в цифровом обществе // Российский гуманитарный журнал. 2020. № 3. С. 165–173.

4. Кодекс административного судопроизводства Донецкой Народной Республики: Закон Донецкой Народной Республики от 30.06.2021 № 296-ПНС. URL: <https://dnrsovet.su/zakonodatelnaya-deyatelnost/prinyatye/zakony/kodeks-administrativnogo-sudoproizvodstva-donetskoj-narodnoj-respubliki/>

5. Распоряжение Правительства Российской Федерации от 20.09.2012 № 1735-р «Об утверждении Концепции федеральной целевой программы «Развитие судебной системы России на 2013–2020 годы» // СПС «КонсультантПлюс».

6. Рожкова М. А. Цифровые права: публично-правовая концепция и понятие в российском гражданском праве // Хозяйство и право. 2020. № 10. С. 3–12.

7. Талапина Э. В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. С. 5–17.

М. Ю. Баучкина,

магистрант,

Московский городской педагогический университет

ЭЛЕКТРОННЫЙ ФОРМАТ КАК ПЕРСПЕКТИВНОЕ НАПРАВЛЕНИЕ РАЗВИТИЯ ГОСУДАРСТВЕННЫХ ЗАКУПОК

Аннотация. Система государственных расходов, в том числе институт государственных закупок, на фоне неустойчивого и неопределенного развития рыночной экономики требует совершенствования. Институт государственных и муниципальных закупок постоянно находится в стадии реформирования. Действующая система государственных закупок не позволяет рационально и эффективно использовать финансовые ресурсы. Механизм осуществления закупок на фоне развития современного общества, а также информатизации и электронизации, требуется модернизировать. Повышение качества, а также внедрение инноваций, позволит увеличить прозрачность и эффективность системы закупок. Данное обеспечение является важнейшим инструментом, который позволит обеспечить снижение коррупционных рисков и транзакционных издержек. Важнейшей задачей процесса электронизации системы закупок является обеспечение взаимосвязи этапов процесса проведения закупок с целью реализации общественных интересов, а также интересов коммерческих организаций.

Ключевые слова: государственные закупки, электронный аукцион, информационные ресурсы, инновация

ELECTRONIC FORMAT AS A PROMISING DIRECTION FOR THE DEVELOPMENT OF PUBLIC PROCUREMENT

Abstract. The system of public spending, including the institution of public procurement against the background of unstable and uncertain development of the market economy requires improvement. The Institute of State and Municipal Procurement is constantly being reformed. Unfortunately, the current system of public procurement does not allow rational and efficient use of financial resources. The mechanism of procurement

against the background of the development of modern society, as well as informatization and electronics, needs to be modernized. Improving quality, as well as introducing innovations, will increase the transparency and efficiency of the procurement system. In my opinion, this software is the most important tool that will ensure the reduction of corruption risks and transaction costs. The most important task of the procurement system electronics process is to ensure the interconnection of the stages of the procurement process in order to realize the public interests, as well as the interests of commercial organizations.

Keywords: Public procurement, Electronic auction, Information resources, Innovation

Электронные формы закупок становятся все более распространенными в современных условиях для бюджетных организаций. Особенности этих закупок являются следующие: все этапы закупочного процесса проводятся с использованием информационных систем, начиная с планирования закупки и заканчивая заключением контракта; все документы в рамках такого взаимодействия закрепляются при помощи электронно-цифровой подписи.

Начало внедрению электронных форм в систему государственных и муниципальных закупок стало принятие в 2009 г. Государственной Думой Федерального Собрания Российской Федерации гл. 3.1 Закона № 94-ФЗ, в которой описана процедура электронных аукционов. Вначале такая процедура была принята без энтузиазма, тем не менее стала обязательной при закупке обширного перечня товаров, работ, услуг. Первыми начали работать с новой формой закупок федеральные заказчики, а с 2011 г. и все остальные. В результате такой своеобразной «электронной революции» в области госзаказа Россия значительно опередила западных конкурентов во внедрении закупок при помощи информационных технологий [4. С. 49].

Широкому распространению государственных закупок при помощи электронных аукционов Россия способствовало изучение бразильского опыта здесь, в Бразилии с 2005 г. активно использовалась такая практика при размещении заказов для государственных нужд. Россия и Бразилия оказались лидерами среди стран, изменив вектор закупочного процесса в сторону электронного проведения процедур, обогнав большинство развитых стран. Позднее комиссия ООН UNSITRAL, на основании подобного опыта, включила данную процедуру определения поставщика в реестр рекомендуемых к применению на мировом уровне. Активное использование электронного аукциона позволило таким странам, как Бразилия и Россия, чья экономика, согласно международным стандартам, определяется как развивающаяся, снизить уровень коррупции, который был значителен [5. С. 33–46]. В дальнейшем подобный способ определения поставщика станет не только обязательным для всех заказчиков, но будет приоритетным для увеличения экономии бюджетных средств и оптимизации расходов.

Динамика числа электронных аукционов очень быстро нарастала. Если в 2013 г. через электронный аукцион проводилось менее миллиона закупок, то уже в 2014 г. их количество выросло на 50 % – до полутора миллионов. И, как следствие, экономия средств бюджета (разница между заявленной ценой при проведении закупок и ценой заключенного контракта) составила в 2014 г. 891 млрд руб. против 424 млрд годом ранее [6. С. 4].

Формирование процессов закупок в рамках информационных систем имеет огромный потенциал для дальнейшего развития. Даже страны с более развитой экономикой на настоящее время не используют электронный формат проведения закупочных процедур в полном объеме. В России же затруднение при формировании информационных ресурсов для проведения закупочных процедур в полном объеме связано с безопасностью потоков информации, а также стандартизации систем. Учет российского законодательства, а также его модернизация под постоянный поток инноваций, позволят создать систему закупок в электронной форме, но только при тщательном планировании и с учетом национальной экономики. Для модернизации российских торгов необходимо в полном объеме изучить международный опыт с учетом ошибок, допущенных другими странами, и их причин для формирования эффективной системы [7. С. 168].

Факторами развития системы закупок в рамках цифровизации являются следующие:

- экономический рост и увеличение потребности в ресурсах;
- изменение макрорегуляторов;
- использование как инструмента борьбы с коррупцией;
- простота участия в закупке, сокращение издержек для потенциальных участников торгов;

– интеграция России в мировую электронную закупочную сеть.

Возможности, которые позволяют реализовать электронные закупки:

– полнота и открытость информации об закупочных процедурах для каждого заинтересованного лица;

– неограниченный круг поставщиков, потенциальных участников;

– организация процесса закупок без участия человека, минимизирующая риски коррупционного сговора;

– системный анализ поступающей информации в рамках проведения закупки.

Существенным недостатком проведения аукциона в электронной форме можно определить процесс определения победителя, так как предложение наименьшей цены контракта, хоть и является существенным преимуществом с точки зрения экономики бюджетных средств, однако не всегда позволяет заказчику получить услугу или товар для достижения поставленных результатов. Заказчик в рамках определения поставщика подобным образом лишается возможности выбрать наиболее эффективные условия исполнения контракта, что на данный момент реализовано в проведении конкурсов [2. С. 47].

Электронный аукцион может совершенствоваться в направлении соответствия требованиям международного сообщества. Для этого необходимо внести следующие изменения:

– ценовые предложения должны быть последним этапом проведения открытого аукциона, по аналогии с молоточными аукционами;

– защита информации, которая предоставляется как участниками закупки, так и со стороны поставщика, путем шифрации и кодирования предоставляемых сведений;

– автоматизация работы электронной площадки при рассмотрении заявок электронного аукциона.

Построение системы электронных закупок дает возможность гражданам ознакомиться с графиком закупок, принять участие в обсуждении целесообразности закупок, отследить извещения о закупках на всех уровнях, проанализировать заявки, поданные на участие в закупках, и протоколы, содержащие информацию о результатах проведения процедур [3. С. 41].

Таким образом, необходимая непрерывная модернизация процедур электронных закупок должна осуществляться с учетом следующих принципов:

- наличие определенной стратегии реформ, адаптация к происходящим изменениям;
- разумное сочетание инновационного развития и консерватизма;
- целенаправленное управляющее воздействие со стороны органов власти, поэтапные действия по внесению изменений в управленческие процессы;
- внедрение правовых инноваций в систему государственного и муниципального управления.

Список литературы

1. Готовцев Д. Контрактная система: первые итоги, ближайшие перспективы // Контрактные отношения. 2018. № 1. С. 2.
2. Орлинская О. Г., Бунгуев А. У. Разработка автоматизированной информационной системы проверки заявки участника электронного аукциона // Вестник Северо-Кавказского федерального университета. 2018. № 2 (47). С. 4.
3. Корытцев М. А., Белокрылов К. А. Проблемы трансплантации и модификации экономических институтов в сфере государственных закупок современной России // Journal of Economic Regulation. 2014. Т. 5, № 2. С. 4.
4. Постановление Правительства Российской Федерации от 28.11.2013 № 1088 «Об утверждении Правил проведения совместных конкурсов и аукционов». URL: <http://www.consultant.ru/> (дата обращения: 25.03.2022).
5. Постановление Правительства Российской Федерации от 28.11.2013 № 1090 «Об утверждении методики сокращения количества товаров, объемов работ или услуг при уменьшении цены контракта». URL: <http://www.consultant.ru/> (дата обращения: 25.03.2022).
6. Постановление Правительства Российской Федерации от 28.11.2013 № 1093 «О порядке подготовки и размещения в единой информационной системе в сфере закупок отчета об исполнении государственного (муниципального) контракта и (или) о результатах отдельного этапа его исполнения» (вместе с «Положением о подготовке и размещении в единой информационной системе в сфере закупок отчета об исполнении государственного (муниципального) контракта и (или) о результатах отдельного этапа его исполнения») (утратил силу). URL: <http://www.consultant.ru/> (дата обращения: 25.03.2022).
7. Распоряжение Правительства Российской Федерации от 24.09.2012 № 1762-р «Об одобрении Концепции развития национальной системы стандартизации Российской Федерации на период до 2020 года». URL: <http://www.consultant.ru/> (дата обращения: 25.03.2022).

А. К. Баяндурян,

студент,

Высшая школа права,

Балтийский федеральный университет имени И. Канта

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ ПОЛУЧЕНИИ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ ИЗ IoT-УСТРОЙСТВ

Аннотация. Статья посвящена изучению IoT-устройств как потенциальных носителей криминалистически важной информации. Затрагивается понятие цифровой криминалистики. Описан алгоритм работы IoT-устройств, приведены их примеры. Указано, что в зависимости от функции устройства оно может оставлять самые разнообразные «следы». Рассматривается концепция рассмотрения IoT-устройств в качестве «цифрового свидетеля». Приведена криминалистическая методология анализа IoT-устройства, которая включает в себя несколько этапов и уровней.

Ключевые слова: интернет вещей, IoT-устройства, свидетель, следы, аппаратная архитектура, цифровая криминалистика, криминалистическая характеристика

THE USE OF SPECIAL KNOWLEDGE IN OBTAINING EVIDENTIARY INFORMATION FROM IOT DEVICES

Abstract. The article is devoted to the study of IoT devices as potential carriers of criminally important information. The concept of “digital forensics” is touched upon. The algorithm of operation of IoT devices is described, their examples are given. It is indicated that depending on the function of the device, it can leave a variety of “traces”. The concept of considering IoT devices as a “digital witness” is considered. A forensic methodology for analyzing an IoT device is presented, which includes several stages and levels.

Keywords: Internet of things, IoT devices, Witness, Traces, Hardware architecture, Digital forensics, Forensic characteristics

С развитием технологического процесса в мире возникают все более новые способы сбора криминалистически важной информации. Так, сегодня почти каждый человек неразрывно связан с цифровыми технологиями, и это не остается бесследно. Появляется новая категория криминалистически важной информации – цифровые следы, именуемые также интернет-следами. Цифровой след есть у каждого, он включает в себя все следы онлайн-активности, это и покупки в Интернете, и переход по ссылкам, и регистрация на сайтах, и использование интернета вещей.

Появилось и новое направление, именуемое цифровой криминалистикой. Единого понятия цифровой криминалистики не существует, некоторые авторы отождествляют данное понятие с понятиями компьютерной криминалистики, электронной криминалистики и использованием ЭВМ. Данный вопрос носит спорный характер. Кажется, понятие компьютерной криминалистики носит более узкий характер по отношению к понятию цифровой, так как носителями цифровой информации, которые в дальнейшем могут сыграть характер доказательств является

не только компьютер, но и любая другая технология, которая хранит цифровые данные, однако данные понятия остаются взаимосвязанными.

Так, Д. Ю. Русанова определяет цифровую криминалистику как отрасль криминалистики, изучающую обнаружение, фиксацию и дальнейшее использование в раскрытии и расследовании преступлений цифровых следов, образовавшихся в ходе преступных процессов, протекающих в «виртуальном мире» [1. С. 142].

В зависимости от того в какой сфере был обнаружен цифровой след, можно выделить виды цифровой криминалистики. Выделяют сетевую криминалистику, криминалистику баз данных, памяти, облачную криминалистику, криминалистику дисков, электронной почты и вредоносных программ.

В настоящее время отдельным направлением в науке является изучение интернета вещей (Internet of Things, IoT). Понятие интернета вещей носит научный характер и определяется как способность различных вычислительных устройств, подключенных к сети интернет, выполнять свои функции непосредственно с помощью различных датчиков и интернет технологий, без прямого участия человека. В работе IoT-технологий присутствует большой поток конфиденциальной информации, большинство может храниться как в облачном пространстве, так и в протоколах, операционной системе. Самый известный пример реализации интернета вещей – это программа умного дома, где бытовые предметы могут исполнять свои функции с помощью сопутствующего устройства, роль которого, как правило, играет мобильный телефон, который передает соответствующие сигналы. Например, в случае пролива воды из крана, которая попадает на соответствующий датчик (устройство), он подает сигнал в телефон, на который приходит уведомление о возможной протечке воды и блокирует систему водоснабжения с целью обезопасить дальнейшие возможные негативные последствия. Еще одним примером является использование смарт-часов. Так, во время пробуждения часы получают определенные сигналы, в частности это изменение положения тела, изменение пульса и передают сигнал сопутствующему устройству, которое сигнализирует кофе-машине, которая уже готовит кофе для утреннего пробуждения.

Следы от устройств IoT самые разнообразные, это и пройденное расстояние, и сожженные калории. IoT-технологии встречаются и в транспортных средствах, это и передача музыки с телефона на аудиосистему машины и GPS-навигация. Отдельные транспортные средства, именуемые беспилотными, в целом является результатом развития IoT-технологий. Исследователи из Университета Лозанны в Швейцарии отмечают, что IoT-устройства оставляют в качестве следов журналы активности системы с подробной информацией о событиях, зафиксированных датчиками устройства, а также о командах, отправленных пользователем [5. С. 23]. Благодаря данным следам следователь может сделать вывод, в какое время была открыта дверь или когда была отключена сигнализация. Детекторы дыма и угарного газа могут свидетельствовать о времени и месте возникновения пожара. Приложения на смартфонах также содержат важные следы, сюда включают кэшированные миниатюры изображений, фрагменты потоков с камер. Самое важное что IoT-устройства могут записывать фотографии и видео, по которым возможно будет описать конкретного человека.

IoT-устройство можно рассматривать даже как цифрового свидетеля, отмечают исследователи Университета Малаги, Испания [4. С. 3]. Для того чтобы устройство можно было обозначить понятием «цифровой свидетель» оно должно обладать рядом признаков. Первый – это защита от несанкционированного доступа, второй – связывание учетных данных т. е. устройство должно быть привязано к личности владельца, третий – обязательное делегирование, устройство должно уметь передавать цифровое доказательство, иначе оно становится цифровым хранителем, а не свидетелем, четвертый признак четко определенные процедуры.

Однако, как извлекать эти данные в целях расследования преступлений? Предполагается, что следователи должны использовать широко распространенные методы сбора, которые стали уже шаблонными, однако с постепенным развитием технологий нужно придумывать новые методы. Исследователи из Университета Альбасете считают, что для анализа IoT-технологий необходимо адаптировать существующие криминалистические методологии [3. С. 1]. Указанная ими методология включает в себя несколько этапов. Первый – предварительная обработка. Его можно назвать также подготовительным этапом, здесь следователю необходимо заранее подготовиться и разработать план действий, заранее определить какое оборудование необходимо доставить на место происшествия. Далее следует «удостоверение личности», под которым понимается процедура отбора устройств по критерию важности и изменчивости, т. е. если какая-то информация может храниться определенное количество времени и срок ее хранения иссякает, то необходимо по критерию изменения в первую очередь изучить именно это устройство. Следующий этап – приобретение и хранение, здесь может изучаться все, начиная от памяти, заканчивая сетевым трафиком. Далее – анализ (обнаружение доказательств) и оценка (сортировка доказательств).

Однако IoT-технологии настолько разнообразны в плане их программной и аппаратной архитектуры, что невозможно разработать что-то объединяющее их всех, чтобы в случае утечки данных или кибератаки своевременно совершить необходимые действия в частности проведение экспертизы. Так исследователи из Университета Алабамы в Хантсвилле более подробно изучили данный вопрос. В своей работе они вывели многоуровневую модель, по которой возможно изучать устройства IoT [2. С. 3].

Первый уровень – это уровень физического интерфейса, который представляет собой совокупность аппаратных датчиков и приводов. Датчики могут собирать информацию и преобразовывать ее в данные, а приводы выполняют роль механического воздействия и могут взаимодействовать с окружающей обстановкой. Примером устройства IoT использующего датчики, может быть станция «Алиса», а примером привода может быть любой роботизированный манипулятор, тот же известный всем робот-пылесос. Если преступления не связаны с киберпреступностью, то с большей вероятностью можно остановиться на изучении артефактов, созданных на данном уровне. Второй уровень – это уровень устройства. Уровень устройства – это его программное обеспечение и операционная система. Далее необходимо проанализировать сетевой/транспортный уровень, который выражается в проводных и беспроводных протоколах, которые поддерживают сеть IoT (Интернет,

Wi-Fi, Bluetooth и т. д.). Уровень представления, или слой презентация, представляет собой изучение пользовательского интерфейса без распознавания. Последний уровень – уровень интеграции. Здесь необходимо изучить облачные технологии и базы данных, т. е. все, что связано с долгосрочным хранением информации. Особенно полезным изучение данного уровня будет в том случае, если устройство имеет маленькую локальную память, вследствие чего передает информацию в облачное хранилище или на сопутствующее устройство.

Это наиболее общий способ изучения IoT-устройств, позволяющий получить криминалистическую характеристику, поскольку учитывает в себе все элементы, которыми оно должно обладать, начиная от физического устройства, описания датчиков, заканчивая наиболее сложными внутренними связями от интернет-протоколов, дистанционных функций, заканчивая облачным хранилищем. В зависимости от сложившейся ситуации, возможно изучение не всех пяти уровней, а только каких-то конкретных, тех в которых содержится необходимая информация.

Список литературы

1. Русанова Д. Ю. Цифровая криминалистика: возможности и перспективы развития // Международный журнал гуманитарных и естественных наук. 2019. № 12–4 (39). С. 142–145.
2. Boozer Abel Alex, John Arun, Mukherjee Tathagata. Internet of Things Software and Hardware Architectures and Their Impacts on Forensic Investigations: Current Approaches and Challenges // Journal of Digital Forensics, Security and Law. 2021. Vol. 16. Article 4.
3. Gómez J. M., Mondéjar J. C., Gómez J. R., Martínez J. M. Developing an IoT forensic methodology. A concept proposal // Forensic Science International: Digital Investigation. 2021. Vol. 36. Article 301114.
4. Nieto A., Rios R., Lopez J. IoT-forensics meets privacy: towards cooperative digital investigations // Sensors. 2018. № 18. P. 492.
5. Servida, Casey E. IoT forensic challenges and opportunities for digital traces // Digital Investigation. 2019. Vol. 28. Pp. S 22–S 29.

Н. С. Белов,

студент,

Московский институт электронной техники

ПРАВОВЫЕ И ТЕХНИЧЕСКИЕ АСПЕКТЫ ВНЕДРЕНИЯ СТЕЙБЛКОИНОВ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В современном обществе цифровые активы стали важным элементом повседневной жизни многих людей. Теме стейблкоинов (стабильных монет) в отличие от криптовалют до недавнего времени не уделялось большого внимания. Государству необходимо предусмотреть не только надлежащее правовое регулирование высокотехнологичных финансовых продуктов, но и инфраструктуру для этих процессов. В данной статье рассмотрены некоторые правовые и технические аспекты внедрения стейблкоинов в Российской Федерации. Представлен

сравнительный анализ цифрового рубля и «крипторубля», а также предлагается легальное определение понятия «стейблкоин».

Ключевые слова: высокотехнологичное право, цифровые технологии, стейблкоин, криптовалюта, цифровой рубль, крипторубль, информационные технологии

LEGAL AND TECHNICAL ASPECTS OF THE INTRODUCTION OF STABLECOINS IN THE RUSSIAN FEDERATION

Abstract. In modern society, digital assets have become an important element in the daily lives of many people. The topic of stablecoins (stable coins), unlike cryptocurrencies, has not received much attention until recently. The State needs to provide not only adequate legal regulation of high-tech financial products, but also infrastructure for these processes. This article discusses some legal and technical aspects of the introduction of stablecoins in the Russian Federation. The comparative analysis of the digital ruble and «crypto ruble» is presented, as well as the legal definition of the concepts of «stablecoin» is offered.

Keywords: High-tech law, Digital technologies, Stablecoin, Cryptocurrency, Digital ruble, Crypto ruble, Information technology

В современном обществе активно развивается интерес к цифровым активам, что влечет за собой необходимость правового регулирования данных процессов со стороны государства. За последние три года популярность у населения криптовалют и иных высокотехнологичных продуктов в России возросло почти в четыре раза. По некоторым оценкам по состоянию на 1 сентября 2022 г. примерно 20 % граждан нашей страны являются обладателями цифровых финансовых активов.

Следует отметить, что экономика Российской Федерации в 2022 г. понесла крупные негативные последствия, такие как заморозка активов Банка России, отключение от международной системы передачи финансовых сообщений между банками (SWIFT) а также целого ряда иных санкций, направленных на экономическую дестабилизацию нашей страны.

В этой ситуации решение хотя бы одной из проблем может значительно способствовать в восстановлении экономики страны. Министерство финансов России полагает, что одной из главных задач на данный момент являются преодоление ограничений на трансграничные переводы. В этой связи предложено возможное решение – разработка стейблкоина, который будет приниматься на торговых площадках дружественных стран.

Аналогичную позицию с Министерством финансов занимают специалисты института исследований и экспертизы Внешэкономбанка Российской Федерации. Аналитики в своем докладе высказались, что для обхода санкций может помочь выпуск стейблкоина с обеспечением в золоте. Они утверждают, что «заблокировать операции с криптозолотым рублем не будет никакой возможности, так как курс цифровой валюты привяжется к курсу золота на мировом рынке» [3. С. 31].

История стейблкоинов как нового явления мира криптоактивов начинается с 2015 года, когда появился первый стейблкоин – Tether (USDT), хотя первое упоминание о стейблкоине возникло еще в 2012 г. с появлением проекта Mastercoin. USDT

первоначально был привязан к доллару США по курсу 1: 1. В процессе развития курс Tether не всегда оставался стабильным, тем не менее колебания в большую или меньшую сторону не были существенными.

Нет единого мнения о том, чем сейчас является стейблкоин. В зарубежной литературе им признается криптовалюта, стоимость которой привязана к какой-либо материальной основе – чаще всего выступающей в роли доллара США [9. С. 1]. По мнению, например, японских ученых Макико Мита (Makiko Mita), Кензуке Ито (Kensuke Ito), Шохей Осава (Shohei Ohsawa), Хидеюки Танака (Hideyuki Tanaka), стейблкоины – это криптовалюты с механизмами стабилизации цен, которые соответствуют цене другой валюты с более низкой волатильностью [8]. Однако подобные определения не имеют под собой правовых оснований в России, по причине отсутствия в национальном законодательстве понятия «криптовалюта».

Именно поэтому предлагаем определение стейблкоина основанное на Федеральном законе «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (№ 259-ФЗ) [7], которое позиционирует его как цифровую валюту, использующую в качестве собственного обеспечения денежную единицу какой-либо страны, ценные бумаги или полезные ископаемые. При этом возникает вопрос о необходимости создания «крипторубля» – стейблкоина обеспеченного валютой, золотом, нефтью или ценными бумагами, в ситуации, когда в России уже происходит разработка цифрового рубля.

Цифровой рубль – это цифровая форма российской национальной валюты, которую Банк России планирует выпускать в дополнение к существующим формам денег [1]. Ожидается, что по своей природе цифровой рубль будет достаточно близок по концепции с «крипторублем»: обе денежные единицы будут существовать исключительно в цифровом виде, могут быть использованы для упрощения трансграничных платежей, а также допускается возможность их привязки к национальной валюте. Однако если провести технический и юридический анализ данных денежных единиц, то мы увидим важные обстоятельства.

Цифровой рубль способен претендовать на форму электронных средств платежа, предусмотренных в Федеральном законе от 27 июня 2006 г. № 161-ФЗ «О национальной платежной системе» [6]. Кроме того, Центральный банк России рассчитывает разработать проект законодательства для внедрения цифрового рубля до конца 2022 г., в то время как для «крипторубля» отсутствуют даже предложения по нормативно-правовой инфраструктуре.

Помимо аспектов, связанных с нормативным регулированием, возникает вопрос технических особенностей в части выпуска «крипторубля». Поскольку стейблкоин относится к цифровой валюте (криптовалюте), то и концепция его выпуска и поддержания должна быть неизменной, что означает необходимость использования распределенного реестра. Из этого формируется основная проблема – необходимость равномерного распределения количества узлов связи между всеми странами-участницами цифровой платформы, иначе концепция распределенного реестра, исключая монополию, будет нарушена. Цифровой рубль в свою очередь будет выпускаться исключительно Банком России, что означает монополию на ее выпуск.

Несмотря на то, что обе денежные единицы смогут претендовать на использование для трансграничных переводов, цифровой рубль направлен в основном на внутренний рынок страны, если исходить из ее основных концепций. «Крипторубль» целенаправленно разрабатывается в качестве альтернативного способа для расчетов с иностранными контрагентами.

Помимо данных аспектов немаловажным является и вопрос формирования международных торговых площадок среди дружественных стран для внедрения «крипторубля». Основная проблема состоит в том, каким образом данные площадки будут законодательно урегулированы, на сколько закрытая информация о транзакциях будет внутри нее, и не появится ли новый способ для оттока финансов с открытием такой биржи. Кроме того, необходимо предусмотреть, кто будет основным владельцем такой площадки, будет ли необходимость в создании нового агрегатора для его контроля или ее роль возьмут на себя крупные национальные компании-экосистемы.

Дополнительно потребуется предусмотреть необходимую нормативную инфраструктуру в уголовное и уголовно-процессуальное законодательство, а также провести масштабное обучение следователей, прокуроров, судей, адвокатов и всех лиц, принимающих участие в уголовных делах. Сложилась практика, при которой хищение криптоактивов не всегда трансформируется в возбуждение уголовного дела, поиску виновного лица и восстановлению нарушенных прав потерпевшего.

Многое зависит от «технической подкованности» конкретного следователя, которому предстоит производить поиск цифровых следов хищения в данных обстоятельствах. Однако определенные позитивные изменения происходят, несмотря на отсутствие необходимых нормативно-правовых изменений. Так, в мае 2022 г. Петроградский районный суд города Санкт-Петербурга впервые признал криптовалюту имуществом по уголовному делу, указав, что цифровая валюта могла быть принята в качестве средства платежа, продана и конвертирована в рубли, которыми противоправно завладели фигуранты уголовного дела. Следует отметить, что уже сейчас происходит развитие высокотехнологичного права, которому необходимы специалисты нового поколения [2].

Кадровая проблема обеспечения необходимой правовой защиты инфраструктуры стейблкоинов в России крайне актуальна. Правоохранительным органам необходимо одновременно понимать, как юридические, так и технические аспекты функционирования новых цифровых активов. Во многих субъектах страны практически невозможно добиться возбуждения уголовного дела за хищение криптовалюты не только по причине пробелов в законодательстве, но и в связи с отсутствием у следователя знаний в сфере высоких технологий. Требуется переподготовка всех правоохранительных органов.

Анализ правовых и технических аспектов перспектив внедрения стейблкоинов в Российской Федерации позволяет сделать вывод о том, что создание своего собственного «крипторубля» имеет действительную необходимость на данный момент, однако на пути ее реализации потребуется разработать необходимый перечень нормативно-правовых актов, в которых будет предусмотрено определение стейблкоина, его правовое положение. Кроме того, техническая сторона вопроса требует создания качественной инфраструктуры без игроков с монополией на выпуск

данных цифровых активов. Для правовой защиты новых финансовых инструментов и выработки доверия к ним со стороны общества потребуется предусмотреть необходимые кадровые изменения в правоохранительных органах.

Список литературы

1. Банк России. Цифровой рубль. URL: <https://www.cbr.ru/fintech/dr/>
2. Бертовский Л. В. Понятие высокотехнологичного права // Высокотехнологичное право: генезис и перспективы: материалы II Международной межвузовской научно-практ. конференции. Москва, Красноярск, 26 февраля 2021 г. Красноярск: Красноярский государственный аграрный университет, 2021. С. 43–47.
3. Внешэкономбанк РФ. Международные платежи в санкционных условиях: состояние и перспективы. URL: http://www.inveb.ru/attachments/article/838/%D0%BF%D0%BB%D0%B0%D1%82%D0%B5%D0%B6%D0%B8_%D1%81%D0%BE%D1%81%D1%82%D0%BE%D1%8F%D0%BD%D0%B8%D0%B5%20%D0%B8~.pdf
4. Лолаева А. С., Макиев С. А., Бутаева Э. С. Правовая природа криптовалюты // Юридические исследования. 2021. № 12. С. 20–32. URL: https://nbpublish.com/library_read_article.php?id=37110. DOI: 10.25136/2409-7136.2021.12.37110
5. Рождественская Т. Э., Гузнов А. Г. Цифровые финансовые активы: проблемы и перспективы правового регулирования // Актуальные проблемы российского права. 2020. № 6 (115). С. 43–54.
6. О национальной платежной системе: Федеральный закон от 27.06.2011 № 161-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 05.01.2021).
7. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 05.01.2021).
8. Makiko M., Kensuke I., Shohei O., Hideyuki T. What is Stablecoin?: A Survey on Price Stabilization Mechanisms for Decentralized Payment Systems. URL: https://www.researchgate.net/publication/333815432_What_is_Stablecoin_A_Survey_on_Price_Stabilization_Mechanisms_for_Decentralized_Payment_Systems
9. Stablecoins: Legal Issues and Regulatory Options 2022. URL: https://crsreports.congress.gov/product/pdf/LSB/LSB_10753

Д. Д. Белозерова,

студент,

Национальный исследовательский Томский государственный университет

УЧАСТИЕ ГРАЖДАН В ЗАКОНОДАТЕЛЬНОМ ПРОЦЕССЕ ПРИ ПОМОЩИ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Аннотация. В данной статье рассматриваются цифровые способы участия граждан в жизни государства, расширение возможностей вовлечения большого количества человек в законодательный процесс как ключевой элемент демократии.

Показано, что публичные слушания и общественные обсуждения являются разновидностями институтов делиберативной, т. е. совещательной демократии. Проведен анализ нормативных правовых актов, принятых в стране, которые обеспечивают участие граждан в законодательном процессе при помощи цифровых технологий.

Ключевые слова: право, цифровые технологии, демократия, институты участия граждан, законодательный процесс, общественное мнение, делиберативная демократия

CITIZENS' PARTICIPATION IN THE LEGISLATIVE PROCESS WITH THE HELP OF DIGITAL TECHNOLOGIES

Abstract. This article discusses digital ways of citizens' participation in the life of the state, the expansion of opportunities for involving a large number of people in the legislative process as a key element of democracy. It is shown that public hearings and public discussions are varieties of institutions of deliberative, that is, deliberative democracy. The analysis of regulatory legal acts adopted in the country, which ensure the participation of citizens in the legislative process with the help of digital technologies, is carried out.

Keywords: Law, Digital technologies, Democracy, Institutions of citizen participation, Legislative process, Public opinion, Deliberative democracy

Введение. Граждане России по Конституции имеют множество различных политических прав в связи с тем, что «Россия есть демократическое» и «правовое государство», где «человек, его права и свободы являются высшей ценностью» [3]. Данная тема имеет особую актуальность, так как участие граждан в жизни государства является ключевым элементом демократии. В демократическом обществе существует острая потребность в публичном обсуждении и корректировке различных законопроектов с целью мониторинга общественного мнения. Таким образом, в последнее время создается все больше возможностей, позволяющих гражданам принимать участие в законотворческом процессе через различные общественные образования, Интернет-ресурсы и так далее. Именно для большего удобства граждан и их более активного участия в жизни государства в правовую деятельность внедряются цифровые технологии.

При помощи данных средств граждане России могут привлечь внимание властей к острым проблемам, существующим в обществе, к потребностям граждан. Государство же при помощи данных механизмов может определить характер общественных настроений, более четко и конкретно расставить приоритеты законодательной деятельности, повышая тем самым доверие населения к действующей власти и поднимая ее авторитет.

Следствием активного участия граждан в процессе обсуждения и принятия законопроектов при помощи различных технологий является интенсивное развитие права, которое происходит путем определения общих целей и социальных задач, направленных на преодоление существующей в обществе социальной несправедливости и урегулирование возможных конфликтов. С помощью цифровых механизмов, обеспечивающих общественное участие в законодательном процессе, становится

возможной реализация этих целей, так как именно с помощью них общество может путем конструктивного диалога и активного взаимодействия с властью прийти к консенсусу, выработав самый оптимальный вариант решения данных вопросов.

В данной работе следует рассмотреть некоторые пути, с помощью которых граждане имеют реальную возможность принимать участие в законотворческой деятельности государства на разных ее стадиях при помощи цифровых технологий.

Основная часть. Способом обеспечения участия граждан в управлении делами государства является интернет-ресурс «Российская общественная инициатива», который обеспечивает участие граждан путем выдвижения гражданской инициативы.

«Российская общественная инициатива» – это сайт, который был создан с целью публикации гражданами их общественных инициатив и проведения голосования по данным предложениям. Этот сайт был создан указом Президента Российской Федерации от 04.03.2013 № 183 «О рассмотрении общественных инициатив, направленных гражданами Российской Федерации с использованием интернет-ресурса “Российская общественная инициатива”». В Указе Президента содержатся правила рассмотрения общественных инициатив, порядок подачи инициативы и ее проверки.

В соответствии с этим Указом интернет-ресурс «Российская общественная инициатива» создавался с целью обеспечения развития гражданского общества, защиты прав и свобод человека и гражданина и повышения степени участия граждан в политической жизни государства [6].

Чтобы предложение гражданина было размещено на Интернет-ресурсе, оно должно пройти несколько этапов. Сначала гражданин выдвигает общественную инициативу, представляющую собой предложение гражданина России по вопросам развития страны. Эта инициатива может быть подана на разных уровнях – от регионального до федерального. В предложенной инициативе гражданин описывает проблему и пути ее решения.

Следующим шагом является «предварительная модерация», когда модераторы сайта проверяют инициативу, соответствует ли она правилам, содержащимся в Указе Президента от 04.03.2013 № 183 и в дополнение к этому Указу от 23.06.2014 № 452. Одним из правил является то, что выражать инициативу может только гражданин РФ, который обязательно лично предъявил при регистрации в федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре» основной документ, удостоверяющий его личность [6]. Данная стадия является стадией предварительного рассмотрения и не может превышать срока двух месяцев.

Далее предложенный проект публикуется на интернет-ресурсе «Российская общественная инициатива», и ему присваивается уникальный номер. На этом этапе начинается «сбор голосов в поддержку инициативы в течение не более года со дня размещения» [5].

По закону устанавливается минимальное число голосов, которое необходимо для рассмотрения на федеральном, региональном или муниципальном уровне. В зависимости от уровня инициативы соблюдаются определенные требования по необходимому количеству голосов в поддержку законопроекта: на федеральном

уровне – не менее ста тысяч; на региональном установлено два вида – для регионов с населением свыше 2 миллионов необходимо также не менее ста тысяч, для остальных – 5 % от населения региона; на муниципальном уровне – 5 % от населения муниципалитета [5].

При условии, что к установленному сроку законопроект наберет необходимое количество голосов, то он направляется на рассмотрение в экспертную рабочую группу федерального, регионального или муниципального уровня в зависимости от уровня инициативы. Экспертная группа должна вынести решение по предложению гражданина в течение не более двух месяцев со дня направления. В зависимости от решения рабочей группы законопроект может быть или отклонен или одобрен. Если он одобрен, тогда начинается его реализация, и он размещается на сайте «Российской общественной инициативы».

Рабочая группа проверяет законопроект по нескольким критериям: отсутствие нецензурных либо оскорбительных выражений, отсутствие призывов к экстремизму; соответствие Конституции РФ, принципам международного права, а также по вопросам, указанным в статье 6 пункте 5 Федерального конституционного закона от 28 июня 2004 г. № 5-ФКЗ «О референдуме». Также в предложенном проекте должно быть описание проблемы, которая может быть решена этим законопроектом, варианты ее решения и обоснованность данных вариантов.

Таким образом, предложить инициативу и проголосовать в поддержку других инициатив имеет возможность любой гражданин, достигший возраста восемнадцати лет, который имеет доступ к Интернету и зарегистрирован на сайте «Госуслуги».

Следует привести пример законопроекта, по которому было вынесено решение. Например, федеральная инициатива по отмене обязательного тестирования на коронавирус для прошедших вакцинацию. Данная инициатива должна, по мнению подавшего ее гражданина, привести к тому, что «те, кто привились абсолютно надежной отечественной вакциной, не будут тратить свое время, деньги, ресурсы медицинских организаций на то, чтобы сдавать абсолютно бессмысленные тесты на коронавирус». Это предложение было одобрено, вследствие чего Постановлением от 02.07.2021 были внесены изменения в постановление Главного государственного врача РФ от 18.03.2020 № 7 «Об обеспечении режима изоляции в целях предотвращения распространения COVID-2019» по отмене требования Роспотребнадзора сдавать тест на коронавирус по возвращении из-за границы тех, кто прошел вакцинацию «Спутником-V» [5].

Таким образом, создание нового интернет-ресурса «Российская общественная инициатива» призвано обеспечить вовлечение граждан в государственное управление с помощью информационных технологий, побудить их к активной политической деятельности и дать каждому совершеннолетнему гражданину право влиять на принятие того или иного законопроекта.

Бывший мэр Иркутского района Игорь Нарумов поддержал указанное нововведение: «Считаю, что данный проект позволит населению непосредственно участвовать в жизни своего поселка, области, страны. Это уникальный шанс и показатель доверия президента своему народу... Именно общественные инициативы должны стать решением наших насущных проблем, а не пустая критика, как было

ранее» [4]. Но в то же время он обратил внимание на одну из проблем, связанных с этим интернет-ресурсом, указав на то, что не все жители России имеют доступ к Интернету.

Однако, несмотря на то, что созданный по Указу Президента сайт имеет ряд проблем, он является примером настоящей демократии, позволяющей гражданам непосредственно участвовать в законодательном процессе для решения насущных проблем.

Другим вариантом участия граждан в общественной жизни государства с помощью информационных технологий являются публичные слушания и общественные обсуждения законопроектов. Рассмотрим, что представляют из себя данные публичные мероприятия.

В соответствии со ст. 18 Федерального закона от 21.07.2014 № 212-ФЗ «Об основах общественного контроля в Российской Федерации» общественный контроль осуществляется в формах общественного мониторинга, общественной проверки, общественной экспертизы, а также в формах взаимодействия институтов гражданского общества с государственными органами и органами местного самоуправления, как общественные слушания и общественные обсуждения [8].

Общественное обсуждение и публичное слушание являются формами участия совершеннолетних граждан в деятельности органов местного самоуправления. Данные формы участия представляет собой публичное обсуждение проектов на муниципальном уровне, вынесенных по вопросам местного значения, с участием граждан данного муниципального образования.

Таким образом, публичные слушания и общественные обсуждения являются разновидностями институтов делиберативной, т. е. совещательной демократии.

Можно выделить принципы проведения данных публичных мероприятий: прежде всего, это открытость. Исходя из законодательства, слушания должны быть открытыми и не зависимыми от заинтересованных должностных лиц и органов власти [2]. В соответствии с данным положением каждый участник может свободно высказать свое мнение по тому или иному вопросу или внести предложения и какие-либо замечания по затрагиваемым в обсуждении и слушании вопросам.

Исходящая из самого названия мероприятий публичность подразумевает под собой доступность обсуждения для каждого, а также возможность и право каждого принимать в нем участие. Более того, публичность включает в себя гласность обсуждения рассматриваемых вопросов и открытость процесса принятия решения для публики и средств массовой информации [2]. Кроме того, граждане принимают непосредственное участие в публичных слушаниях.

Для большего удобства граждан существует две формы их участия в общественном обсуждении и публичном слушании. В Федеральном законе не установлен четко ограниченный формат обсуждений, однако существует очная и заочная формы. Очное обсуждение законопроектов и различных вопросов предполагает присутствие лиц, желающих принять живое участие в рассмотрении вопросов, в определенном месте, о котором жители муниципального образования должны быть заблаговременно оповещены. Более того, им заранее дают возможность ознакомиться с предлагаемым к обсуждению проектом. С этой целью проект, в соответствии с законодательством, размещается на сайте определенного органа самоуправления

субъектом Российской Федерации или муниципальным образованием в Интернете либо на официальном сайте [7]. При заочном участии гражданин может направить свое мнение или имеющиеся предложения и замечания организатору обсуждения посредством сети Интернет.

Процедуру проведения заочного публичного слушания можно рассмотреть на примере Закона «О порядке проведения публичных слушаний по проекту бюджета Санкт-Петербурга и годовому отчету об исполнении бюджета Санкт-Петербурга», который был принят Законодательным собранием города Санкт-Петербурга 16 мая 2007 г. В п. 1 ст. 4 говорится, что при проведении публичных слушаний в заочной форме предполагается размещение проекта бюджета города Санкт-Петербурга на официальном сайте Законодательного собрания в электронном виде вместе с возможными замечаниями и вопросами участников публичных слушаний, на которые обязательно предоставляется возможность получить ответ, который размещается в том же разделе на сайте Законодательного собрания Санкт-Петербурга [1].

Одним из самых актуальных в настоящее время способов выражения мнения граждан по вопросам общественной жизни государства является дистанционное электронное голосование.

Обращаясь к истории становления данного вида голосования, важно отметить, что Венесуэла – первая страна, где состоялись выборы при помощи машин, которые сразу же печатали заполненный бланк голосования. Машины представляли собой комплексные устройства, оснащенные сенсорным экраном и принтером, и каждый избиратель мог в электронном бюллетене отметить партию или имя. С течением времени систему модифицировали для усиления защиты, была разработана комплексная аутентификация, при которой машина активировалась только после распознавания отпечатка пальца избирателя [10].

Данный формат голосования используется в России в целях обеспечения реализации избирательных прав и прав на участие в референдуме граждан, который не требует очного посещения избирательного участка гражданином, а позволяет принять участие в голосовании дистанционно.

Наиболее подробно данную форму голосования можно рассмотреть в соответствии с Федеральным законом от 12.06.2002 № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации». Федеральный закон дополнен ст. 64.1 «Дистанционное электронное голосование» с 14 марта 2022 г. В статье идет речь о том, что допускается проведение дистанционных электронных выборов при проведении выборов и референдумов.

Данный вид голосования проводится с помощью государственной автоматизированной системы «Выборы», которая предоставляет свободную и полную информацию о выборах и предназначается для автоматизации избирательного процесса, или на иных государственных информационных системах, как федеральных, так и региональных.

Порядок проведения дистанционного электронного голосования должен полностью соответствовать требованиям к проведению данного вида голосования, которые установлены Центральной избирательной комиссией Российской Федерации.

В соответствии с данными требованиями порядок проведения должен содержать процедуру и «сроки подачи заявления об участии в дистанционном электронном голосовании и его отзыва, ... порядок аутентификации и идентификации избирателя, участника референдума для участия в дистанционном электронном голосовании, ... порядок обеспечения возможности наблюдения при организации ... и установлении его итогов с учетом особенностей такого голосования, а также порядок назначения наблюдателей» [9].

Для участия в данном виде голосования избиратель или участник референдума должен в сети Интернет или с помощью мобильного приложения обратиться на специальный портал и проходит процедуру авторизации, после чего он получит доступ к дистанционному электронному голосованию.

Также важно отметить, что в ходе вышеуказанной формы электронного голосования происходит процедура анонимизации, «по завершении которой осуществляется переход к электронному бюллетеню и предоставляется возможность осуществить волеизъявление» [9].

Заключение. Формы политического участия достаточно разнообразны, поэтому граждане имеют огромное количество возможностей для участия в политической жизни общества. За последние десятилетия в Российской Федерации появляется все больше цифровых механизмов взаимодействия между институтами гражданского общества и органами государственной власти. Данный процесс происходит потому, что государство стремится максимально вовлечь граждан в политическую жизнь и повысить существующий на данном этапе уровень политического участия граждан.

Так, для обеспечения возможности всех граждан высказывать свое мнение происходит активное развитие заочного участия граждан через различные порталы в сети Интернет.

Создание все большего количества институтов различных способов цифрового участия граждан происходит с целью обеспечить, прежде всего, максимально обширное и наиболее эффективное участие граждан в жизни государства, которое определяется тем, что в результате достигается консенсус между обществом и органами власти и выносятся наиболее оптимальное решение, максимально учитывающее мнение всего общества.

Проявление общественной инициативы и развитие каналов для ее обеспечения имеет огромную ценность для государства, так как именно через эти каналы власть может выявить мнение общества и проводить на его основе взвешенную и разумную политику. Более того, регулярный мониторинг мнения граждан может обеспечить наличие альтернативного варианта решения того или иного вопроса, позволяющее учесть интересы большинства. Это может помочь принять наиболее благоприятное решение, при этом избежав возможных конфликтов и нарушений интересов и прав граждан.

Кроме того, наличие цифровых технологий участия граждан в законодательном процессе обеспечивает осведомленность и информированность граждан по вопросам управления, по существующим в обществе проблемам и спорам и по путям, позволяющим отстаивать свою позицию, интересы и свое мнение. Грамотность в политической жизни обеспечит более «просвещенное» и «взвешенное» участие

граждан в обсуждении вопросов, повышению правовой культуры, что непосредственно приведет к более осмысленным и рациональным решениям и позволит государству чаще обращаться к данным способам принятия решения.

Участие граждан в разработке и принятии законов влияет на повышение эффективности решения возникающих в обществе проблем, так как народ выражает через вышеперечисленные механизмы свою волю и свое мнение, и к большему пониманию властями потребностей общества через его структуризацию. В свою очередь, это приводит и к развитию права, в котором теперь постепенно появляется ярко выраженная социальная направленность. Развитие права, все более ориентированного на удовлетворение потребностей всего общества и отдельно взятого человека, также создает нормативно-правовую базу для совершенствования и эволюции демократического строя в России.

Так, эволюция государства и права в данном направлении обеспечивает максимальный учет и согласование интересов как государства, так и общества, и отдельно взятой личности, что обеспечивает стабильность в гражданском обществе.

Список литературы

1. Администрация Санкт-Петербурга. Колпинский район. URL: https://www.gov.spb.ru/gov/terr/reg_kolpino/publichnye-slushaniya/zakon-sankt-peterburga-o-poryadke-provedeniya-publichnyh-slushaniy-po-/ (дата обращения: 21.08.2022).
2. Киселев, К. В. Публичные слушания в муниципальных образованиях / Киселев К. В., Ляпустина М. В., Руденко В. Н. Екатеринбург: УрО РАН, 2007. 152 с. ISBN 5-7691-1893-8
3. Конституция РФ: Принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года // Собрание законодательства РФ. 2020. № 9. Ст. 2.
4. Проект «Российская общественная инициатива». Иркутское районное муниципальное образование. URL: <https://www.irkraion.ru/airmo/165-obshchestvo/proekt-rossijskaya-obshchestvennaya-initsiativa> (дата обращения: 18.08.2022).
5. Российская общественная инициатива. URL: <https://www.roi.ru/page/how-it-works/> (дата обращения: 11.08.2022).
6. Указ Президента Российской Федерации «О рассмотрении общественных инициатив, направленных гражданами Российской Федерации с использованием интернет-ресурса “Российская общественная инициатива”» от 04.03.2013 № 183 // СПС «Гарант».
7. Федеральный закон «Об общих принципах организации местного самоуправления в Российской Федерации» от 06.10.2003 № 131-ФЗ // СПС «Гарант».
8. Федеральный закон «Об основах общественного контроля в Российской Федерации» от 21.07.2014 № 212-ФЗ // СПС «Гарант».
9. Федеральный закон «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» от 12.06.2002 № 67-ФЗ // СПС «Гарант».
10. Descripción del Sistema de Elección Venezolano. URL: http://www.cne.gov.ve/web/sistema_electoral/tecnologia_electoral_descripcion.php

А. А. Блохина,

студент,

Финансовый университет при Правительстве Российской Федерации

ПРИМЕНЕНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ФАРМАЦЕВТИЧЕСКОМ БИЗНЕСЕ: ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРОДАЖИ РЕЦЕПТУРНЫХ ПРЕПАРАТОВ ЧЕРЕЗ ПЛОЩАДКИ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Аннотация. В статье рассматривается вопрос стремительного развития фармацевтического бизнеса на территории Российской Федерации, а также вопрос легализации продажи рецептурных лекарственных средств через площадки электронной коммерции. В работе представлены графики, анализ которых позволяет определить особенности потребительского рынка при использовании сервисов дистанционного заказа необходимых препаратов. Обосновывается необходимость внесения поправок в существующую отечественную нормативно-правовую базу: снятие законодательного запрета на продажу рецептурных препаратов. Представлены статистические данные, свидетельствующие о необходимости введения данной меры в действие, а также приведен зарубежный опыт использования данного сервиса и его влияние на экономическую сферу. Проанализированы возможные проблемы в случае легализации продажи лекарственных средств, отпускаемых по рецепту врачей, и представлены пути их решения.

Ключевые слова: площадка электронной коммерции, лекарственные средства, фармацевтический рынок, онлайн-аптека, электронный рецепт

APPLICATION OF DIGITAL TECHNOLOGIES IN THE PHARMACEUTICAL BUSINESS: LEGAL REGULATION OF THE SALE PRESCRIPTION DRUGS THROUGH E-COMMTRCE PLATFORM

Abstract. The article deals with the rapid development of pharmaceutical business in the Russian Federation, as well as the issue of legalizing the sale of prescription drugs through e-commerce platforms. The paper presents graphs, the analysis of which allows us to determine the features of the consumer market when using remote ordering services for necessary drugs. The article substantiates the need to amend the existing domestic regulatory framework: lifting of the legislative ban on the sale of prescription drugs. Statistical data indicating the need to put this measure into effect are presented, as well as foreign experience in using this service and its impact on the economic sphere. The possible problems in the case of legalizing the sale of prescription medicines are analyzed and ways to solve them are presented.

Keywords: E-commerce platform, Medicines, Pharmaceutical market, Online pharmacy, Electronic prescription

Принятый национальный проект «Здравоохранение» положил начало модернизации оказания медицинской помощи всем нуждающимся. Но события 2020 г. существенным образом изменили вектор развития национального проекта, поскольку требовалось принятие серьезных решений, от которых зависела жизнь миллионов россиян, в кратчайшие сроки. Медицина столкнулась с ранее неизвестной эпидемией COVID-19, которая за считанные дни унесла жизни тысячи людей. Несмотря

на отрицательный опыт, с которым столкнулись многие государства, тем не менее данная критическая ситуация послужила отправной точкой для развития информационных технологий во многих сферах жизни общества.

Пандемия существенным образом поменяла привычный уклад жизни на новые правила, в том числе в области продажи лекарств. Были внесены изменения в законодательные акты в сфере здравоохранения, закрепившие право аптечных организаций осуществлять розничную торговлю лекарственными препаратами для медицинского применения, используя дистанционные технологии. Законодатель установил четкие требования, соблюдение которых дает право аптечной организации осуществлять торговлю лекарственными препаратами на площадке электронной коммерции. Так, сети онлайн-аптек реализуют только безрецептурные лекарства, не допускается продажа тех лекарственных препаратов, в состав которых входит объем этилового спирта, превышающий 25 %. Наркотические и психотропные вещества, отпускаемые по рецепту врача, реализуются исключительно в аптечных учреждениях. Установленные действующим законодательством требования, касающиеся продажи исключительно безрецептурных лекарств, оправданы, поскольку могут возникнуть негативные последствия для здоровья гражданина, который, например, осуществлял бесконтрольный прием антибиотиков, что может привести к различным последствиям вплоть до летального исхода. Федеральный закон от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств», а также Постановление Правительства Российской Федерации от 16 мая 2020 г. № 697 «Об утверждении правил выдачи разрешения на осуществление розничной торговли лекарственными препаратами для медицинского применения дистанционным способом...» регламентируют порядок осуществления онлайн-торговли лекарственными средствами, в том числе вопрос об установленных законодательных требованиях к данным организациям, претендующим на право получения разрешения на осуществление такого вида деятельности.

Важно обратить внимание на следующий факт: введенная законодателем указанная мера получила отклик со стороны граждан, для которых покупка всех необходимых лекарств посредством электронной коммерции не только сокращает время на дорогу и поиск нужной аптеки, но и предотвращает возможность заразиться от других людей, избегая контакта. Для более детального анализа необходимо обратиться к статистическим данным за 2020 г. (рис. 1).

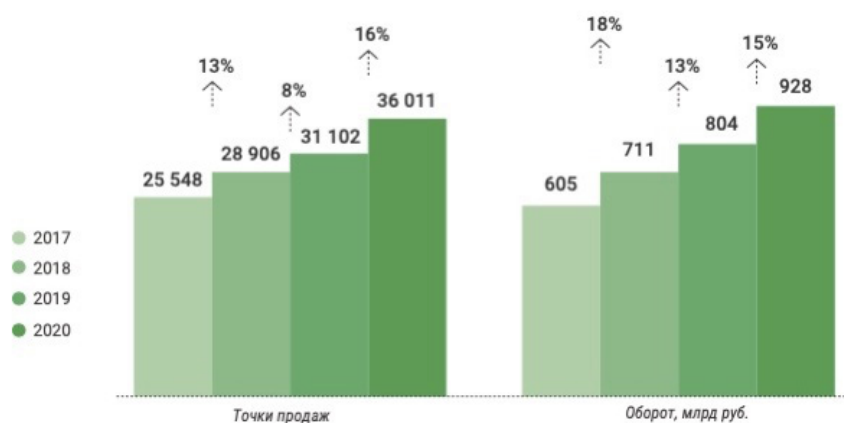


Рис. 1. Динамика роста оборота и количества точек топ-20 аптечных сетей [3]

Приведенный график свидетельствует о том, что в 2020 г. доля продажи лекарственных препаратов через площадки электронной коммерции существенным образом возросла в сравнении с показателями 2019 г. И действительно, использование современных информационных технологий в медицинской отрасли повышает качество оказания услуг клинического характера, а также повышается доступность медицинской помощи. Так, используя сервис дистанционного заказа лекарственных препаратов, позволяет потенциальному потребителю сравнить цены в различных онлайн-магазинах, ознакомиться с аналогами препаратов и принять рациональное решение. Указанное подтверждается рис. 2, в котором отражается рейтинг сервисов онлайн-заказов по обороту в 2020 г., а также прирост оборота по сравнению с 2019 г.

Рейтинг	Сервис дистанционного заказа	Количество точек продаж	Объем, млрд руб.	Прирост оборота по сравнению с 2019	Доля на коммерческом сегменте, 2020
1	Аптека.ру	15 867	50,1	46%	3,6%
2	Сбер Еаптека	731 (116*)	11,0	96%	0,8%
3	Здравсити	15 828	6,3	134%	0,4%

Таблица 25
Рейтинг сервисов дистанционного заказа по обороту в 2020 году
* количество собственных точек

Рис. 2. Рейтинг сервисов дистанционного заказа по обороту в 2020 г. [3]

Подводя итог, стоит сказать следующее: реализация товаров через площадки электронной коммерции оказала позитивное влияние на развитие экономики Российской Федерации. Так, представленные статистические данные за 2020 г. свидетельствуют о популяризации использования сервисов дистанционного заказа лекарственных препаратов, что в свою очередь повышает динамику продаж. Согласно данным фармацевтического рынка Российской Федерации DSM Group за 2020 г. объем ecom-сегмента составил около 93,2 млрд руб. [3]. Таким образом, E-commerce – удобный, надежный, быстрый и комфортный сервис для покупки лекарственных средств. Потребитель может спокойно ознакомиться с составом соответствующего препарата, увидеть его наличие или отсутствие на торговой площадке. К тому же у сервиса «Еаптека» есть звонок фармацевту для получения необходимой консультации. Данная функция крайне удобна для потребителя, поскольку позволяет узнать дополнительную информацию о выбранном товаре, например, о наличии или отсутствии подобных эффектов, а также совместимость с другими препаратами. Электронная коммерция в фарминдустрии очень перспективна.

Несмотря на позитивный момент, связанный с использованием сервисов дистанционной продажи лекарственных средств, тем не менее существуют проблемы, с которыми столкнулся фармацевтический бизнес. Первоочередная проблема связана с запретом на реализацию лекарственных средств, отпускаемых по рецепту врачей. В случае заболевания гражданин обращается к нужному специалисту, который в свою очередь в ходе осмотра назначает соответствующий план лечения и выписывает рецепт на приобретение лекарства в аптечной организации. В связи с внесенными

изменениями с законодательство в сфере осуществления медицинской деятельности предоставляется возможности выписывать рецепты как в электронной, так и в традиционной бумажной версии [7]. В случае выписки рецепта в электронной форме пациент получает всю необходимую информацию на смартфон. В аптечной организации гражданин показывает QR-код фармацевту, последний же в свою очередь выдает лекарственные средства. Приобрести же дистанционным способом лекарственные препараты рецептурного назначения невозможно, что создает потенциальную опасность для здоровья гражданина, поскольку он будет вынужден направиться в аптечную организацию. В связи с этим возникает необходимость законодательной реформы, предоставляющей возможность реализовывать данные лекарства с использованием сервисов дистанционных технологий.

Стоит обратиться к зарубежному опыту использования электронной коммерции для продажи рецептурных лекарственных препаратов. Так, 17 ноября 2020 г. американский онлайн-ритейлер Amazon объявил о создании онлайн-аптеки Amazon Pharmacy, в которой будет возможность приобрести лекарственные препараты, отпускаемые по рецепту врачей [1].

Введение в действие сервиса дистанционной продажи лекарственных средств рецептурного назначения на площадке онлайн-аптеки Amazon Pharmacy оказала позитивное влияние на увеличение выручки до \$ 386,1 млрд за 2020 г. За 2021 г. выручка данной компании увеличилась на 22 % и достигла \$ 469,8 млрд [2]. Статистические данные свидетельствуют о том, что сервис онлайн-продажи товаров занимает ведущее положение по сравнению с офлайн-магазинами. Продажа лекарственных средств, в том числе тех, которые отпускаются по рецепту врачей, имеет большие перспективы, поскольку позволяет сократить время на поиск ближайшей аптеки, сравнение цен в каждом учреждении. К тому же использование дистанционных технологий для торговли лекарственными препаратами обеспечивает охрану здоровья потребителей, потому что он не контактирует с другими людьми, тем самым сохраняет не только свое здоровье, но и создает безопасные условия для других субъектов.

В отношении же Российской Федерации следует сказать следующее: введение дистанционной продажи лекарственных средств получило отклик со стороны общества. Существует сдерживающий фактор – законодательный запрет на реализацию лекарственных средств рецептурного назначения через онлайн-аптеки. В связи с этим в обществе возникла потребность в ведении в действие продажи рецептурных лекарств. Так, первый заместитель председателя Комитета Государственной Думы по охране здоровья, член фракции «Единая Россия» Л. А. Огуль считает, что потребители заинтересованы в снятии законодательного запрета на продаже рецептурных препаратов через сервисы дистанционного заказа, поскольку это позволит обеспечить доступность необходимых средств для нуждающихся [4].

В связи с этим Минэкономразвития выступило с инициативой о снятии законодательного запрета на продажу рецептурных лекарств онлайн. Указанное нововведение увеличит доступность лекарственных препаратов для всех категорий нуждающихся. К тому же легализация рецептурных препаратов позволит распространить на территории Российской Федерации систему электронный рецептов, которые невозможно будет подделать, поскольку защищены специальный QR-кодом.

Данная мера позволит сократить количество преступлений, квалифицируемых по ст. 233 УК РФ.

Несмотря на позитивное влияние утверждения дистанционной продажи лекарственных препаратов рецептурного назначения на фармацевтический бизнес Российской Федерации, тем не менее существуют сдерживающие факторы, в связи с чем Министерство экономического развития Российской Федерации предложило провести эксперимент, по итогам которого будет ясно каким образом стоит осуществлять эту деятельность. Так, Федеральная служба по надзору в сфере здравоохранения представила проект приказа, в котором утверждается перечень документов, необходимых аптекам для дистанционной продажи лекарств [6]. В перечень необходимых документов вошли следующие: документы, подтверждающие наличие принадлежащих аптеки помещений для хранения заказов для пациентов, документы, подтверждающие наличие у аптеки специального оборудования (камеры хранения, поддерживающие оптимальную температуру, вентиляционная система и иное оборудование), наличие лицензии у аптеки на осуществление розничной торговли рецептурными препаратами дистанционным способом и т. д. Помимо вышеназванных требований, аптека должна иметь собственный интернет-сайт, мобильное приложение, а также курьерскую службу. В ходе экспериментально-правового режима также не допускается дистанционная реализация препаратов, содержащих наркотические, психотропные и сильнодействующие вещества.

В случае введения в действие продажи рецептурных лекарств через сервисы дистанционного заказа фармацевтический бизнес может столкнуться со следующими проблемами:

1. Каким образом осуществить консультацию с фармацевтом при оформлении заказа онлайн?

2. Как быть уверенным в том, что онлайн-аптека не является мошенником?

Вероятнее всего, первое, с чем могут столкнуться потребители при введении данной меры, – это недоверие к онлайн-аптекам. Многие люди при наличии рецепта приходят в аптечное учреждение, с тем чтобы не только приобрести нужный товар, но и получить консультацию фармацевта. Пациент может спросить про аналоги определенного препарата, совместимость данного средства с другими, если у него имеется индивидуальная непереносимость соответствующего вещества, и т. д. Именно совет специалиста крайне важен для потребителей, поскольку позволяет им выбрать хорошее средство без вреда для здоровья. Но каким образом осуществить консультацию в дистанционном формате? На сайте онлайн-аптеки следует расположить информацию о телефоне специалиста, с которым можно связаться, позвонив ему лично либо задав соответствующий вопрос в чат.

Вторая проблема, с которой может столкнуться фармацевтический бизнес при снятии законодательного запрета на реализацию лекарств рецептурного назначения, – это мошенничество, которое выражается в подделке сайтов онлайн-аптек и продаже фальсифицированных лекарственных средств потребителям. Мошеннические действия создают потенциальную угрозу для здоровья пациентов, а также наносят ущерб репутации интернет-аптекам, поскольку возникнет недоверие со стороны субъектов к достижениям в области медицины. Так, руководитель службы иссле-

дований, кибераналитики и развития Группы компаний Т1 Александр Новиков отметил негативную тенденцию роста числа мошеннических сайтов, реализующих лекарственные средства [5]. В связи с этим следует предпринять действия, направленные на сокращение числа преступлений в сфере цифровой экономики. К сожалению, на данный момент более 10 % лекарственных средств, предназначенных для розничной торговли, не имеют подлинной сертификации, поскольку их производство осуществляется на подпольных предприятиях. Так, согласно представленным данным новостного портала МК. RU, 18 июня настоящего года в Красноярском крае мужчина лишился 13 000 рублей вследствие мошеннических действий со стороны фэйковой аптеки, на сайте которого он сделал заказ необходимого препарата [5]. Негативную тенденцию роста числа несертифицированных онлайн-аптек подтверждают представители Роспотребнадзора, а также фармацевтического бизнеса. Продажа лекарственных препаратов, не имеющих сертификатов о соответствии, через сервисы дистанционного заказа может не только принести вред денежным средствам потенциального потребителя, но и здоровью в случае использования данных средств.

Указанную проблему возможно решить путем предоставления потребителям открытой информации о деятельности интернет-аптеки. Так, важно размещать сертификаты о соответствии лекарственных препаратов, сертификаты, подтверждающие право на осуществление дистанционной продажи лекарственных средств, рецептурного назначения и т. д.

При грамотном ведении фармацевтического бизнеса выигрывают не только его представители, но и потребители. Ведение фармацевтического бизнеса через площадки электронной коммерции имеет преимущества, например: привлечение большего количества клиентов, заинтересованных в приобретении необходимого препарата; в случае размещения необходимых сертификатов возрастет доверие со стороны потребителей, поскольку они будут уверены в качестве и надежности представленной услуги; посредством информационных технологий возможно отследить и в дальнейшем осуществить актуализацию информации о товарах на складах; увеличение и улучшение продаж, поскольку интернет-магазин может принимать заказы в любое время суток, а ответы на часто задаваемые вопросы приходят благодаря системе технической поддержки. О преимуществах для потребителей было сказано выше.

Таким образом, революция фармацевтического бизнеса уже на пороге. Введение экспериментально-правового режима продажи рецептурных лекарств онлайн получит поддержку со стороны потребителей, поскольку приобретение необходимого лекарства станет удобно и быстро. К тому же эта мера позволит маломобильным гражданам получить препарат посредством курьерской доставки, а также получить всю важную информацию о товаре и его аналогах от профессионального фармацевта, сделав звонок на сайте аптеки. Помимо этого, эта мера приведет к распространению электронного рецепта и Единой медицинской информационно-аналитической системы (ЕМИАС), что приведет к повышению качества и доступности медицинской помощи в государственных учреждениях здравоохранения во всех регионах Российской Федерации. Использование электронного рецепта снизит количество случаев подделки

рецептов и незаконного приобретения лекарственных средств. Доходы фармацевтического рынка России увеличатся ввиду имеющегося большого спроса.

Список литературы

1. Amazon запустила интернет-аптеку, торгующую рецептурными препаратами. URL: <https://www.kommersant.ru/doc/4575477> (дата обращения: 30.08.2022).
2. Amazon в IV квартале увеличил чистую прибыль почти в два раза. URL: <https://www.interfax.ru/business/820204> (дата обращения: 29.08.2022).
3. Данные розничного аудита фармацевтического рынка РФ DSM Group за 2020 г. URL: https://dsm.ru/docs/analytics/2020_Report_rus.pdf (дата обращения: 01.09.2022).
4. Онлайн-торговлю рецептурными лекарствами хотят запустить в форме экспериментально-правового режима. URL: <https://www.pnp.ru/economics/onlayn-torgovlyu-recepturnymi-lekarstvami-khotyat-zapustit-v-forme-eksperimentalno-pravovogo-rezhima.html>
5. Осторожно! Фальшивых онлайн-аптек становится все больше. URL: https://www.buhgalteria.ru/news_old/detail.php?ELEMENT_ID=201923
6. Росздравнадзор подготовил требования к аптекам для дистанционной торговли лекарствами. URL: <https://www.pnp.ru/social/roszdravnadzor-podgotovil-trebovaniya-k-aptekam-dlya-distancionnoy-torgovli-lekarstvami.html>
7. Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» от 29.07.2017 № 242-ФЗ. Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>, 30.07.2017 (дата обращения: 06.09.2022).

К. Э. Богославская,
магистрант,

Донецкая академия управления и государственной службы
при главе Донецкой Народной Республики

ЦИФРОВЫЕ ТЕХНОЛОГИИ В НАЛОГОВЫХ И ГРАЖДАНСКИХ ПРАВООТНОШЕНИЯХ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. На сегодняшний день соответствующие новшества активно поддерживают многогранную деятельность органов государственной власти и местного самоуправления; вооруженные силы и правоохранительные органы страны; хозяйственные субъекты разных форм собственности и организационной структуры; политические партии и движения; общественные и профессиональные объединения; творческие союзы и объединения; повседневная жизнь граждан. Поэтому в предлагаемой статье предметом исследования являются положения отдельных законодательных актов, официально устанавливающих порядок применения информационных технологий, основанный на интенсивном и масштабном использовании вычислительной техники, систем связи и телекоммуникаций. Актуальность

исследования обусловлена тем, что на рубеже двух столетий эти новшества фактически произвели революционный переворот не только в экономике, политике и культуре, но и в общественном сознании, морали и формах поведения человека. В то же время действующие законодательные положения требуют периодической корректировки и уточнения.

Ключевые слова: право, цифровые технологии, государство, право, налог, деятельность, сфера, информация

DIGITAL TECHNOLOGIES IN TAX AND CIVIL LEGAL RELATIONS

Abstract. To date, the relevant innovations actively support the multifaceted activities of state authorities and local self-government; armed forces and law enforcement agencies of the country; economic entities of different forms of ownership and organizational structure; political parties and movements; public and professional associations; creative unions and associations; everyday life of citizens. Therefore, in the proposed article, the subject of research is the provisions of individual legislative acts that officially establish the procedure for the use of information technology, based on the intensive and large-scale use of computer technology, communication and telecommunications systems. The relevance of the study is due to the fact that at the turn of two centuries these innovations actually made a revolutionary revolution not only in the economy, politics and culture, but also in public consciousness, morality and forms of human behavior. At the same time, the current legislative provisions require periodic adjustment and clarification.

Keywords: Law, Digital technologies, State, Law, Tax, Activity, Sphere, Information

Введение. Уже не вызывает сомнения тот факт, что не только эффективность принимаемых решений, но и конечные результаты функционирования всех вышеперечисленных образований, реализация интересов отдельных лиц и других пользователей системы национального и международного информационного обеспечения зависят от качественного и оперативного использования этих технологий. В то же время введение информационных технологий (далее – ИТ) в общественный оборот настоятельно и объективно требовало их надлежащего нормативно-правового оформления.

Основная часть. Отправной точкой проведенного научного исследования явилось содержание ст. 5 Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [13], в которой говорится, что названное явление может быть объектом публичных, гражданско-правовых отношений. При этом законодательный орган учитывал отдельные требования Налогового кодекса Российской Федерации, Гражданского кодекса Российской Федерации и других законов.

В заключительной части статьи сформулированы выводы, связанные с необходимостью более углубленного использования ИТ в различных социальных процессах.

В Российской Федерации правовую основу для внедрения информационных технологий в повседневную практику общественных отношений и деловых контактов самого широкого и разнообразного круга заложил Федеральный закон Российской Федерации от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» [14].

Вслед за ним вступила в силу новая редакция Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон № 149-ФЗ) [3]. Здесь следует сразу подчеркнуть, что в указанном акте, в числе прочих, формулируются два понятия, красной нитью проходящие через все содержание данного издания.

Отсюда, согласно ст. 2, информацией являются сведения (сообщения, данные) независимо от формы их представления. В свою очередь, информационные технологии определяются как процессы, способы поиска, сбора, хранения, обработки, предоставления, распространения информации, а также способы реализации соответствующих процессов и методов.

В соответствии с этим необходимо подчеркнуть, что содержится в ст. 5 названного закона, поскольку в ней подчеркивается, что информация может быть объектом публичных, гражданских и иных правоотношений. Данная формулировка является одним из существенных аспектов, лежащих в основе проводимых научных исследований.

Первый упомянутый закон сыграл известную положительную роль на начальном этапе становления информационных технологий. Однако практика его применения выявила наличие существенных недостатков. В частности, они выражались в обоснованные претензии со стороны пользователей. К ним относились, прежде всего, субъекты различных видов экономической деятельности, должностные лица органов государственной исполнительной власти и органов местного самоуправления, предприниматели и физические лица.

В конечном итоге это стало одной из причин принятия нового, дополненного и усовершенствованного Федерального закона Российской Федерации от 6 апреля 2011 г. № 63-ФЗ (в редакции от 14 июля 2022 г.) «Об электронной подписи», а предыдущий утратил юридическую силу [15].

Следует отметить, что с литературоведческой точки зрения формулировка, закрепленная в законе, представляется весьма неудачной из-за перегруженности базового термина. Под указанной подписью понимается информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Следует подчеркнуть, что кардинальное отличие электронных документов от обычных, исторически сложившихся бумажных образцов характеризуется специфическими особенностями ИТ и совершенно иными, чем прежде, способами фиксации соответствующих данных:

- а) нет жесткой, прямой связи между документом и его материальным носителем;
- б) при этом внутреннее содержание электронного документа и его внешнее оформление сохраняют и отражают установленные параметры представления информации, присущие бумажным носителям;
- в) подготовка текста электронных документов и последующая передача информации различным заинтересованным лицам, в том числе уполномоченным государственным структурам, в подавляющем большинстве случаев не требует длительной, специальной подготовки среди широких слоев пользователей.

Фактически перечисленные акты дали возможность закрепления положений об использовании ИТ в повседневной практике в нормах российского отраслевого законодательства. В настоящее время эти нововведения официально стали неотъемлемыми элементами функционирования органов государственной власти и местного самоуправления; структуры с полномочиями по надзору и контролю; приобрели статус обязательных компонентов в деятельности всех отечественных хозяйствующих субъектов независимо от их производственного, коммерческого или иного назначения; последовательно входят в повседневную жизнь граждан.

Все процессы, связанные с внедрением информационных технологий в различные сферы общественной жизни, с самого начала их зарождения находились и продолжают находиться под пристальным вниманием российских ученых и специалистов. Из огромного блока источников разных лет необходимо привести лишь несколько достаточно типичных фактов.

В частности, еще в 1988 г. вышла статья Ершова о компьютерной грамотности подрастающего поколения и информационной культуре общества [7. С. 82–92]. На протяжении последнего десятилетия прошлого века регулярно выходили публикации на актуальную тематику. Характерно, что уже тогда обсуждались перспективы подготовки действующих нормативных правовых актов. Поэтому в настоящее время практически все монографии и журнальные статьи так или иначе строятся на положениях названных выше законов.

Например, Швецов в своей работе затрагивает проблемы формирования теории и практики информационного общества в мире и в России [22]. Коллектив авторов под руководством Бабкиной уделяет особое внимание тенденциям развития экономики и промышленности в условиях цифровизации на региональном и отраслевом уровнях [2]. В свою очередь, тема Лapidуса поднимала вопросы управления электронным бизнесом и электронной коммерцией [8].

Другие исследователи анализируют более узкие темы, связанные с информационными технологиями, в зависимости от целей и задач собственных научных исследований; специализация и направления профессиональной деятельности; практические и другие многогранные интересы; идеи и общественно значимые ожидания.

В одном из разделов монографии Бурцева подробно сформулированы основные параметры информации, обрабатываемой в системе налоговых органов [5. С. 130–146]. Бобров анализирует некоторые гуманитарные аспекты информационных технологий [4. С. 268–270]. Писенко и Гаспарян затрагивают проблемы правового обеспечения антимонопольной политики на цифровых финансовых рынках [19. С. 71–78].

Санников и Харитонов рассматривают особенности цифровых активов как объектов предпринимательского оборота [20. С. 27–34]. Невская и Кондеев акцентируют внимание на средствах правового регулирования электронной торговли на евразийском пространстве и участии в ней Российской Федерации [10. С. 59–71].

Поскольку роботы становятся реальными участниками цифровой экономики, в статье Серовой рассматриваются проблемы определения их правовой природы [21. С. 22–24]. Со своей стороны Нам исследует сущность электронных форм сде-

лок по законодательству Европейского союза и Германии [9. С. 18–128]. Ахметов говорит о путях и средствах использования информационных технологий в национальном юридическом образовании [1. С. 71–78].

В настоящее время широкое распространение получил неофициальный термин «цифровизация». Следует отметить, что юридически закрепленного правового определения, характеризующего действительно планетарные масштабы этого явления XXI в., пока не существует. «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы», утвержденная Указом Президента Российской Федерации от 9 мая 2017 г. № 203 [18], описывает только цифровую экономику и экосистему цифровой экономики (далее – Стратегия).

Согласно ст. 4 указанного документа, цифровая экономика определяется как исключительно экономическая деятельность, где ключевым фактором производства являются цифровые данные, обработка больших объемов и использование результатов анализа которых, по сравнению с традиционными формами хозяйствования, позволяют значительно повысить эффективность различных видов производства, технологий, оборудования, хранения, реализации, поставки товаров и услуг.

В свою очередь, экосистема цифровой экономики понимается как партнерство организаций, обеспечивающих постоянное взаимодействие их технологических платформ, прикладных интернет-сервисов, аналитических систем, информационных систем органов государственной власти Российской Федерации, организаций и граждан.

Критическая оценка приведенных выше формулировок ясно показывает, что они отражают исключительно экономический аспект применения ИТ. Между тем все приведенные выше примеры научных исследований раскрывают очень широкий спектр социальных сфер, где эти инновации активно внедряются и используются.

Ранее отмечалось, что на законодательном уровне информация официально признается объектом публичных, гражданских и иных правоотношений. На данный момент этот постулат имеет не только теоретическое значение, но уже широко реализуется в практической плоскости. Об этом свидетельствует специфическое содержание ряда норм отечественного законодательства.

В качестве иллюстрации сугубо публичных правоотношений необходимо обратиться к статьям Налогового кодекса Российской Федерации [11], поскольку именно налоговые органы реализуют одну из наиболее значимых функций государства – функцию налогообложения. Она присуща самой природе налогов во все исторические периоды существования государственной системы организации общества. С ее помощью формируются необходимые денежные средства и создаются финансовые условия деятельности государства в интересах различных социальных слоев и групп населения.

В то же время публично-правовые отношения заведомо предусматривают неравноправие сторон, поскольку основным методом реализации внутренней политики государства являются директивы и императивные требования. В этом типе отношений отсутствуют диспозитивные принципы и не применяется метод договоров.

Анализ изменений и дополнений, внесенных в Налоговый кодекс Российской Федерации за последние годы, показывает, что по сравнению с другими законода-

тельными актами его содержание дополнено множеством четких и развернутых норм, последовательно определяющих порядок обязательного использования ИТ. Фактически налоговое законодательство претерпело достаточно детальную реформу, что подтверждается тремя существенными обстоятельствами:

а) с момента создания Федеральной налоговой службы (ФНС) ее сотрудники в своей деятельности оперировали огромным объемом бумажных документов, ручная обработка которых быстро стала затратной, малоэффективной и потеряла должную оперативность. Поэтому именно Федеральная налоговая служба инициировала активное внедрение ИТ в сфере повседневного общения с физическими и юридическими лицами – налогоплательщиками;

б) только с принятием законов, регламентирующих порядок использования электронных форм отчетности, содержащаяся в них информация приобрела полноценный статус в рабочем процессе. Например, электронная цифровая подпись (далее – ЭЦП) налогоплательщика имеет равную ценность с собственноручной подписью, выполненной на бумаге. Характерно, что он может заверить несколько взаимосвязанных документов одной ЭЦП – пакетом соответствующих данных, передаваемых в налоговые органы;

в) кроме того, не только в контактах с налогоплательщиками, но и во взаимодействии с другими властными структурами на федеральном, региональном и местном уровнях налоговые органы и их должностные лица в пределах своих полномочий и границ, установленных законодательством, также действуют с электронными документами.

В настоящее время с применением электронно-цифровых технологий, в том числе сети Интернет, широко проводится виртуальная сверка отчетных документов налогоплательщиков с целью выявления возможных расхождений в расчетах с бюджетом и учете налоговых платежей. Таким же образом представители налоговых органов дают официальные ответы и разъяснения по правовым условиям и другим нормативным актам.

Стоит отметить, что активное использование ИТ сыграло важную роль в том, что в 2018 г. общие налоговые поступления в бюджеты всех уровней составили 21,3 трлн рублей, что на 23 % больше, чем в предыдущем 2017 г. Если вспомнить итоги десятилетней давности, сбор налогов, по сравнению с тем отчетным периодом, увеличился практически вдвое [23].

Необходимо обратить внимание на содержание отдельных норм НК РФ, формулирующих требования к налогоплательщикам по вопросам, связанным с использованием ИТ [11].

Общеизвестно, что для осуществления эффективного и действенного налогового контроля уполномоченные органы должны располагать необходимой информацией о размере и сроках уплаты налогов и сборов, которые связаны с конкретными налоговыми периодами.

В наиболее обобщенном виде под отчетностью традиционно понимается система определенного рода данных о том или ином непосредственном объекте налогообложения. Соответствующая информация, выраженная в документальной форме, передается налогоплательщиками в Федеральную налоговую службу

в установленном порядке. Основным отчетным документом является налоговая декларация и достоверные, объективные расчеты по всем проведенным операциям.

Их характеристика и сущность содержания изложены в ст. 80 НК РФ «Налоговая декларация, расчеты» [11].

Так, согласно п. 1 указанной нормы, налоговая декларация представляет собой письменное заявление или заявление налогоплательщика, составленное в электронной форме. В последнем случае она передается по телекоммуникационным каналам связи с использованием электронной подписи или через личный кабинет налогоплательщика. Однако в любом случае налоговая декларация обязательно должна содержать следующую исчерпывающую информацию:

- об объектах налогообложения;
- о полученных доходах и понесенных расходах;
- об источниках доходов и налоговой базе;
- о налоговых льготах и исчисленной сумме налога;
- уточнению подлежат и другие данные, которые призваны служить основанием для исчисления и уплаты налога.

В свою очередь, в п. 3 ст. 80 НК РФ приводится полный перечень категорий налогоплательщиков и плательщиков страховых взносов, представляющих декларации (расчеты) по установленным формам только в электронной форме. В первую очередь к ним относятся хозяйствующие субъекты, в которых среднесписочная численность работников за предыдущий календарный год превысила сто человек. В такой ситуации соответствующая информация передается исключительно по телекоммуникационным каналам. При этом оператором электронного документооборота может быть только российская организация.

Здесь следует подчеркнуть, что в подавляющем большинстве случаев юридическая ответственность налогоплательщиков наступает именно за несоблюдение правил ведения, составления и представления отчетной документации. Эти требования закреплены в гл. 15 НК РФ «Общие положения об ответственности за совершение налоговых правонарушений» [11].

Далее необходимо проанализировать положения закона, где общественные отношения в сфере применения ИТ находятся в прямой связи с гражданскими правоотношениями. В частности, Федеральный закон Российской Федерации от 27 ноября 2018 г. № 422-ФЗ «О проведении эксперимента по установлению специального налогового режима “Налог на профессиональный доход” в городе федерального значения Москве, в Московской и Калужской областях, а также в Республике Татарстан (Татарстан)» [16].

Не только в научных кругах и среди широкой общественности, но и в комментариях представителей различных органов власти данный нормативно-правовой акт приобрел краткое, но неофициальное название: «Закон о самозанятых гражданах» (далее – Закон № 422-ФЗ).

Актуальность его принятия объясняется тем, что Закон № 422-ФЗ позволяет придать правовой статус налогоплательщиков физическим лицам, имеющим регулярный доход от определенного вида деятельности, но не уплачивающим налоги в бюджет РФ. Их численность оценивалась примерно в 15 миллионов человек, а в не-

которых источниках – до 28 млн чел. Конечно, с позиции государства эта категория граждан, как потенциальных налогоплательщиков, вызывает пристальный интерес.

В то же время в начальный период обнародование этого акта вызвало шквал диаметрально противоположных выводов. В различных обзорах встречались как поверхностные представления, так и вполне объективные взгляды на содержание и сущность экспериментального закона.

Например, в работе Бакаевой рассмотрены перспективы правового регулирования самозанятых граждан [3. С. 3–6]. В другом коллективном издании Закон № 422-ФЗ рассматривался с разных сторон. В частности, были проанализированы его положительные стороны, нововведения, а затем дана критическая оценка некоторым положениям, нуждающимся в дополнительном совершенствовании [6. С. 96–105].

Стоит отметить, что ряд существенных факторов, характеризующих Закон № 422-ФЗ, не получили должной и глубокой оценки в уже проведенных научных исследованиях.

Прежде всего, он содержит, хотя и не выраженные прямо, некоторые элементы, присущие договорным отношениям и регулируемые гражданским законодательством. Это положение может быть подтверждено несколькими аргументами.

Итак, исходя из общих требований НК РФ, налогоплательщиками являются все субъекты рынка, имеющие статус юридических лиц, индивидуальных предпринимателей и физических лиц, состоящих в юридически оформленных трудовых отношениях с работодателями. Они, безусловно, обязаны уплачивать все установленные законодательством налоги, сборы и страховые взносы.

Государство не заключает никаких договоров по этому поводу с названными субъектами. Между тем с лицами, на которых распространяются нормы Закона № 422-ФЗ, соответствующие контакты формируются в несколько иной форме. Фактически государство предлагает им свободно выбирать форму поведения, наиболее характерную для гражданских правоотношений:

- либо самостоятельно зарегистрировать свой вид деятельности в налоговых органах и уплатить налог в размере 4 или 6 % от суммы профессионального дохода;
- либо продолжать оставаться в тени с перспективой рано или поздно быть привлеченным к юридической ответственности за осуществление незаконной предпринимательской деятельности.

Закон № 422-ФЗ также содержит развернутые положения, раскрывающие достаточно свободный порядок использования широкого спектра ИТ самозанятыми гражданами в сфере взаимодействия с государственными налоговыми органами.

Например, необходимо обратиться к содержанию ст. 3 – Мобильное приложение «Мой налог». На основании его условий в настоящее время таким физическим лицам предоставляется возможность регистрации без личного посещения налоговых органов. Это делается путем обращения на сайт ФНС России через банк или портал Госуслуг. При этом заинтересованное лицо может использовать мобильный телефон, смартфон или компьютер, в том числе планшет.

Правовые и технологические новшества – это правила, согласно которым самозанятым гражданам больше не нужно подавать налоговую декларацию. Через указанное мобильное приложение передается информация о полученных доходах и понесенных расходах при реализации товаров (работ, услуг, имущественных прав).

По информации Минфина РФ, на 1 ноября 2019 г. численность самозанятых граждан, состоящих на официальном учете, составила более 240 тыс. человек [23]. В свою очередь, их совокупный задекларированный доход на конец года составил более 32,6 млрд рублей, а сумма исчисленного налога за период с начала эксперимента в четырех вышеуказанных регионах превысила 1,07 млрд руб. [25].

В течение 2020 г. действие Закона № 422-ФЗ постепенно распространялось на все регионы России, поскольку даже небольшой опыт применения, несмотря на все претензии, доказал его состоятельность и социальную значимость.

Если говорить об ИТ как об объектах сугубо гражданских правоотношений, то их индивидуальное описание в национальном законодательстве пока не представлено. Единственными исключениями являются некоторые нормативные положения общего назначения.

Например, перечень объектов гражданских прав, изложенный в ст. 128 ГК РФ, дополненной ссылкой на цифровые права [12]. Кроме того, в сам кодекс была включена ст. 141.1 «Цифровые права». На данный момент они признаны в качестве обязательных и иных прав, содержание и порядок реализации которых должны быть определены в соответствии с правилами информационной системы, а также соответствовать установленным законодательством критериям.

Специфика этого права заключается в том, что его осуществление, распространение, в том числе передача, залог, обременение иными способами или любое ограничение в распоряжении возможны только в информационной системе без обращения к третьему лицу. Обладателем цифровых прав является физическое лицо, которое, согласно правилам информационной системы, имеет возможность распоряжаться ею в полном объеме.

В иных актах, в определенной мере развивающих положения ГК РФ, также отсутствуют широкие формулировки, раскрывающие значение ИТ как объектов гражданских правоотношений. Так, в ст. 2 Федерального закона Российской Федерации от 12 января 1996 г. № 7-ФЗ (в редакции от 14 июля 2022 г.) «О некоммерческих организациях» [17] упоминается лишь о том, что данные субъекты могут осуществлять свою деятельность в виде распространения с использованием информационных технологий о принятых государством решениях и политике, проводимой органами власти.

С одной стороны, закрепление в ГК РФ и других законах краткосрочных понятий, где, хотя и в неразработанном виде, указанные нововведения фактически признаются основным объектом, вполне понятно. Граждане и юридические лица свободны в заключении любых видов договоров, представляющих для них завидный интерес в той или иной социальной сфере. Субъекты соответствующих договоров, так или иначе, призваны руководствоваться положениями различных законов, устанавливающих необходимые правила, вне зависимости от полноты их содержания и качества.

С другой стороны, закрепление четких определений в законах исключает возникновение противоречивых толкований тех или иных норм и призвано поднять на более высокий уровень технику юридических конструкций. Стоит подчеркнуть то, что вышеуказанные статьи нуждаются в дополнительной и тщательной доработке.

Тем не менее, независимо от уровня законодательных образований, собственная инициатива играет важную роль в гражданских правоотношениях. В конкретных условиях творческое использование научно-технических достижений может служить залогом позитивного достижения ранее поставленных целей. Это касается не только крупных хозяйствующих субъектов, но и индивидуальных предпринимателей и физических лиц.

В качестве примера своевременного и оригинального подхода к решению неотложных хозяйственных вопросов с использованием ИТ необходимо упомянуть действия Сбербанка России, который в июне 2019 г. запустил процесс электронной регистрации договора купли-продажи жилья в первичный рынок недвижимости. Первая такая сделка была проведена с использованием системы Единого государственного реестра объектов недвижимости (ЕГРОН).

В результате время регистрации на эту операцию сократилось в несколько раз. Если раньше соответствующая процедура занимала почти месяц, то теперь покупатель получает по электронной почте выписку из вышеназванного реестра о переходе права собственности через 3–5 дней с момента подачи документов.

Кроме того, отпала необходимость личного присутствия заинтересованного лица в органах регистрации. Указанная услуга уже применяется во всех субъектах Российской Федерации. Его правила в равной степени распространяются и на ипотечные сделки, и на покупку недвижимости за наличные денежные средства.

Заключение. В целом использование информационных технологий и других современных достижений науки и техники является выражением свободного волеизъявления участников любой разрешенной законом сделки. Целью нововведений является объективное удовлетворение многочисленных содержательных запросов физических и юридических лиц, а также реального положения дел в различных сферах общественной жизни.

Анализ кардинальных изменений и дополнений, внесенных в Налоговый кодекс РФ за последние годы, показывает, что в сфере внедрения ИТ он является наиболее прогрессивным нормативным правовым актом, поскольку содержит четкие и подробные положения, определяющие порядок комплексного использования вычислительной техники, средств связи и систем телекоммуникаций.

При этом отсутствие единого понятия «цифровизация» не является препятствием для правильной, непредвзятой и всесторонней оценки действительной практики применения ИТ в различных сферах общественных и государственных интересов, а также контакты и взаимоотношения юридических и физических лиц.

В то же время было бы логично дополнить ст. 128 ГК РФ с конкретным указанием на то, что информационные технологии, а также иные средства вычислительной техники, системы связи и телекоммуникаций являются объектом гражданских прав, наряду с иными многочисленными объектами, предусмотренными положениями ГК РФ.

В целом творческое, юридически оформленное заимствование юридических, научных, технических и иных разработок, имеющихся в арсенале других субъектов мирового сообщества, по своей сути призвано обогатить как российскую юридическую науку, так и современную практику широкого использования информационных технологий.

Список литературы

1. Ахметов А. С. К вопросу об использовании информационных технологий в юридическом образовании // Право и образование. 2017. № 10. С. 71–78.
2. Бабкина А. В. Тенденции развития экономики и промышленности в условиях цифровизации. СПбГТУ, 2017. 658 с.
3. Бакаева О. Ю. Перспективы правового регулирования самозанятых граждан // Налоги. 2018. № 5. С. 3–6.
4. Бобров А. В. Новые информационные технологии: некоторые гуманитарные аспекты // Общество и право. 2020. № 2 (20). С. 268–270.
5. Бурцев Д. Г. Проблемы совершенствования налогового администрирования. Центр подготовки персонала федеральной налоговой службы, 2018. 164 с.
6. Гогин А. А., Гогина Г. Н., Медведев В. Г. Экспериментальный закон: позитивные аспекты, инновации и критические оценки // Сборник статей Всероссийской научно-практической конференции «Проблемы научно-практической деятельности, перспективы внедрения инновационных решений». OMEGA SCIENCE, 2019. № 2 С. 9–12.
7. Ершов А. П. Информатизация: от компьютерной грамотности обучающихся к информационной культуре общества // Коммунист. 1988. С. 82–92.
8. Лапидус Л. Б. Цифровая экономика: управление электронным бизнесом и электронной коммерцией. Москва ИНФРА-М, 2019. 479 с.
9. Нам К. Электронная форма сборки в праве Европейского союза и Германии // Хозяйство и право. 2019. С. 118–128.
10. Невская А. А., Кондеев А. В. Регулирование электронной торговли в евразийском пространстве // Российский внешнеэкономический вестник. 2019. №2.
11. Об утверждении Налогового кодекса Российской Федерации от 31.07.1998 № 146-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_19671/ (дата обращения: 01.08.2022).
12. Об утверждении Гражданского кодекса Российской Федерации от 30.11.1994 № 51-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 01.08.2022).
13. Об утверждении Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 03.08.2022).
14. Об утверждении Федерального закона Российской Федерации от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_34838/ (дата обращения: 04.08.2022).
15. Об утверждении Федерального закона Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 04.08.2022).
16. Об утверждении Федерального закона Российской Федерации от 27.11.2018 № 422-ФЗ «О проведении эксперимента по установлению специального налогового режима «Налог на профессиональный доход» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_311977/ (дата обращения: 04.08.2022).

17. Об утверждении Федерального закона Российской Федерации от 12.01.1996 № 7-ФЗ «О некоммерческих организациях» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_8824/ (дата обращения: 05.08.2022).

18. Об утверждении Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 09.05.2017 № 203. URL: http://www.consultant.ru/document/cons_doc_LAW_216363/ (дата обращения: 05.08.2022).

19. Писенко К. А., Гаспарян Е. Г. Актуальные вопросы правового обеспечения антимонопольной политики на цифровых финансовых рынках // Финансовое право. 2018. № 8. С. 34–38.

20. Санникова Л. В., Харитоновна Ю. С. Цифровые активы как объекты предпринимательского оборота // Право и экономика. 2018. № 4. С. 27–34.

21. Серова О. А. Роботы как участники цифровой экономики: вопросы определения правовой природы // Гражданское право. 2018. № 3. С. 22–24.

22. Швецов А. Н. Информационное общество. Теория и практика становления в мире и в России. Москва: Красанд, 2021. 277 с.

23. Министерство финансов. URL: <https://min-fin.gov.ru/ru/press-center/> (дата обращения: 04.08.2022).

24. ФНС сообщила, сколько собрала налогов в 2018 году // Бухгалтерский учет. Налоги. Закон. URL: <https://www.gazeta-unp.ru/news/20586-fns-soob-shchila-skolkosobrala-nalogov-v-2018-godu> (дата обращения: 05.08.2022)

25. Rambler Finance. 2019. URL: <https://finance.rambler.ru/money/43201518-glava-fns-samozanyaty-zadeklarirovali-dohod-32-6-milliarda-rublej/> (дата обращения: 04.08.2022).

П. В. Бойкова,
магистрант,

Тольяттинский государственный университет

НЕОБХОДИМОСТЬ СИСТЕМАТИЗАЦИИ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Аннотация. Сегодня человечество является информационным обществом с цифровой экономикой. Общественные отношения во всех сферах связаны со стремительно развивающимися цифровыми технологиями. Регламентируют отношения, возникающие при использовании цифровых технологий, тысячи правовых актов, включая региональное законодательство. Громадный массив понятий и несогласованных правовых норм порождает противоречия и коллизии. В статье приводятся примеры, обосновывающие необходимость систематизации законодательства в сфере цифровых технологий и со стороны понятийного аппарата (на примере понятий в отношении обработки и защиты персональных данных), и с точки зрения правовых норм (на примере электронных торгов). Для регулирования и развития цифровой экономики нужны не тысячи подзаконных актов, а единый законодательный кодификационный нормативный документ. Утверждается, что в цифровом обществе будет

востребован информационный или цифровой кодекс. Создание цифрового кодекса станет объективно необходимым и состоится в ближайшие годы. В настоящее время систематизация законодательства может осуществляться путем консолидации. Консолидация может стать промежуточным мероприятием перед кодификацией. Положения статьи могут быть применены в целях совершенствования федерального и регионального законодательства.

Ключевые слова: систематизация законодательства, цифровая экономика, кодификация, консолидация, цифровые технологии, кодекс, электронные торги, кодификационный нормативный правовой акт

THE NEED TO SYSTEMATIZE LEGISLATION IN THE FIELD OF DIGITAL TECHNOLOGIES

Abstract. Humanity is currently an information society with a digital economy. Public relations in all spheres are connected with rapidly developing digital technologies. To one degree or another, thousands of legal acts, including regional legislation, regulate the relations arising from the use of digital technologies. A huge array of concepts and inconsistent legal norms generates contradictions and collisions. The article provides examples justifying the need to systematize legislation in the field of digital technologies both from the conceptual apparatus (on the example of concepts regarding the processing and protection of personal data) and from the point of view of legal norms (on the example of electronic trading). To regulate and develop the digital economy of the digital economy, not thousands of by-laws are needed, but a single legislative codification regulatory document. The author is sure that an information or digital code will be in demand in a digital society. The creation of a digital code will become objectively necessary and will take place in the coming years. Currently, the systematization of legislation can be carried out through consolidation. Consolidation can become an interim measure before codification. The provisions of the article can be applied in order to improve federal and regional legislation.

Keywords: Systematization of legislation, Digital technologies, Codification, Digital economy, Code, Electronic trading, Consolidation, Codification normative legal act

Человеческое общество, пройдя аграрную и индустриальную ступени развития, в настоящее время по полному праву может считать себя информационным или цифровым обществом, в котором высшей ценностью стали знания, информация, цифровые технологии, коммуникации.

Человечество уже не одно десятилетие является информационным обществом с цифровой экономикой. Согласно воззрениям профессионального юридического сообщества, цифровая экономика – это система экономических отношений, в которой ключевым фактором производства во всех сферах являются данные в цифровой форме, а хозяйственная деятельность осуществляется посредством цифровых технологий, при этом определяющим фактором является не использование программного обеспечения, а услуги, сервисы, товары, продаваемые путем электронной коммерции [1. С. 376].

Сегодня мы живем в мире глобального информационного пространства, больших данных, цифровых рынков, электронной демократии, электронного правительства и государства, электронных государственных и муниципальных услуг. Каждый знает про искусственный интеллект, робототехнику, автоматизацию процессов производства, цифровое моделирование, машинное обучение, дистанционное обучение, компьютерное зрение, нейросети, виртуальную и дополненную реальность, интернет вещей, цифровой код, облачные вычисления.

В нашу жизнь вошли цифровые деньги или криптовалюты, токены («заменители» ценных бумаг в цифровом мире), цифровые финансовые активы. Стремительно развивается телемедицина – обмен медицинской информацией и предоставление медицинских консультаций с использованием телекоммуникационных и компьютерных технологий, дистанционное предоставление медицинских услуг. Оцифрованы игры. Произведения искусства создаются нейросетями. Формируются базы отзывов и предложений в торговле. Цифровые технологии определяют будущие модные тренды. Осуществляются электронные голосования по выборам государственных и муниципальных руководителей и общественные обсуждения. Люди совершают покупки на сайтах и общаются в сетях...

Сегодня все сферы жизни общества пронизаны цифровыми технологиями. При этом общественные отношения, связанные со стремительно развивающимися цифровыми технологиями, должны быть урегулированы нормами права. Неоднородность регулируемой сферы делает цифровое право самой сложной и до сих пор непризнанной отраслью права. При этом нельзя не согласиться с О. В. Танимовым, который говоря о системе права в отношении использования цифровых технологий, отмечает, что «пока в научных кругах велись споры о существовании информационного права как отдельной отрасли, оно уже зарекомендовало себя в этой роли», и ставит к настоящему времени нерешенный вопрос о том, как определять процессы цифровизации и цифровое право, как соотносить цифровое и информационное право [5. С. 2–5]. Дебаты юридического научного сообщества на эти темы еще ведутся, а информационное и цифровое право объективно существует и регулирует общественные отношения, порождаемые цифровыми технологиями.

Цифровые технологии, ставшие основой экономических отношений, их предметом, с одной стороны усложняют экономику и право, требуют от них революционных изменений, с другой стороны цифровые технологии, ставшие инструментом экономики и права, являются их бесценными помощниками, оптимизирующими работу каждого юриста, каждого современного специалиста.

Справедливо отмечает Е. И. Казакевич, что в процессе развития цифровой экономики возникают правовые вызовы (трансформация общественных отношений, происходящая под влиянием цифровых технологий и влекущая необходимость правовых реформ), которые «являются как угрозой экономических процессов, так и стратегическим фактором развития» [4. С. 24–32].

Нельзя не согласиться с Т. А. Желдыбиной, что при широком внедрении цифровых технологий в различные сферы жизни юридическая наука имеет тенденцию к объединению в крупные комплексы различных областей правового знания, на пересечении которых возникают проблемы, которые могут быть решены только в рамках междисциплинарного подхода [3. С. 51–55].

Тысячи правовых актов, включая региональное законодательство, регламентируют отношения, возникающие при использовании цифровых технологий.

Сложность не только в огромном массиве правовых актов, но и в том, что многие законы и подзаконные акты между собой не согласованы, своевременно не отменяются и не изменяются, порождают коллизии и противоречия.

В цифровом праве очень ответственно необходимо подходить к формулировке правовых понятий, определений и правовых норм, характеризующихся междисциплинарностью, комплексностью, соединением воедино технических терминов и юридических конструкций. Даже сами понятия довольно сложны для понимания человеком, несвязанным с этой сферой, например, для обывателя цифровая технология блокчейн – децентрализованная, надежная, прозрачная, при этом конфиденциальная база данных для хранения последовательных блоков с информацией о предыдущих действиях в сети, еще более простыми словами блокчейн – это цепь, в которой нельзя разорвать или поменять местами звенья, или цифровая книга с возможностью добавлять страницы в режиме онлайн и отсутствием возможности отредактировать или удалить остальные страницы. Но в правовых актах блокчейн должен быть описан так, чтобы и программист не улыбнулся, и юристу было понятно, и обыватель смог разобраться, о чем идет речь.

Сегодня сложность состоит не только в сопоставлении правовых норм нескольких правовых актов, но и даже в том, чтобы разобраться в понятиях одной сферы, приведенных в различных законодательных источниках. Например, определение автоматизированной обработки персональных данных приводится в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», термин доступа к информации определяется Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», понятие аттестации объектов информатизации фигурирует в ГОСТ РО 0043–004–2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний», понятие защиты информации содержит другой ГОСТ – ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения».

При таких обстоятельствах только с понятиями и определениями, даже не рассматривая ситуацию со стороны правовых норм, очевидна необходимость систематизации законодательства в сфере цифровых технологий с целью устранения противоречий и коллизий и облегчения пользования правовым материалом.

Необходимость систематизации законодательства в сфере цифровых технологий путем принятия сводного закона рассмотрим на примере правового регулирования имущественных торгов в электронной форме.

В Российской Федерации около полусотни нормативных правовых актов регламентируют организацию и проведение обязательной процедуры публичных торгов по продаже имущества в различных сферах: при приватизации публичного (государственного и муниципального) имущества, при реализации имущества в ходе банкротства, продаже арестованного имущества в рамках исполнительного производства, заложенного имущества в порядке обращения взыскания и т. д.

На официальном сайте Российской Федерации в сети Интернет для размещения информации о торгах (torgi.gov.ru) с 2010 г. реализовано имущества на общую сумму более двух триллионов рублей (более двух миллионов лотов).

Законодателем решены проблемы труднодоступности информации о торгах, ограниченного доступа к участию в торгах, влияния человеческого фактора на определение победителя путем введения обязательной процедуры реализации и приобретения имущества онлайн на торгах, проходящих в электронной форме на электронных площадках. При этом законодательное регулирование торгов в электронной форме имеет фрагментарный характер, в действующем законодательстве отсутствуют общие нормы, регламентирующие основные принципы и правила проведения электронных торгов. Торги в каждой сфере общественных отношений имеют собственное правовое регулирование (например, в отношении информационного обеспечения торгов, оснований для отказа заявителям в участии в аукционе). Отсутствуют единые требования к различным торгам (например, к операторам электронных площадок). Для некоторых торгов установлена только обязанность их проведения, но не утвержден их порядок (например, реализация заложенного и арестованного имущества). При этом правила торгов определяются организаторами торгов самостоятельно, следствием чего являются многочисленные нарушения: размещение неполной информации о торгах, установление непредусмотренных законодательством требований, необоснованные отказы в допуске к участию в аукционах, нарушения при определении победителя торгов.

Деятельность электронных площадок в некоторых случаях не может обеспечить соблюдение всех гражданско-правовых норм. Например, до настоящего времени нереализованной на электронных площадках является процедура обязательной нотариальной заверки договоров купли-продажи доли в праве общей долевой собственности, что является прямым нарушением закона при заключении сделок в отношении долей в праве общей долевой собственности недвижимого имущества.

Комплексным решением проблемы является утверждение для всех торгов единой универсальной электронной процедуры, единого порядка их проведения, единого перечня требований к электронным площадкам, общих требований к участникам торгов, к информационному извещению, с сохранением только наиважнейших отраслевых особенностей.

Назрела необходимость в едином сводном законе о торгах в электронной форме, который должен содержать общие положения об электронных торговых процедурах. Такой закон должен утверждать нормы, которые не вправе изменять отраслевые правовые акты, и определять позиции, которые могут определяться отраслевым законодательством.

Принятие в отношении имущественных торгов в электронной форме комплексного федерального закона обеспечит единые правила и принципы организации электронных торгов.

Таким образом, систематизация законодательства в сфере цифровых технологий необходима и со стороны понятийного аппарата, и с точки зрения правовых норм.

Высшим уровнем систематизации законодательства является кодификация. П. С. Долгополов определяет ее как наиболее совершенную форму систематизации законодательства, результатом которой является новый комплексный системный законодательный акт, предназначенный для регулирования наиболее важных сфер общественных отношений [2. С. 2]. А. Н. Чашин дает определение классическому варианту кодификации законодательства, который привык понимать под этим понятием каждый юрист: «при классической кодификации законодатель заменяет

единым кодификационным нормативным правовым актом действующее разрозненное законодательство с переработкой последнего» [6. С. 18–20].

Сегодня еще идут споры? есть ли цифровое и информационное право, как они соотносятся, но нет сомнения, что в цифровом обществе будет востребован информационный или цифровой кодекс, его создание станет объективно необходимым и состоится в ближайшие годы.

Для развития и регулирования цифровой экономики нужны не тысячи подзаконных актов, в которых присутствуют понятия и правовые нормы, порождаемые цифровыми технологиями, а единый законодательный документ, в котором будут собраны все понятия, им будут даны легальные и понятные термины и определения, в котором будут логически сгруппированы, переработаны все нормативные акты в цифровой сфере.

Создание цифрового кодекса «не за горами», но не состоится в самой ближайшей перспективе из-за того, что это масштабная деятельность, необходимость которой до конца даже еще не осознана профессиональными правовым и технологическим сообществами.

На сегодняшнем этапе решением проблемы необходимости систематизации законодательства в сфере цифровых технологий может стать консолидация законодательства, при которой объединяются в единый нормативный акт без изменений правовые нормы нескольких нормативно-правовых актов. Консолидацию можно рассматривать как промежуточное мероприятие перед кодификацией.

Подытоживая сказанное, необходимо отметить, что в сегодняшнем информационном обществе с цифровой экономикой назрела и необходима систематизация огромного массива правовых понятий и правовых норм в отношении цифровых технологий, которая должна осуществляться объединением правовых норм в единые сводные комплексные законы как с изменениями и дополнениями путем кодификации, так и методом консолидации. Законодательное регулирование широкого круга постоянно меняющихся общественных отношений, порождаемых цифровыми технологиями, должно обеспечиваться комплексными правовыми актами и создавать благоприятные условия для инновационного развития цифровой экономики.

Список литературы

1. Белицкая А. В., Белых В. С., Беляева О. А. Правовое регулирование экономических отношений в современных условиях развития цифровой экономики: монография. Москва: Юстицинформ, 2019. С. 376.
2. Долгополов П. С. Понятие и виды систематизации законодательства // СПС КонсультантПлюс.
3. Желдыбина Т. А. Механизм обеспечения процесса законотворчества в условиях развития цифровых технологий // Государственная власть и местное самоуправление. 2022. № 5. С. 51–55.
4. Казакевич Е. И. Правовые вызовы применения цифровых технологий для целей устойчивого развития // Право и бизнес. 2021. № 3. С. 24–32.
5. Танимов О. В. Влияние цифровых технологий на появление новых структурных элементов системы права // Российская юстиция. 2019. № 7. С. 2–5.
6. Чашин А. Н. Формы кодификации // История государства и права. 2012. № 4. С. 18–20.

А. Г. Бордакова,

старший преподаватель кафедры
организации борьбы с экономическими преступлениями,
Самарский государственный экономический университет

А. В. Калягин,

магистрант,
Самарский государственный экономический университет

МОНИТОРИНГ И МЕРЫ ПО ПРОФИЛАКТИКЕ КАК ФОРМЫ ГОСУДАРСТВЕННОГО КОНТРОЛЯ (НАДЗОРА)

Аннотация. В статье рассматривается вопрос о разумности и практичности применения таких новых форм государственного контроля, как мониторинг и меры профилактики, применяемые государственными фискальными органами. Современное развитие государственных функций управления и контроля с применением цифровых, электронных средств и технологий становится все более востребованным. Меры по внедрению информационно-коммуникационных технологий и средств контроля и управления подтверждают свою эффективность и результативность. Проведен анализ правового обеспечения этих форм государственного контроля, обозначены положительные моменты их применения.

Ключевые слова: государственный контроль, мониторинг, меры профилактики, налоговый мониторинг, информационно-коммуникационные технологии, дистанционный контроль, цифровые электронные средства

MONITORING AND PREVENTIVE MEASURES AS A FORM OF STATE CONTROL (SUPERVISION)

Abstract. The article deals with the question of reasonableness and practicality of applying such new forms of state control as monitoring and preventive measures used by state fiscal authorities. The modern development of state functions of management and control with the use of digital, electronic means and technologies are becoming increasingly popular. Measures to introduce information and communication technologies and controls and management demonstrate their effectiveness and efficiency. An analysis of the legal support of these forms of state control has been carried out, the positive aspects of their application have been outlined.

Keywords: State control, Monitoring, Preventive measures, Tax monitoring, Information and communication technologies, Remote control, Digital electronic means

Государственный контроль является одной из основных и ведущих функций, осуществляемых государственными органами в механизме государственного управления.

На современном этапе развития госуправления все более востребованными и эффективными становятся меры по внедрению новых средств контроля и управления. Так, благодаря информационно-коммуникационным технологиям (далее – ИКТ) в сети Интернет стало возможным применение электронных и цифровых

средств в форме онлайн-мониторинга и мер профилактики по предупреждению и устранению правонарушений.

В частности, мероприятия, проводимые государством в ходе контроля над выполнением обязательных требований и профилактики нарушений, закреплены в статье 45 Федерального закона от 31.07.2020 № 248-ФЗ (ред. от 06.12.2021) «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» [4].

Федеральным законом № 248 предусматривается перечень мер профилактических воздействий, применяемых контролирующими органами Российской Федерации для эффективности стоящих перед ними целей по достижению поставленных задач, а именно: стимулирование добросовестности, самообследование, информирование, визиты, консультации, обобщение правоприменительной практики, предостережения.

Возможность применения современных средств и форм во многом связана с развитием технического прогресса за последние десятки лет. Колоссальный скачок ИКТ и развитие всемирной сети Интернет позволяют расширять горизонты воздействия госуправления в форме контроля без фактического, можно сказать даже физического, воздействия со стороны этих структур на сферу предпринимательской и иной социально-экономической сферы развития общественных отношений. Пандемия COVID-19 – это еще одна причина, которая ускорила данный процесс.

Осуществление такой формы контроля, как мониторинг, стало возможным в связи с развитием государственной политики по повсеместной цифровизации сфер публичных общественных отношений. «Электронное правительство», «Электронный бюджет» и «Портал государственных программ РФ» – это то малое, что входит в масштабную реформу госаппарата и его механизма управления и контроля.

В цивилизованном и правовом государстве без правового обеспечения механизма управления и контроля структур госаппарата не может быть и речи. Таким образом, правовое регулирование госреформ осуществляется и на федеральном, и на региональном уровнях.

Так, масштабными изменениями, закрепленными на законодательном уровне, можно назвать Федеральный закон от 31.07.2020 № 248-ФЗ (ред. от 06.12.2021) «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» (с изм. и доп., вступ. в силу с 01.01.2022) (далее – ФЗ «О государственном контроле»), а также на Налоговый кодекс Российской Федерации (Раздел V.2 «Налоговый контроль в форме налогового мониторинга») [3].

С июля 2021 г. вступили в силу изменения в ФЗ «О государственном контроле». Акцентировались изменения на мерах профилактики, об этом говорит ст. 8 вышеупомянутого закона, определяющая профилактические меры более приоритетными, чем непосредственно контрольные проверки.

Также рассматриваемый Федеральный закон закрепляет положения о правилах проведения профилактических проверок. Так, проверки могут проводиться совместно разными органами, предприниматели могут сами проявить инициативу к началу профилактической проверки, в иных случаях она должна проводиться

при их согласии. Если в ходе проверки будут выявлены серьезные нарушения, то инспектор обязан доложить об этом.

Также в ч. 1 ст. 9 Закона говорится о том, что выбор профилактических мер должен зависеть от вреда, который может быть причинен охраняемым ценностям (жизнь и здоровье граждан, сохранность объектов окружающей среды, права и свободы и др.) [1], т. е. от риска и вероятности наступления этого вреда и от перспективы характера нарушений обязательных требований.

Профилактические меры являются довольно качественной формой контроля со стороны государства, а также позволяют предпринимателям самим проявлять инициативу к ведению прозрачного с точки зрения закона бизнеса. Профилактические мероприятия позволяют лучше понять работу государственного контроля, посмотреть на ход проверок на практике, а также избежать возникновения различных видов нарушений. Поэтому не может не радовать, что государство начинает уделять данному методу больше внимания, ведь еще недавно осуществление профилактических мероприятий по контролю представляло из себя довольно формальную процедуру [2. С. 420].

Термин «мониторинг» применяется во многих областях государственного контроля, ст. 96 Федерального закона № 248-ФЗ дает его конкретное определение. «Мониторинг – режим дистанционного государственного контроля, заключающийся в целенаправленном, постоянном, опосредованном получении и анализе информации о деятельности граждан и организаций, об объектах контроля с использованием систем дистанционного контроля, в том числе с применением специальных технических средств, имеющих функции фотосъемки, аудио- и видеозаписи, измерения, должностными лицами контрольного органа в целях предотвращения причинения вреда охраняемым законом ценностям».

При проведении мониторинга с субъектами (например, предпринимателем) не ведется прямого общения, проверяющие используют для получения информации общедоступные данные, а также могут специально запросить какие-либо сведения об организации.

Если мониторинг выявил, что какая-то организация отклоняется от исполнения законных предписаний или ее деятельность может быть признана опасной для ценностей, охраняемых государством, и причиняет ущерб, то это повлечет за собой проверки организации, фирме может быть направлено предписание о том, что выявленные несоответствия необходимо устранить, или же предостережение.

Важно учитывать, что мониторинг – это добровольный метод контроля и для того, чтобы государственные органы смогли его начать, нужно добровольное соглашение контролируемого лица, заключаемое не менее чем на один год. Порядок проведения мониторинговых мероприятий утверждают контрольные органы в форме положения о виде контроля и соглашения сторон. Положение о виде контроля будет определять, какие информационные технологии нужно будет подключить, чтобы дистанционное наблюдение могло осуществляться, в каком количестве и в каких точках это оборудование будет устанавливаться, а также определяет порядок обмена бумажной документацией о работе организации.

Мониторинг является важным методом контроля со стороны государства, так как помогает вести наблюдение в любое время. Мониторинг отчасти совмещает в себе и функции профилактического характера, направленные на предупреждение и своевременное выявление возникающих отклонений деятельности субъектов предпринимательской деятельности от действующего законодательства и контролирующие функции, позволяющие вовремя обнаружить и пресечь нарушения законодательства со стороны участников правоотношений.

В соответствии с динамикой развития действующего налогового законодательства можно проследить и проанализировать эффективность функциональных возможностей применяемого с 2015 г. на практике налогового мониторинга. Налоговый мониторинг на современном этапе входит в систему финансового контроля, а точнее в систему налогового контроля, как одна из новых форм контроля государственного управления, интегрирующая в себе многогранность фактического применения его на практике.

Проведение налогового мониторинга регулируется Разделом V.2 «Налоговый контроль в форме налогового мониторинга» НК РФ (ч. 1). За время его применения популярность данной формы налогового контроля все больше растет, и диапазон его применения расширяется. Тем самым количество участников налогового мониторинга выросло во много раз.

Такая форма налогового контроля обеспечивает превентивное выявление налоговых рисков и быстрое урегулирование спорных неопределенных налоговых позиций и позволяет уже в момент планирования операций и сделок предупредить возникновение налоговых рисков и спорных ситуаций (ст. 105.26 НК РФ).

Внедрение информационных технологий позволяет сконцентрировать ресурсы ФНС и применять рискориентированный подход.

В настоящее время российская налоговая система является мировым лидером в сфере установления электронного документооборота и автоматизации процессов контроля и взаимодействия с налогоплательщиками.

С процессами цифровизации и выявления рискованных областей связана деятельность отдела предпроверочного анализа и истребования документов. Полномочия налогового инспектора позволяют не только изучать данные о предприятиях (организациях), которые находятся в его распоряжении, с помощью специально разработанных автоматизированных компьютерных программных продуктов, но и собирать статистические данные на порядок проведения сравнительного анализа по налогоплательщикам, имеющим одинаковый ОКВЭД, и те, что имеют отличные от установленных коридоров средних значений показатели деятельности, попадают под подозрение.

Автоматизированная информационная система ФНС России (АИС «Налог-3») [5] представляет собой единую информационную систему ФНС России, обеспечивающую автоматизацию деятельности ФНС России по всем выполняемым функциям, определяемым Положением о Федеральной налоговой службе РФ, утвержденным Постановлением Правительства Российской Федерации от 30.09.2004 № 506, в том числе прием, обработку, предоставление данных и анализ информации, формирование информационных ресурсов налоговых органов, статисти-

ческих данных, сведений, необходимых для обеспечения поддержки принятия управленческих решений в сфере полномочий ФНС России и предоставления информации внешним потребителям.

В целом применение автоматизированных форм проверок сокращает затраты на исполнение реальных, фактических форм проверок, осуществляемых налоговыми органами, при этом качество данной формы не столь сильно уступает остальным ныне действующим, так как осуществляемая аналитика в виде сплошного анализа основных показателей деятельности налогоплательщиков позволяет результативно выявлять налогоплательщиков, предпринимательская деятельность которых требует более тщательного исследования. На основе данной информации принимается решение о проведении выездной налоговой проверки – еще одной формы налогового контроля.

Таким образом, применение налогового мониторинга является современной и эффективной формой модернизации и совершенствования видов налогового контроля. Применение информационно-коммуникационных и цифровых средств автоматизации процесса получения данных, их сбора и анализа позволяет ФНС России оперативно и своевременно применять соответствующие меры по сбору налогов.

На современном этапе развития функции государственного контроля мониторинг как одна из его форм зарекомендовал себя эффективным и оперативным средством, используемым госорганами.

Список литературы

1. Базовая модель определения критериев и категорий риска (утв. протоколом заседания проектного комитета от 31.03.2017 № 19 (3)) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_222112/2727ab6a0cc8ab820bf1acfe7713b4b999d1e2c0/ Опубликован не был (дата обращения: 23.06.2022).
2. Морозов Г. Б. Правовое регулирование предпринимательской деятельности: учебное пособие для академического бакалавриата. 3-е изд., перераб. и доп. Москва: Юрайт, 2019. 420 с.
3. Налоговый кодекс Российской Федерации (часть первая): Федеральный закон от 31.07.1998 № 146-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_19671/ (дата обращения: 23.06.2022).
4. О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации: Федеральный закон от 31.07.2020 № 248-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_358750/ (дата обращения: 23.06.2022).
5. Об утверждении Положения об автоматизированной информационной системе Федеральной налоговой службы (АИС «Налог-3»): Приказ ФНС России от 14.03.2016 № ММВ-7-12/134@ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_195780/3d11b084ed21fa07ef56859dcf159cc81a041f39/ (дата обращения: 23.06.2022).

Е. Г. Буравцова,

студент,

Всероссийский государственный университет юстиции

ТРАНСФОРМАЦИЯ ПРАВ ЧЕЛОВЕКА В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ: ОПЫТ ЗАРУБЕЖНЫХ СТРАН

Аннотация. Статья посвящена рассмотрению и анализу динамики изменения фундаментальных прав человека в эпоху цифрового развития с использованием опыта разных стран. Отдельное внимание отводится политике регулирования деятельности в сети Интернет, а также созданию специальных учреждений для контроля и охраны прав человека в виртуальном пространстве. В качестве нормативной базы на уровне каждого государства взяты и проанализированы основополагающие документы, содержащие положения о текущем состоянии прав и свобод человека и о дальнейших методах и действиях к обеспечению их защиты в Интернете. Одним из методов исследования выступает сравнение действий и осуществления защиты прав человека нормотворческой деятельности различных государств, отмечается также специфика действий каждого из них.

Ключевые слова: права человека, цифровая среда, правовое пространство, цифровые права, граница свободы Интернета

TRANSFORMING HUMAN RIGHTS IN THE DIGITAL AGE: EXPERIENCES FROM ABROAD

Abstract. The article examines and analyses the dynamics of fundamental human rights in the era of digital development using the experience of different countries. Particular attention is paid to policies regulating activities on the Internet, as well as the creation of special institutions to monitor and protect human rights in virtual space. The fundamental documents containing provisions on the current state of human rights and freedoms and on further methods and actions to ensure their protection on the Internet are taken and analysed as a normative framework at the level of each state. One method of research is to compare the actions and implementation of human rights protections by different states, noting also the specificity of each state's actions.

Keywords: Human rights, Digital environment, Legal space, Digital rights, Frontier of Internet freedom

Одним из фундаментальных документов, закрепляющим базовые права человека является Всеобщая Декларация прав человека (далее – Декларация), длительное время сохранявшая свое традиционное содержание и облик. Однако развитие цифровых технологий стало одной из причин изменения уже существующих положений с целью соответствовать той информационной реальности, в которой живет человечество на данный момент.

Рассматривая настоящую Декларацию, стоит обратить внимание, прежде всего, на содержание таких ее статей, как право на жизнь, свободу и личную неприкосно-

венность (ст. 3 Декларации), право на защиту от дискриминации (ст. 7 Декларации) на примере, КНР и Австралии и США.

Все государства, названные выше, взяли на себя обязательство создавать необходимые условия для обеспечения и сохранения естественных прав в Интернете. Например, в Австралии защита прав человека в Интернете является обязанностью специально созданных для этого профильных институтов на государственном уровне, первостепенная задача которых охранять и контролировать соблюдение прав человека как в онлайн-, так и офлайн-пространстве [1].

В США другой подход: здесь на федеральном и региональном уровнях принимают законы, обеспечивающие безопасность и защиту от киберугроз. Причем виды составов киберпреступлений постоянно обновляются, появляются новые: например, буллинг и разжигание ненависти.

Одно из государств с самой строгой политикой регулирования деятельности в Интернете – Китайская Народная Республика (далее – КНР): здесь уже с 1997 г. существует уголовный кодекс, криминализирующий преступления, а основным законом, регулирующим право интернет-среды является «Белая книга», состоящая из ключевых шести пунктов, включающих в себя направления реализации политики в сети, а также цифровые права человека и их соблюдение в виртуальном пространстве. В соответствии с положениями Белой книги в КНР правительство поощряет развитие коммуникационных систем в интернет-среде и предоставление доступа общественности ко всем новостям. Однако гражданам гарантируется свобода слова: «граждане Китая в полной мере пользуются свободой слова в Интернете. С правом на свободу слова в Интернете они могут высказывать свое мнение различными способами в Интернете. Энергичный обмен идеями в сети – есть основная характеристика развития Интернета в Китае» [2].

Также Белая книга КНР защищает права несовершеннолетних: правительство КНР уделяет большое значение онлайн-безопасности детей и способствует принятию мер для их защиты, поскольку они самые многочисленные субъекты интернет-пространства и больше всех нуждаются в охране. Так, в КНР был принят закон, предусматривающий меры предотвращения чрезмерного использования интернета несовершеннолетними. В нем прописано, что запрещено продавать, производить, сдавать в аренду электронные публикации и информацию, представляющих вред для несовершеннолетних. Также властями КНР поощряется разработка инструментов и технологий, способствующих защите детей в неизведанной для них среде [3].

Следующим государством в продвижении прав человека выступает Австралия. Здесь основным источником, затрагивающим цифровые права человека, является документ по вопросам прав человека и технологий от 2018 г.: в нем зафиксированы и проанализированы права, связанные с цифровой средой, а также влияние интернета на жизнь граждан. В документе подчеркивается, что право на свободу выражения мнений приравнивается к свободному доступу в Интернет [4]. Также австралийское законодательство является сторонником позиции, что цифровые права – это не новое поколение прав, а часть уже известных до этого гражданских, политических, экономических, социальных и культурных. По вопросу реализации прав в интернете Австралия придерживается таких принципов как

участие, ответственность, отсутствие дискриминации, расширение прав и возможностей, законность – в науке их называют правозащитными принципами PANEL [5]. Правительством Австралии была принята стратегия электронной безопасности 2019–2022 гг. по обеспечению безопасности граждан и защиты их прав в Интернете, проводимыми мероприятиями которой являются: профилактика нарушений в Интернете посредством информирования граждан, как быть в безопасности, что делать, если кибератака уже произошла, специальные программы развития цифровой грамотности для социально уязвимых групп, защита австралийцев и людей, отстаивающих права человека в интернете с помощью систем отчетности, расследований и уведомлений [6].

Другой подход наблюдается в Штатах: несмотря на то, что данное государство принимает активное участие в работе различных организаций по защите прав и свобод в сети, в нем так и не было принято ни одной инициативы по праворегулированию Интернета, хотя таких было немало (например, Закон о мошенничестве в Интернете, устанавливающий ответственность за несанкционированный доступ к конфиденциальным данным). Более того, в США даже нет единого закона о защите свободы слова в цифровом пространстве.

Также разнятся и мнения о свободе Интернета в стране: за 2020 г. уровень открытости Сети для всех граждан был оценен специалистами в 76 баллов из 100 как средне свободный. В ушедшем же году данный показатель стал выше на единицу, сохранив прежний статус свободы для граждан. Говоря о конфиденциальности, компания Freedom House также отмечает среднее значение: она составляет 25 баллов из 40, что также является нормальным показателем свободы Интернета [7]. Однако у организации «Репортеры без границ» другое видение ситуации: уже несколько лет Штаты находятся в «списке врагов сети» вместе такими государствами как КНДР и Иран, что говорит о сомнительном показателе свободы Сети [8].

Проведенное исследование на основе опыта разных государств показало разницу подходов к цифровым правам и свободе интернета как единого пространства. Так, сделать однозначный вывод об эффективности моделей разных стран нельзя, поскольку общего мнения о свободе глобальной среды не сформулировано. Однако происходит постепенный переход к позиции, что интернет должен быть открытой ячейкой для доступа любого гражданина независимо от его расы и социального положения. По поводу принадлежности цифровых прав к естественным правам человека существуют дискуссионные мнения.

Список литературы

1. Конопий А. С. Цифровая трансформация государства и права Китая // Северо-Кавказский юридический вестник. 2021. № 3. URL: <https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-gosudarstva-i-prava-kitaya> (дата обращения: 08.09.2022).
2. Соединенные Штаты: Страновой отчет о свободе сети за 2020 год. URL: <https://freedomhouse.org> (дата обращения: 08.09.2022).
3. Стремление к общим ценностям человечества – подход Китая к демократии, свободе и правам человека. 2021. URL: <http://english.www.gov.cn> (дата обращения: 08.09.2022).

4. A human rights based approach: an introduction. 2008. URL: <https://www.scottishhumanrights.com> (дата обращения: 08.09.2022).
5. E-Safety strategy plan. 2022. URL: <https://www.esafety.gov.au/about-us/who-we-are/regulatory-schemes> (дата обращения: 08.09.2022).
6. Free and Equal: An Australian conversation on human rights. 2019. URL: <https://humanrights.gov.au/free-and-equal> (дата обращения: 08.09.2022).
7. Institute for Security & Development Policy. 2020. URL: <https://isdpr.eu> (дата обращения: 08.09.2022).
8. Marshall Jarrett H. Prosecuting Computer Crimes. Office of Legal Education Executive Office for United States Attorneys, 2007.

З. А. Булатова,
аспирант,

кафедра конституционного и административного права,
Казанский (Приволжский) федеральный университет

РАЗВИТИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В УСЛОВИЯХ СОВЕРШЕНСТВОВАНИЯ КОНСТИТУЦИОННО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРОСТРАНСТВЕННОГО РАЗВИТИЯ

Аннотация. В статье рассматриваются вопросы, связанные с правовым регулированием цифровых технологий для обеспечения ликвидации инфраструктурных ограничений. Анализируется принцип равенства прав субъектов во многих областях общественных отношений, проанализировано стратегическое планирование Российской Федерации. Сделаны выводы о том, что в области развития цифровизации необходимо устранить правовых пробелов в части привлечения должностных лиц к ответственности за нарушение законодательства в сфере стратегического планирования.

Ключевые слова: пространственное развитие, право, цифровые технологии, правовое регулирование, цифровизация, стратегическое планирование, цифровая трансформация

THE DEVELOPMENT OF DIGITAL TECHNOLOGIES IN THE CONTEXT OF IMPROVING THE CONSTITUTIONAL AND LEGAL REGULATION OF SPATIAL DEVELOPMENT

Abstract. The article discusses issues related to the legal regulation of digital technologies to ensure the elimination of infrastructure restrictions. The principle of equality of rights of subjects in many areas of public relations is analyzed, and the strategic planning of the Russian Federation was also analyzed. It was concluded that in the field of digitalization, it is necessary to eliminate gaps in terms of holding officials accountable for violations of strategic planning is both relevant and timely.

Keywords: Spatial development, Law, Digital technologies, Legal regulation, Digitalization, Strategic planning, Digital transformation

В Стратегии пространственного развития, утвержденной распоряжением Правительства Российской Федерации от 13 февраля 2019 г. № 207-р [6], отмечается, что для обеспечения ликвидации инфраструктурных ограничений федерального значения и повышения доступности, а также качества информационно-телекоммуникационной инфраструктуры необходимо устранять цифровое неравенство субъектов Российской Федерации за счет создания информационно-телекоммуникационной инфраструктуры для обеспечения высокоскоростной передачи данных, с тем чтобы обеспечить доступность услуг связи и информационных технологий для населения, особенно в труднодоступных местностях, в которых проживает большое количество населения.

По данным Федеральной службы государственной статистики за 2020–2021 гг., у 24 % домохозяйств отсутствует доступ к Интернету. В основном такое положение дел обусловлено недостаточностью у граждан денежных средств для подключения к глобальной сети и по другим причинам. Также, по данным Росстата, отсутствие Интернета наблюдается в сельских населенных пунктах с численностью около 200 человек, а у 38 % семей все еще отсутствуют компьютеры [7]. Конечно, такие данные вызывают определенную степень тревоги, прежде всего у Правительства Российской Федерации, предлагающего решать эти проблемы в рамках Стратегии пространственного развития, согласно положениям которой предлагается повышать информационно-телекоммуникационную связанность территорий страны за счет широкого использования систем спутниковой связи в труднодоступных и удаленных районах. Между тем анализ Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» [9] показывает, что в нем не закреплено такое понятие, как «удаленные местности», которое следует отождествлять с труднодоступными и отдаленными местностями, тогда как в соответствии с п. 3 ст. 2 Федерального закона от 22 мая 2003 г. № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении расчетов в Российской Федерации» субъекты предпринимательской деятельности, осуществляющие свою деятельность в указанных местностях, могут не использовать контрольно-кассовую технику при расчетах с покупателями [8]. Это и не удивительно, поскольку если человек пришел совершить покупку в магазин и решил рассчитаться зарплатной и иной картой, то сделать это невозможно, так как контрольно-кассовая техника не подключена к Интернету. Это означает, что расчет за покупку можно осуществить только в наличной форме. Аналогичные вопросы, связанные с невозможностью в полном объеме реализовывать свои права, свободы и законные интересы, возникают и в сфере образования, когда дети не могут принять участие в конкурсных, образовательных и иных мероприятиях, проводимых с использованием Интернета, и в сфере трудовой, культурно-просветительной и иной деятельности.

Решение перечисленных проблем связано с необходимостью устранения межрегионального неравенства субъектов Российской Федерации как одной из задач Стратегии пространственного развития Российской Федерации. Здесь необходимо подчеркнуть, что цифровое неравенство субъектов Российской Федерации с конституционно-правовой точки зрения выглядит весьма оригинально, поскольку положения Основного закона, наоборот, провозглашают принцип равен-

ства прав субъектов во многих областях общественных отношений, что согласуется с положениями п. 4 ст. 5 и п. 2 ст. 72 Конституции Российской Федерации [1]. Между тем необходимо отметить, что сама по себе категория неравенства проявляется в объеме компетенций уполномоченных органов государственной власти, а также в диспропорциях субъектов Российской Федерации по уровню социально-экономического развития, в которых действительно проявляется неравенство, поскольку по уровню развития процессов информатизации субъекты Федерации равными быть не могут, так как это обусловлено географическими, климатическими и иными особенностями местоположения регионов. К тому же регионы различаются по степени финансового и материального развития.

В то же время функционал у органов власти всех субъектов РФ, согласно Конституции РФ и законодательства, одинаков, но «осуществление функции возможно только в том случае, если реализующий ее орган наделен достаточными полномочиями и ресурсами» [2. С. 50].

Так, общеизвестно, что Республика Татарстан является субъектом-донором, тогда как можно привести немало примеров, когда субъекты Федерации характеризуются дотационным положением, что, конечно же, не позволяет эффективно развивать информационно-телекоммуникационную связанность внутри региона, особенно в отдаленных и труднодоступных местностях. Уровень финансового и материального обеспечения субъектов Российской Федерации, является одним из важнейших показателей успешности реализации стратегий в области цифровой трансформации социальной, экономической сферы, областей государственного и муниципального управления, поскольку без должного уровня финансирования развивать такие направления, как искусственный интеллект, платформенные решения и другие, не представляется возможным.

В настоящее время субъекты Российской Федерации на уровне исполнительных органов государственной власти разработали стратегии в области цифровизации отраслей государственного и муниципального секторов хозяйствования. Между тем анализ таких стратегий [3–5] позволяет прийти к выводу, что в них запланировано весьма объемное количество мероприятий, которые требуется разрешить в короткие сроки. Причем система мероприятий настолько различна, ибо затрагивает различные области общественных отношений: сельское хозяйство, строительство, молодежную политику, экологию и т. д., – что возникает вопрос, каким образом в короткие сроки, особенно в финансовом плане, обеспечить все эти мероприятия. Важным еще является вопрос определения круга субъектов, ответственных за реализацию таких стратегий, поскольку, исходя из анализа стратегий цифровизации социальной, экономической сферы, областей государственного и муниципального управления, не совсем ясно, кто будет нести юридическую ответственность при невыполнении или ненадлежащем исполнении мероприятий, направленных на цифровизацию отраслей государственного строительства. Так, в Федеральном законе № 172 «О стратегическом планировании в Российской Федерации», а именно этот закон положен в основу формирования Стратегии пространственного развития, утвержденной распоряжением Правительства Российской Федерации от 13 февраля 2019 г. № 207-р, закреп-

ляется, что лица, виновные в нарушении законодательства в сфере стратегического планирования, несут дисциплинарную, гражданско-правовую, административную ответственность [10]. Однако анализ норм трудового, административного и гражданского законодательства Российской Федерации показывает, что в них отсутствуют специальные нормы, предусматривающие санкции за нарушение законодательства в сфере стратегического планирования. А поскольку сфера стратегического планирования затрагивает такую важную область, как информационно-телекоммуникационная инфраструктура и предмет правового регулирования цифровизации, то устранение правовых пробелов в части привлечения должностных лиц к ответственности за нарушение стратегического планирования является и актуальным, и своевременным. Представляется, что решение вышеизложенных вопросов позволит усовершенствовать процесс поступательного развития цифровых технологий в условиях конституционно-правового регулирования пространственного развития.

Список литературы

1. Конституция Российской Федерации. Принята всенародным голосованием 12.12.1993 // Собрание законодательства Российской Федерации. 2020. № 1. Ст. 4392.
2. Малый А. Ф. Функции органов государственной власти: институционализация правовой категории // Ученые записки Казанского ун-та. Серия: Гуманитарные науки. 2012. Т. 154, кн. 4. С. 46–51.
3. О применении контрольно-кассовой техники при осуществлении расчетов в Российской Федерации: Федеральный закон от 22.05.2003 № 54-ФЗ // Собрание законодательства Российской Федерации. 2003. № 21. Ст. 1957.
4. О связи: Федеральный закон от 07.07.2003 № 126-ФЗ // Собрание законодательства Российской Федерации. 2003. № 28. Ст. 2895.
5. О стратегическом планировании в Российской Федерации: Федеральный закон от 28.06.2014 № 172-ФЗ // Собрание законодательства Российской Федерации. № 26. Ч. I. Ст. 3378.
6. Об утверждении Стратегии в области цифровой трансформации отраслей экономики, социальной сферы и государственного управления Республики Мордовия // Известия Мордовии. 2021. № 93–42.
7. Об утверждении Стратегии в области цифровой трансформации отраслей экономики, социальной сферы и государственного управления Республики Татарстан // Собрание законодательства Республики Татарстан. 2021. № 67. Ст. 1876.
8. Об утверждении Стратегии в области цифровой трансформации отраслей экономики, социальной сферы и государственного управления в Чувашской Республике. URL: <https://docs.cntd.ru/document/574848338?section=status> / (дата обращения: 18.06.2022).
9. Об утверждении Стратегии пространственного развития Российской Федерации на период до 2025 года: распоряжение Правительства РФ от 13.02.2019 № 207-р // Собрание законодательства Российской Федерации. 2019. № 7. Ст. 702.
10. Росстат: почти треть домохозяйств не имеет доступа к интернету. URL: <https://www.kommersant.ru/doc/4900915> / (дата обращения: 18.06.2022).

Н. И. Бурак,
студент,

Гродненский государственный университет имени Янки Купалы

О ВЛИЯНИИ РАЗВИТИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА СУЩНОСТЬ ПРАВООТНОШЕНИЙ

Аннотация. Цель данного исследования – определение влияния развития цифровых технологий на сущность правоотношений. Дается определение цифровых технологий путем исследования их природы. Проводится сравнительный анализ цифровой и аналоговой информации. Показан процесс преобразования из аналогового в цифровой сигнал, предопределяющего цифровую технологию. Исследуется влияние развития цифровых технологий на правоотношения методом анализа и индукции, т. е. изучается каждый элемент правоотношения в отдельности. Автор указывает на появление новых цифровых объектов, таких как цифровые товары и персональные данные. Анализируется появление новых субъектов, связанных с цифровыми технологиями. Исследуется правосубъектность искусственного интеллекта. Проводится исследование влияния цифровых технологий на появление новых цифровых прав и обязанностей, в том числе и потенциально конституционных. Дается оценка влияния развития цифровых технологий на появление новых правонарушений, связанных с цифровыми технологиями.

Ключевые слова: правоотношения, цифровые технологии, аналоговые технологии, цифровая информация, аналоговая информация, цифровизация, информатизация общества, искусственный интеллект

THE IMPACT OF THE DEVELOPMENT OF DIGITAL TECHNOLOGIES ON THE ESSENCE OF LEGAL RELATIONS

Abstract. The purpose of this study is to determine the impact of the development of digital technologies on the essence of legal relations. The author defines digital technologies by studying their nature. A comparative analysis of digital information and analog information is carried out. The process of conversion from an analog signal to a digital signal, which determines the digital technology, is shown. The influence of the development of digital technologies on legal relations is studied by the method of analysis and induction, that is, each element of the legal relationship is studied separately. The author points to the emergence of new digital objects, such as digital goods and personal data. The emergence of new subjects related to digital technologies is analyzed. The legal personality of artificial intelligence is investigated. The impact of digital technologies on the emergence of new digital rights and obligations, including potentially constitutional ones, is being investigated. An assessment of the impact of the development of digital technologies on the emergence of new offenses related to digital technologies is given.

Keywords: Legal relations, Digital technologies, Analog technologies, Digital information, Analog information, Digitalization, Informatization of society, Artificial intelligence

Информация – это одна из важных потребностей человека, хотя бы минимальное удовлетворение которой способствует развитию личности и общества. А значит, перед нами встает вполне очевидный вопрос: а будут ли человек и общество стремиться к тому, чтобы как можно наилучшим образом удовлетворять свои потребности? Безусловно, да. Как потребность в передвижении направило человечество к созданию автомобилей, так и потребность в информации направило к созданию технологий, улучшающих получение, сбор, обработку и т. д. информации. Появление новых технологий влечет за собой и появление новых отношений, связанных с данными технологиями. Но разве право не стремится упорядочить значимые для общества и человека общественные отношения? Конечно же, право желает упорядочить связи между людьми, в том числе и новые, ранее не известные связи.

Изучение любого объекта невозможно без его определения. Прежде чем приступить к рассмотрению, безусловно, самого интересного аспекта выше заявленного вопроса, а именно к изучению влияния развития цифровых технологий на сущность правоотношений, необходимо обозначить ключевые понятия. Таким образом, сначала нам необходимо ответить на вопрос. А что есть цифровые технологии? И ответ этот должен быть конкретным, а не абстрактным.

Исходя из семантики словосочетания «цифровые технологии» вполне, что это такие технологии, сущность которых кроется в цифрах. Однако такое объяснение, очевидно, недостаточно. Пойдем от обратного. Какие технологии противоположны цифровым? Таковыми являются аналоговые технологии. Семантика последнего представляется более ясной, нежели первой (цифровые технологии). Так, аналоговые технологии основаны на использовании определенной аналогии или же, иначе, абстракции. Следует сказать, что изучение понятия аналоговой информации (и аналоговой технологии) несет в себе философский окрас, так как эти явления плод размышлений, а не рук. Например, книга – это яркий пример аналоговой технологии. Наши слова – это аналоговая информация, так как это определенный набор звуков, который мы силой мысли, т. е. создав абстракцию, назвали словами, а в последующем придали им форму. Но для любой информации необходимы действия, такие как поиск, получение, передача, сбор, обработка и т. д. Следовательно, для осуществления данных действий необходима определенная технология. Не назовем ли мы технологию для аналоговой информации аналоговой? Конечно, да, такая технология и будет носить название аналоговой технологии. Возвращаясь к примеру с книгой, сейчас стало вполне ясно, что слова, находящиеся в книге, – это абстракция (аналогия) звуков. Поэтому книга, содержащая аналоговую информацию, является аналоговой технологией. Мы изучаем не слова в прямом их смысле, а информацию, передаваемую данной абстракцией звуков.

Однако следует заметить, что аналоговая информация тесно связана с понятием аналогового сигнала. Аналоговый сигнал является непрерывным, который порождается физическим процессом, а следовательно, его можно измерить в любой момент времени.

М. В. Гурьянова и А. С. Аброскин определяют аналоговый сигнал как непрерывную функцию, с неограниченным числом значений в различные моменты

времени. Наиболее часто встречающимся аналоговым сигналом являются звуки нашей речи, которые на осциллограммах имеют различные, причудливые формы. Аналоговые сигналы изменяются по тому же закону, что и описываемые им физические процессы [9. С. 219].

Однако необходимо вернуться к вопросу о цифровых технологиях. Проводя параллель с аналоговыми технологиями, можно говорить о том, что определение цифровых технологий значительно зависит от содержания цифровой информации. В свою очередь, цифровая информация определяется качеством сигнала. Ввиду всего вышеперечисленного представляется разумным изучить позицию исследователей данного вопроса на предмет совпадения или различия с представленным выше нами мнением. А в последующем углубиться и изучить значимую для нас классификацию сигналов, которые определяют, будет ли технология цифровой или нет.

С. П. Кушниренко трактует цифровую информацию следующим образом. Так, цифровая информация – это любая информация, которая представлена в виде определенной последовательности цифр, доступной для ввода, обработки, хранения и передачи с помощью технических устройств [14]. Безусловно, технические устройства в данном определении ввиду того, что они обслуживают цифровую информацию, представляются нам цифровыми технологиями. Однако здесь возникает вопрос о допустимости именовании технических устройств цифровыми технологиями. На наш взгляд, понятия технические устройства – это материализованные цифровые технологии. Так как технология – это совокупность методов и инструментов для достижения поставленной цели, а устройство – это объект материального мира, чаще всего со сложной структурой, созданный для выполнения определенных функций. Поэтому цифровые технологии и цифровые устройства, на наш взгляд, соотносятся как объект и предмет.

Представляет особый научный интерес изучение признаков исследуемых нами технологий. Так, Ся Чжюань выделяет следующие характеристики цифровых технологий.

1. Стандартно используется двоичный файл, поэтому два стабильных состояния компонентов могут использоваться для представления двоичного файла (например, «высокий уровень» и «низкий уровень»). Поэтому базовая схема единиц измерения проста, а требования к точности каждого компонента в цепи не очень строгие, и параметры компонента могут быть значительно распределены.

2. Сильная противоинтерференционная способность и высокая точность. Поскольку цифровые технологии передают, обрабатывают и обрабатывают двоичную информацию, внешний мир нелегко беспокоить, поэтому ее против интерференционная способность сильна. Кроме того, это может повысить точность за счет увеличения цифр двоичных чисел.

3. Цифровые сигналы легко хранить в течение длительного времени, поэтому можно хранить большое количество ценных информационных ресурсов.

4. Хорошая конфиденциальность, шифрование может осуществляться в цифровых технологиях, так что некоторые ценные информационные ресурсы нелегко украсть.

5. Он универсален и может использовать стандартизированные логические компоненты для формирования различных цифровых систем [21. С. 141–142].

Таким образом, можно констатировать, что исследователи сходятся во мнении, что цифровой информации присущ дискретный сигнал, определенный набор цифр и она предназначена для использования с помощью специальных устройств.

Ранее было указано, что цифровая информация является более универсальной и надежной, нежели аналоговая информация. Поэтому возникает вполне разумный вопрос о конвертации одной информации в другую. Так, человек принимает аналоговую информацию, используя органы чувств, а вычислительная техника, как правило, работает с цифровой информацией. По этой причине часто аналоговую информацию следует преобразовывать в цифровую. В компьютерах это делает аналогово-цифровой преобразователь. Противоположную операцию осуществляет цифро-аналоговый преобразователь [1].

Соответственно, информацию необходимо преобразовывать для того, чтобы можно было ее воспринять как на аналоговой, так и на цифровой технологии. Данный процесс преобразования аналоговой информации, которая изначально имеет волнообразный сигнал (непрерывный), в цифровую информацию именуется дискретной обработкой. Из самой семантики слова «дискретный» видно, что преобразованный сигнал является прерывистым. Но данная прерывистость означает то, что цифровая информация – это набор дискретных сигналов, которые могут принимать только определенный набор значений, меняющихся скачкообразно.

При обработке сигналов в вычислительных устройствах его отсчеты представляются в виде двоичных чисел, имеющих ограниченное число разрядов. Вследствие этого отсчеты могут принимать только лишь конечное множество значений и, следовательно, при представлении сигнала неизбежно происходит его округление.

Процесс преобразования отсчетов сигнала в числа называется квантованием по уровню, а возникающие при этом ошибки округления – ошибками (или шумами) квантования. Сигнал, дискретный по времени и квантованный по уровню, называют цифровым сигналом [2. С. 4–5]

Таким образом, информация будет соответствовать сигналу. А технология – информации. Для лучшего понимания процесса преобразования информации необходимо привести пример (рис. 1).

Исходя из всего вышперечисленного, можно констатировать, что признаком цифровой технологии является функционирование путем использования определенного набора цифр – цифровой информации, состоящей из цифровых сигналов. Важность цифровых технологий заключается в том, что они используют универсальную информацию, которую можно преобразовать в практически любую аналоговую информацию.

Следует сказать, что законодательное закрепление понятия цифровых технологий не столь необходимо ввиду того, что теория права, связанная с цифровизацией и информатизацией, все еще разрабатывается и не устоялась. Поэтому мы придерживаемся того мнения, что изначально необходимо выработать четкую и лаконичную теоретическую базу.

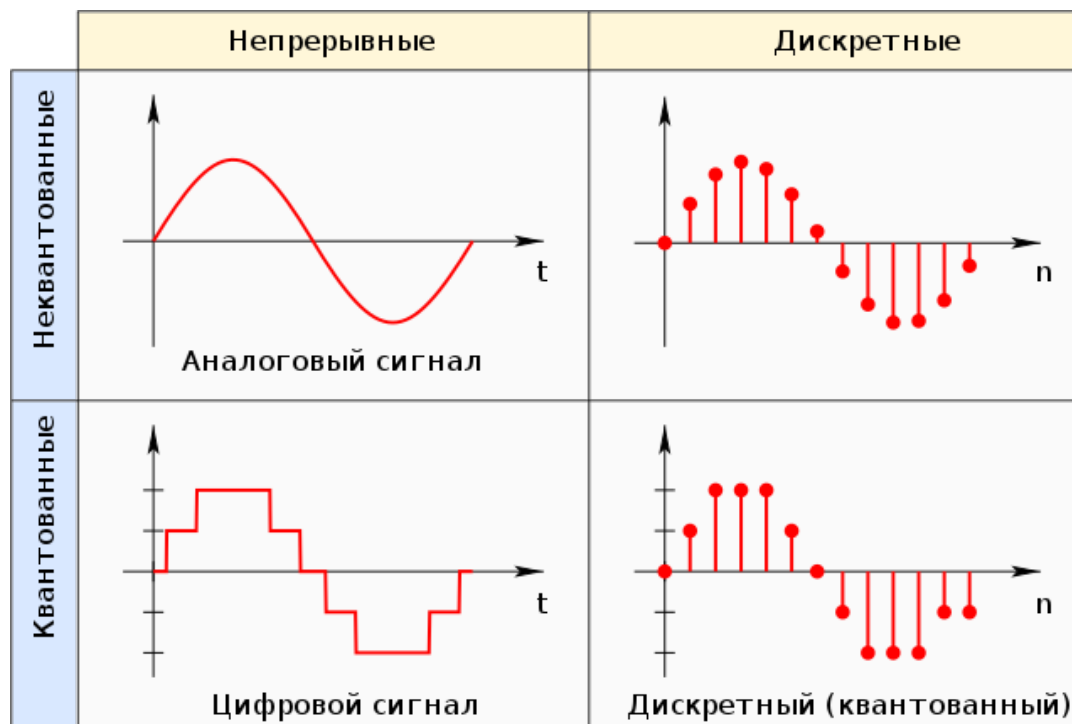


Рис. 1. Классификация сигналов

А что есть развитие цифровых технологий? Развитие цифровых технологий означает создание новых и улучшение старых технологий, основанных на обработке цифровой информации. Вполне очевидно, что такое развитие способствует повышению эффективности использования информации. А это в свою очередь не может не затрагивать и правоотношения, в которых, безусловно, информация о правах и обязанностях играет весьма важную, если не ключевую роль.

Обозначив необходимые понятия и связи в области цифровых технологий необходимо перейти к определению правоотношения и его структуры. Ибо только придя к единому пониманию возможно дальнейшее плодотворное изучение заявленного вопроса.

А. А. Кабанов и С. В. Чижов указывают, что правоотношение состоит из трех элементов: объект, субъекты, содержание. Под содержанием понимается действие, процесс, основанный на юридическом факте, определение и реализация прав и обязанностей субъектов [12. С. 22]. Мы согласны с такой структурой правоотношения, отчего в дальнейшем будем изучать влияние развития цифровых технологий именно исходя из вышеназванной трехэлементной структуры правоотношения.

Объект правоотношения – это общественные отношения, по поводу чего лица (субъекты правоотношения) вступают в соответствующие правоотношения. Объект правоотношения конкретизируется в предмете, который может быть как материальным, так и нематериальным. Например, объект правоотношения – право собственности, а предмет – индивидуально-определенная недвижимость. Значимость объекта правоотношения велика, ибо его отсутствие означает отсутствие правоотношения. По этой причине возникает вполне закономерный вопрос. На что конкретно будут направлены права и обязанности субъектов правоотно-

шения? Цифровые технологии – это более эффективное использование информации, оттого многие новшества или изменения будут тесным образом связаны с регулированием информации.

Статья 141.1 Гражданского кодекса Российской Федерации регламентирует «цифровые права». Под таковыми законодатель Российской Федерации понимает названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам. Осуществление, распоряжение, в том числе передача, залог, обременение цифрового права другими способами или ограничение распоряжения цифровым правом возможны только в информационной системе без обращения к третьему лицу [7]. Таким образом, законодательное закрепление цифровых прав указывает на существование новых объектов правоотношений, возникших или видоизмененных ввиду развития цифровых технологий. Но, безусловно, цифровые права могут также входить и в содержание правоотношения.

Вызывает научный интерес мнение А. В. Нестерова, обосновывающего существования цифрового продукта. Так, он считает, что объект цифровых прав можно рассматривать как цифровой продукт в виде цифрового документа, обладающего не только объектными, но и субъектными (продуцентными) и (или) инструментальными свойствами. Поэтому он может не только продуцировать иные цифровые документы, но и выполнять как транзакции в цифровой среде, так и действительные действия в интернете вещей. Автономного робота также можно рассматривать как цифровой продукт, если он содержит цифровую систему. Цифровой продукт может отображать не только существующие ситуации (виртуальные, фиктивные и (или) мнимые), но и действительные, не только статичные ситуации в некоторый момент времени, но и динамичные ситуации в определенном интервале времени, а также определенное окружение ситуации. В качестве элементов таких ситуаций могут выступать их субъекты, объекты и (или) инструменты, которые отображаются в цифровом продукте [17. С. 15].

Развитие цифровых технологий указало на потребность в защите информации о гражданах. Сегодня такая информация именуется персональными данными. Их значимость подтверждается вниманием, уделяемым законодателями различных стран. Так, сегодня существуют такие законодательные акты, как:

- 1) Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных»;
- 2) Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- 3) Закон Республики Казахстан от 21 мая 2013 г. № 94-V «О персональных данных и их защите»;
- 4) иные схожие акты законодательства различных государств о защите персональных данных.

Представляется, что наша задача – это очертить круг новых цифровых объектов. И нет надобности в даче определения персональных данных, когда оно содержится в законодательстве. Так, законодатель Республики Беларусь считает, что персональ-

ные данные – это любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано [18].

Немаловажным вопросом, связанным с персональными данными, являются цифровые следы. Так, В. Е. Матвеев указывает, что в течение своей сознательной жизни каждый современный человек оставляет цифровой след в Интернете (digital imprint) – совокупность информации о человеке и его вкладе в цифровое пространство. Это могут быть личные профили и учетные записи в социальных сетях, информация о посещаемых вами веб-сайтах, открытые и созданные файлы, личные сообщения и комментарии, видео, фотографии и другие виртуальные действия, включая ввод личных данных пользователя. Некоторые из этих материалов находятся в открытом доступе, в то время как другие являются конфиденциальными [26]. Соответственно, существуют угрозы персональным данным, и именно поэтому необходимы инструменты для их защиты.

Сегодня существует такое явление, как big data, которое означает большие данные. Big data – это статистика действий, интересов и предпочтений пользователей, которая собирается автоматически в сети Интернет и в последующем может использоваться как в коммерческих, так и в иных целях. Вполне очевидно, что это затрагивает существенные интересы граждан на тайну личной жизни и на их свободное пользование персональными данными. Так, В. К. Шайдуллина, с мнением которой мы согласны, указывает на то, что после возникновения технологий big data понятие «информационное общество» обрело первоначальный смысл, а информация получила статус ценнейшего актива, выступающего в качестве движущей силы информационного общества. Большие данные могут эффективно использоваться в разных сферах: банковской и страховой деятельности, медицине, электронной торговле и правоохранительной работе. Тем не менее у них имеются и недостатки, главный из которых – вторжение в частную жизнь людей. Также следует отметить, что технологии big data обнажают очевидный факт: действующее законодательство о персональных данных все меньше и меньше отвечает требованиям современности, в связи с чем нуждается в скорейшем реформировании [23]. Технология, позволяющая получать огромные массивы неструктурированной информации о каком-либо факте или общественном процессе с большой степенью вероятности, не сможет предварительно оценить законность получения персональных данных людей. Другими словами, весь объем данных, собранных big data, не может быть «чистым» с юридической точки зрения [8].

Существование цифровых технологий и их развитие сотворило понятие нового объекта – цифрового образа. Заслуживает особого внимания исследование Д. Е. Богданов на тему влияния биопринтинга на развитие концепции защиты права на цифровой образ. Он делает вывод, что право на персональный образ человека эволюционирует в право на цифровой образ. И это можно проиллюстрировать на примере биопринтинга, поскольку данная технология связана с цифровизацией тела человека, созданием его цифровой трехмерной модели. Отчего необходимо законодательно определить эффективную модель деликтной ответственности за совершение посягательств на трехмерный цифровой образ человека [5].

Д. С. Маркевич считает, что для обеспечения определенности и предсказуемости правового регулирования на некоторые объекты в виртуальной среде может быть целесообразно перенесение режима, действующего в отношении других объектов правоотношений. В частности, игровые компании, как правило, рассматривают обеспечение доступа к игровому имуществу в качестве услуги в рамках организации игрового процесса. Это, в свою очередь, оказывает значительное влияние на круг прав и обязанностей субъектов данного вида правоотношений, механизмы и способы защиты прав и т. д. Объекты правоотношений в виртуальной среде отличает то, что они подчиняются, прежде всего, технологическим закономерностям оборота, а технические нормы могут включаться в программное обеспечение в качестве составной части объекта правоотношения. При этом в одних случаях технические правила существуют для обеспечения соответствующих правовых предписаний (например, системы Digital Rights Management), а в других – они направлены на изменение объема или содержания имеющихся прав, т. е. на установление нового регулирования. Данный феномен одновременно является и преимуществом, и угрозой для существующего правопорядка, так как, с одной стороны, при помощи технологий можно достичь более эффективного правоприменения, с другой стороны, такой подход может привести к снижению роли права и иных социальных регуляторов, деформации правосознания [16. С. 74–75].

В. В. Кресс указывает, что введение в структуру действующего законодательства цифровых прав не создает принципиально новой категории объектов гражданских прав. Уникальность цифровых прав то, что делает их именно качественным изменением законодательства, состоит в существовании и содержании прав на имущество и обязательств исключительно в рамках правил информационной системы, наряду с автоматическим характером их существования и возникновения [13. С. 75]. Соответственно, развитие цифровых технологий способствует расширению содержания правоотношений, нежели внедрения принципиально новых объектов.

Таким образом, можно констатировать, что развитие цифровых технологий расширяет возможные объекты правоотношений. Однако, многие устоявшиеся объекты правоотношений лишь видоизменяются под воздействием цифровых технологий. Но тем не менее нельзя отрицать вопросы правового регулирования таких новых объектов правоотношений, связанных с цифровыми технологиями, как: цифровой товар, персональные данные, big data, цифровой образ и иных объектов, возникших под влиянием цифровых технологий.

Появление новых и видоизменение старых объектов правоотношений всегда неотрывно связано с появлением новых субъектов права, которые будут вступать в правоотношения по поводу вышеназванных благ. Но какие же новые субъекты открылись взору юристов в связи с развитием цифровых технологий?

Следует изначально указать, что весьма важным вопросом является изучение цифровой дееспособности. Так, занимательно с научной точки зрения исследование А. К. Фетисова на тему цифровой дееспособности [22]. Представляется, что цифровая дееспособность – это разновидность реальной (обычной) дееспособности, которая реализуется посредством использования соответствующих технологий.

Однако, для создания условий, способствующих лицу полноценно реализовывать свою дееспособность в цифровой сфере, необходимо развитие соответствующего законодательства и правоприменительной практики.

Весьма актуальным вопросом на сегодняшний день является вопрос о правосубъектности искусственного интеллекта (далее – ИИ). Но что или кто конкретно такое ИИ? Э. М. Пройдаков определяет ИИ, как науку или технологию, включающую набор средств, позволяющих компьютеру на основании накопленных знаний представлять ответы на вопросы и формулировать на их основе экспертные заключения, т. е. получать знания, не вкладываемые в него разработчиками [20].

Возникает вполне логичный вопрос о том, кому будут принадлежать права на результаты, созданные с помощью либо самим ИИ? Ибо, на сегодняшний день ИИ может создать подобие произведения искусства, что автоматически ставит вопрос об авторском праве. Некоторые исследователи данной тематики выделяют следующих субъектов, которые могут быть потенциальными правообладателями:

- 1) разработчик программы по созданию ИИ;
- 2) собственник технических устройств, используемых для функционирования ИИ;
- 3) пользователь программы на основе ИИ;
- 4) непосредственно ИИ [24].

Г. П. Ивлиев и М. А. Егорова считают, что наиболее рациональным, но не бесспорным видится использование концепции правосубъектности ИИ по типу юридического лица либо электронного лица; подход к правовому регулированию в рамках юридической ответственности, связанной с пользователями, владельцами или производителями систем ИИ, а не с технологическими объектами. Применение механизма солидарной ответственности возможно при использовании несертифицированных систем ИИ, а также распределении ответственности при тестировании ИИ для решения конкретных задач, в случае если в ходе тестирования нанесен ущерб системой ИИ [11. С. 46].

А вот В. А. Лаптев считает иначе. Так, по его мнению, ИИ в киберфизическом пространстве в будущем будет приобретать правосубъектность и признаваться участником киберфизических отношений в цифровом пространстве даже с учетом того, что ИИ-система привязана к материальному носителю (вычислительному процессору) [15].

На наш взгляд, ИИ не обладает и не может обладать главными элементами любого здравомыслящего человека для того, чтобы быть субъектом правоотношения – сознанием и волей. Конечно, можно заявить о том, что юридическое лицо также не обладает такими признаками. Но ведь юридическое лицо действует не самостоятельно, а отталкивается от сознания и воли лиц ею руководящих. В то время как ИИ претендует по сущности своей на самостоятельность действий. Ввиду всего вышеперечисленного представляется разумным, что правообладателем на действия ИИ должен быть пользователь данной технологии, если иное не будет предусмотрено договором между пользователем и разработчиком или пользователем и собственником технического устройства, на котором функционирует ИИ. Аналогичная ситуация и с ответственностью за действия ИИ, за исключением тех случаев, когда они не охватывались умыслом лица, использующего технологию ИИ.

Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» содержит определение нового субъекта, ответственного за информационную систему. Таковыми является оператор информационной системы. Законодатель Республики Беларусь регламентирует, что оператор информационной системы – субъект информационных отношений, осуществляющий эксплуатацию информационной системы и (или) оказывающий посредством ее информационные услуги. А информационная система – это совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств [19]. Представляется, что понятие оператора информационной системы – это обобщенное, собирательное определение. Поэтому данный субъект содержит в себе всевозможное множество новых субъектов, связанных с использованием цифровых технологий.

Таким образом, можно говорить о том, что развитие цифровых технологий ставит перед законодателем и учеными вопрос о расширении списка субъектов права. Могут быть как принципиально новые, такие как ИИ, или видоизмененные старые, такие как оператор информационной системы. И иные явления, кроме нами названных, сегодня под вопросом об их правосубъектности. Но важен тот факт, что развитие цифровых технологий влияет на расширение списка субъектов возможных правоотношений.

Следующий вопрос – это влияние развития цифровых технологий на содержание правоотношений. Вполне очевидно, что вышеуказанное нами влияние на иные элементы правоотношения не может не затронуть и его содержание. Так, содержание правоотношения – это взаимосвязанная совокупность субъективных прав и обязанностей в конкретном правоотношении. Ключевыми элементами для нас являются – субъективные права и обязанности. Учитывая все вышеизложенное, разве можно говорить о том, что при существовании новых объектов и субъектов не закрепит законодатель соответствующих им прав и обязанностей? Конечно же, закрепит, ибо любой благодетельный законодатель стремится к упорядочиванию общественных отношений, а тем самым приведения их к гармонии. Но какие именно новые права и обязанности открылись в связи с развитием цифровых технологий?

Весьма интересно не только с теоретической, но и с практической точки зрения мнение О. А. Городова. Так, субъективные права и обязанности участников, составляющие содержание цифрового правоотношения, определяются не только характером конкретного правоотношения, возникающего между должником и кредитором, но и особенностями использования информационных технологий для целей замещения гражданского оборота тех либо иных материальных или нематериальных благ (активов). В системе распределенных реестров (блокчейн) оборот токенов юридически приравнен к обороту активов и осуществляется посредством использования еще одной технологии, заключающейся в способе ведения реестров, которая получила название смарт-контракта. Последний представляет собой компьютерную программу, которая имеет свой алгоритм, направленный на исполнение того либо иного гражданско-правового договора. В указанный алгоритм может быть заложена возможность определения сторонами порядка исполнения договора или

его расторжения. Содержание такого договора по причине переноса его исполнения в цифровую среду, по существу, не меняется, и его традиционно образуют права и обязанности сторон. Какие-либо дополнительные права или обязанностей вследствие использования технологии смарт-контракта у сторон не возникает [6. С. 9].

М. А. Липчанская исследовала новые цифровые права человека и гражданина. Так, она считает, что в настоящее время можно говорить о формировании нового института цифровых прав в науке конституционного права. Она формируются теми конституционными правами, которые либо появились вместе с внедрением современных цифровых технологий, либо приобрели существенно новое содержание. Отличительной особенностью этих прав является тот факт, что в настоящее время они все еще слабо формализованы и не имеют закрепления на конституционном уровне. Однако это должно произойти в ближайшем будущем. Таковыми новыми цифровыми правами она считает:

- 1) право каждого человека на доступ к Интернету;
- 2) право на общение;
- 3) право на защиту от машинной обработки информации [25].

На наш взгляд, развитие цифровых технологий, действительно, приносит новые цифровые права, которые должны быть закреплены на конституционном уровне.

Соответственно, содержание правоотношений, точно так же, как и остальные элементы, подвержено нововведениям ввиду развития цифровых технологий. Появляются новые цифровые права, которые вызывают вопрос об их конституционном закреплении, новые обязанности, которые гораздо эффективнее выполнить, используя цифровые технологии.

Следует обозначить значение цифровых технологий в совершении правонарушений. Так, в механизме совершения правонарушений цифровые технологии могут использоваться в различном качестве:

- 1) как средство совершения правонарушения;
- 2) как составной элемент способа правонарушения;
- 3) как предмет правонарушения.

Обращает на себя внимание то обстоятельство, что все перечисленные формы участия цифровых технологий в совершении правонарушения выступают в роли объективных признаков состава правонарушения [10. С. 256]. Ввиду всего вышесказанного можно констатировать, что развитие цифровых технологий охватывает не только цивилистическое, но и деликтное право.

Нельзя не указать и социальные последствия развития и использования цифровых технологий. Так, М. П. Барболин, мнение которого мы разделяем, утверждает, что цифровые технологии являются эффективным средством развития индивидуального и общественного интеллекта и тем самым повышения качества созидательной деятельности человека и общества, а в конечном итоге генетическим ядром инновационного развития индивидуального и общественного капитала [4. С. 124].

Подводя итог, можно с уверенностью сказать, что развитие цифровых технологий влияет на правоотношения, но оставляет ее структуру неизменной. Мы заключили, что цифровые технологии определяются использованием в них цифровой информации, которая в свою очередь состоит из цифровых сигналов. Цифровые же сигналы – это аналоговые сигналы, прошедшие дискретную обработку по времени,

а в последующем и квантование по уровню. Идея же цифровой информации в том, что она универсальна для использования в технике. Ибо цифровую информацию можно перевести практически в любую аналоговую информацию, которую способен воспринимать человек в отличие от цифровой. Тем самым, можно определить, что развитие цифровых технологий – это улучшение эффективности использования информации человеком.

Мы согласны с профессором Н. Н. Апостоловой о том, что цифровые технологии, включая ИИ, не должны являться инструментом сегрегации людей. Наоборот, благодаря их использованию люди должны получить возможность выйти на более высокий духовно-нравственный и интеллектуальный уровень своего развития [3. С. 133].

Развитие цифровых технологий ставит необходимые правовые вопросы о новых объектах и субъектах права, а соответственно, и о новом содержании правоотношений. На наш взгляд, наиболее остро для законодателей стоят вопросы, связанные с персональными данными, искусственным интеллектом, правами на образ, всеобщий доступ к Интернету и т. д. Учитывая быстрое развитие цифровых технологий, представляется разумным дальнейшее тесное и плодотворное сотрудничество законодателей и ученых всех областей науки.

Список литературы

1. Алексеева М. О., Пайдыганова М. Ю. Средства защиты цифровой и аналоговой информации // Аллея науки. 2019. Т. 1, № 8 (35). С. 322–325.
2. Алпатов Д. А. Классификация сигналов // Международный студенческий научный вестник. 2020. № 6. С. 32–40.
3. Апостолова Н. Н. Цифровое правосудие // Северо-Кавказский юридический вестник. 2022. № 1. С. 130–135.
4. Барболин М. П. К вопросу о возможностях цифровых технологий в развитии человека и общества // Человек и образование. 2018. № 1 (54). С. 121–124.
5. Богданов Д. Е. Технодетерминизм в частном праве: влияние биопринтинга на развитие концепции защиты права на цифровой образ // Вестник Пермского университета. Юридические науки. 2020. № 50. С. 678–704.
6. Городов О. А. Цифровое правоотношение: видовая принадлежность и содержание // Право и цифровая экономика. 2019. № 3 (05). С. 5–10.
7. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 17.09.2022).
8. Губенко А. В. Вопросы защиты персональных данных личности // Академический вестник Ростовского филиала Российской таможенной академии. 2020. № 4 (41). С. 49–53.
9. Гурьянова М. В., Аброскин А. С. Элементы обработки и преобразования аналоговых сигналов // Мировая наука. 2020. № 7 (40). С. 218–222.
10. Значение современных цифровых технологий в совершении преступления / С. А. Иванов [и др.] // Современный ученый. 2022. № 4. С. 255–260.
11. Ивлиев Г. П., Егорова М. А. Юридическая проблематика правового статуса искусственного интеллекта и продуктов, созданных системами искусственного интеллекта // Журнал российского права. 2022. № 6. С. 32–46.

12. Кабанов А. А., Чижов С. В. О структуре и содержании правоотношения // Ленинградский юридический журнал. 2015. № 4 (42). С. 19–29.
13. Кресс В. В. Цифровые права как объекты гражданских прав; правовое регулирование и перспективы развития в условиях цифровизации гражданского оборота // Журнал российского права. 2022. № 4. С. 67–76.
14. Кушниренко С. П. Цифровая информация как самостоятельный объект криминалистического исследования // Вестник криминалистики. 2006. № 2 (18). С. 43–47.
15. Лаптев В. А. Понятие искусственного интеллекта и юридическая ответственность за его работу // Право. Журнал Высшей школы экономики. 2019. № 2. С. 79–102.
16. Маркевич Д. С. Некоторые особенности объектов правоотношений в сфере цифровой экономики // Современная государственность и право: теоретические и практические проблемы формирования и успешного функционирования: материалы науч.-практ. конф., посвященной 75-летию со дня рождения заслуженного юриста Республики Беларусь доктора юридических наук, профессора А. М. Абрамовича, Минск, 24–25 мая 2019 г. Минск: Белорусский государственный университет, 2019. С. 73–76.
17. Нестеров А. В. О цифровых правах и объектах цифровых прав // Право и цифровая экономика. 2020. № 1 (07). С. 11–16.
18. О защите персональных данных: Закон Республики Беларусь от 07.05.2021 № 99-3 // ИПС «ЭТАЛОН-ONLINE». URL: <https://etalonline.by/document/?regnum=h12100099> (дата обращения: 17.09.2022).
19. Об информации, информатизации и защите информации: Закон Республики Беларусь от 10.11.2008 № 455-3 // ИПС «ЭТАЛОН-ONLINE». URL: https://etalonline.by/document/?regnum=h10800455&q_id=5860867 (дата обращения: 17.09.2022).
20. Пройдаков Э. М. Современное состояние исследований в области искусственного интеллекта // Цифровая экономика. 2018. № 3 (3). С. 50–63.
21. Ся Ч. Понятие и виды цифровых технологий // Актуальные научные исследования в современном мире. 2021. № 10 (78). С. 139–144.
22. Фетисов А. К. Цифровая дееспособность // Арбитражный и гражданский процесс. 2021. № 5. С. 3–7.
23. 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.
24. Abbott R. I Think, Therefore I Invent: Creative Computers and the Future of Patent Law // Boston College Law Review. 2016. Vol. 57.
25. Lipchanskaya, M. A. Digital rights of man and citizen: constitutional dimension // Gosudarstvennaya sluzhba. 2020. Vol. 22, № 4 (126). Pp. 37–41.
26. Matveev V. E. Analysis anonymity problems personal data on the Internet // Molodezh'. Obshchestvo. Sovremennaya nauka, tekhnika i innovatsii. 2019. № 18. Pp. 61–73.

Т. Р. Валиуллин,

студент,

Казанский (Приволжский) федеральный университет

С. Д. Мустафина,

студент,

Казанский (Приволжский) федеральный университет

ПРАВОВЫЕ ОГРАНИЧЕНИЯ ИСПОЛЬЗОВАНИЯ КРИПТОВАЛЮТЫ В СОВРЕМЕННУЮ ЭПОХУ

Аннотация. В статье ставится цель рассмотрение цифровых прав, цифровой валюты, понять, какие операции будут считаться осуществляемыми цифровыми правами, какую роль они играют при налоговых отчетах, каких полномочий у налоговых органов становится больше.

Ключевые слова: право, цифровые технологии, цифровые права, криптовалюта, юриспруденция

LEGAL RESTRICTIONS ON THE USE OF CRYPTOCURRENCIES IN THE DIGITAL AGE

Abstract. In this article, we would be able to analyze digital financial assets that are subject to digital rights verification. Consider digital currency. Understand what actions will be taken into account by pop-up digital rights, what role they play in tax reports.

Keywords: Law, Digital technologies, Digital rights, Cryptocurrency, Jurisprudence

1 января вступил в силу Федеральный закон о цифровых финансовых активах и цифровой валюте. Но в нем нет полной информации про криптовалюту.

Больше всего данный Закон посвящен цифровым финансовым активам. Эта некая возможность осуществлять права по эмиссионным ценным бумагам. В нем обозначены правила выпуска, учета и обращения ЦФА. Одним словом, когда приняли данный Закон № 259-ФЗ, необходимо сделать все возможное для активного использования технологий блокчейна для выпуска данных ЦФА. Некие инвестиции для данного проекта.

Давайте разберемся, что же понимается под криптовалютой. С одной стороны, она в нашем государстве разрешена. Во-первых, они могут являться средством платежа, если даже не являются денежной единицей РФ или другого государства. Во-вторых, про это пишется во многих законах: Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Федеральный закон от 26 октября 2002 г. № 127-ФЗ «О несостоятельности (банкротстве)», Федеральный закон от 2 октября 2007 г. № 229-ФЗ «Об исполнительном производстве», Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции». Где говорится, что цифровая валюта – это имущество.

С другой стороны, все требования, помимо правил и обращения, регулируются федеральными законами. Стоит отметить, что наше государство является лидером по цифровой валюте, также у наших граждан большое число криптокошельков.

Но использование такой валюты в какой-то степени имеет запреты. К ним относятся товары, услуги, работы, которые оказывают влияние на юридических лиц и граждан, которые находятся на территории нашего государства не менее 183 дней в течение 12 месяцев.

Действительно, с одной стороны, пользоваться цифровой валютой можно спокойно, в случае нарушения каких-либо прав – законодатель встает на сторону того лица, у которого нарушены права, но в данном случае необходимо помнить о том, что об этих действиях должен знать налоговый орган, об этом говорится в данном законе в ч. 6 ст. 14.

Данный порядок может быть введен уже в первом чтении по данному законопроекту.

Поэтому ФНС России должен будет иметь полномочия по порядку, когда сможет определить рыночную цену на цифровую валюту. В данном случае будет порог 600 тыс. руб.

Стоит отметить, что законодательством также предусмотрена ответственность за недостоверные сведения, в данном случае будет присужден штраф 10 % от суммы цифровой валюты. Также будет штраф, если будет не уплачен налог по переводам и действиям, где была использована цифровая валюта.

Поэтому необходимы многочисленные доработки до второго чтения по данному законопроекту. Для этого необходимо закрепить в ГК РФ понятие цифровой валюты – с возможностью ограничения ее гражданского оборота в соответствии с п. 2 ст. 129 кодекса – и соответствующим образом скорректировать ее определение в Законе № 259-ФЗ.

Можно сказать, что для целей налогообложения принимается цена товаров, работ или услуг, указанная сторонами сделки, – предполагается, что эта цена соответствует уровню рыночных цен.

Налоговые органы после всех данных нововведений спокойно могут запрашивать выписки по операциям на счетах физических лиц, а также в ситуациях, когда есть подозрения на правонарушения со стороны физических и юридических лиц.

Список литературы

1. Алексеев, Р. А. Апробация и перспективы применения технологии блокчейн на выборах за рубежом и в России / Р. А. Алексеев // Журнал политических исследований. 2018. № 3. URL: <http://znanium.com/catalog/product/1005721>
2. Бичева, Е. Е. Электронные деньги как новая форма современного рыночного хозяйства / Е. Е. Бичева, М. В. Пономаренко, А. Е. Пивоварова // Аллея Науки. 2018. № 5 (21). С. 1163–1170. URL: <https://elibrary.ru/item.asp?id=35233478>
3. Буряк, В. В. Deep Web / Dark Net: баланс между конфиденциальностью (individual privacy) и информационной безопасностью (cybersecurity) / В. В. Буряк // Наука через призму времени. 2018. № 10 (19). URL: <http://www.naupri.ru/journal/1245>
4. Варганова, М. Л. Перспективы цифровизации сельского хозяйства как приоритетного направления импортозамещения / М. Л. Варганова, Е. В. Дробот // Экономические отношения. 2018. Т. 8, № 1. С. 1–19. URL: <https://creativeconomy.ru/lib/38881>
5. Горда, А. С. Мировой рынок криптовалют: риски и механизмы регулирования / А. С. Горда // Научный вестник: финансы, банки, инвестиции. 2018. № 4. С. 96–104. URL: <https://elibrary.ru/item.asp?id=36645376>

Ю. И. Великохатко,

студент,

Ростовский государственный экономический университет

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ УГОЛОВНО-ПРАВОВЫХ ОТНОШЕНИЙ

Аннотация. В данной статье анализируются вопросы развития информационных технологий в уголовно-правовой сфере и их роль в уголовном судопроизводстве. Развивающиеся цифровые технологии при взаимодействии с уголовным правом имеют принципиальное значение для правоприменения, законотворчества и изучения уголовного права. Методологическую основу работы составляет система методов научного познания, среди которых следует выделить методы анализа, системности и сравнительно-правовой.

Ключевые слова: уголовное право, искусственный интеллект, сетевое взаимодействие, цифровые технологии, компьютерные преступления, уголовный процесс, электронные доказательства и судопроизводство

DIGITAL TECHNOLOGIES IN THE SYSTEM OF CRIMINAL LAW RELATIONS

Abstract. This article analyzes the issues of the development of information technologies in the criminal law sphere and their role in criminal proceedings. Developing digital technologies in interaction with criminal law are of fundamental importance for law enforcement, lawmaking and the study of criminal law. The methodological basis of this work is a system of methods of scientific cognition, among which the methods of analysis, consistency and comparative law should be highlighted.

Keywords: Criminal law, Artificial intelligence, Networking, Digital technologies, Computer crimes, Criminal proceedings, Electronic evidence and legal proceedings

С развитием Интернета, социальных сетей, банковской безопасности и государственной безопасности тема информации, а также нарушения информационных границ приобретает особое значение. Все же развитие информационных технологий, несомненно, является благоприятной тенденцией в развитии общества и может быть названо одним из основных направлений прогрессивного развития человечества. С другой стороны, возникает проблема регулирования новых общественных отношений, возникающих в связи с цифровизацией, и на первый план выходит вопрос защиты и безопасности ее субъектов.

В последнее время в научном сообществе появились работы монографического уровня, а также написаны множественные диссертационные исследования, касающиеся вопросов использования в уголовно-правовой сфере активно развивающихся цифровых технологий [1. С. 118].

Стоит отметить, что в банковской и финансовой среде введение инновационных инструментов и цифровых технологий, несомненно, открывает новые возможности как для граждан, делая удобным использование нововведений в банковской сфере, так и для хозяйственной деятельности и финансового рынка в целом [3. С. 11].

Информационные технологии в настоящее время проникают также в отдельные институты уголовного судопроизводства, в частности, стало возможно производить видео-конференц-связь в судебном заседании на различных станциях, подавать жалобы, заявления, ходатайства в электронном виде, производить изъятие электронных носителей для проведения уполномоченными лицами следственных действий. Но все-таки для современной реальности этого явно недостаточно. Изучив судопроизводство зарубежных стран, стоит отметить, что многие страны далеко продвинулись вперед в этом вопросе, а именно Великобритания (проведен виртуальный судебный процесс, все участники судебного процесса поддерживали связь через специально созданную закрытую сеть), Республика Казахстан (введена систему КУЗ и ЕРДР, которая позволила в электронном виде проводить регистрацию всех заявлений, а также сообщений о преступлении), Саудовская Аравия (переход на электронные уголовные дела больше 10 лет назад и тем самым существенное сокращение сроков расследования дела) и др. Каждому развитому государству, несомненно, требуется построить единую цифровую среду уголовного судопроизводства, которая включает в себя переход к сохранению записей и результатов процессуальных и следственных действий в электронном виде, построить налаженную систему документооборота между должностными лицами и государственными органами в уголовном судопроизводстве, предоставить возможность потерпевшему в онлайн-режиме отслеживать ход уголовного дела, широко применять дистанционные формы проведения процессуальных действий на каждой стадии уголовного судопроизводства, а также использовать электронного помощника судьи для фиксации фактических данных дела. Все это будет возможно в ближайшем будущем, ведь цифровые технологии не стоят на месте и уголовное судопроизводство подвергается существенным корректировкам.

В результате широкого внедрения цифровых технологий человеческий труд во многих областях постепенно заменяется хорошо функционирующими электронными комплексами и системами. Функции и обязанности работников максимально формализованы, запрограммированы и оцифрованы, тем самым цифровые технологии доказали свою эффективность и успешность во многих областях деятельности человека. Появление, например, компьютерного алгоритма для квалификации преступлений также представляется интересной разработкой, но ученые отзываются о ней двояко.

Стоит отметить, что уголовное право, защищая общественные отношения в сфере информации, выступает как основополагающая охранительная отрасль. Стоит упомянуть некоторые статьи, играющие принципиальное значение в сфере информационной безопасности:

– ст. 137 УК РФ – защищает права граждан в отношении конфиденциальности личной информации;

– согласно Уголовному кодексу РФ, непредоставление определенной информации компетентным органам может рассматриваться как преступление (ст. 306 – умышленно ложное обвинение (донос), ст. 307 – заведомо ложные показания, ст. 316 – сокрытие преступления и другие).

Помимо этого, цифровые технологии могут рассматриваться как средство или способ совершения преступления (например, ст. 159.3, 159.6 – мошенничество с использованием компьютерных технологий и с использованием электронных средств платежа – введены в действие с 2012 г.).

Изучив Стратегию развития информационного общества в Российской Федерации (2017–2030 гг.) [4], можно заметить, что запланировано комплексное развитие коммуникационной и информационной инфраструктуры в стране, обеспечивается поэтапный переход государственных органов к применению сервиса электронного правительства. Следует заметить, что меры, которые применяются правительством, получили активный отклик у граждан и широкое распространение, тем самым показывая готовность граждан взаимодействовать с государственными органами с помощью дистанционных технологий. Согласно статистическим данным, находящимся в открытых источниках, следует привести статистику, по которой за 2021 г. государственные услуги были предоставлены гражданам 150 млн раз [2].

Возможность проведения видео-конференц-связи существует уже достаточно давно, при рассмотрении уголовных, арбитражных и гражданских дел (с 1999 г.), а в 2018 г. вступил в силу закон, который позволяет использование видео-конференц-связи при рассмотрении судами дел об административных правонарушениях [5].

Правоохранительные органы также используют средства электронной коммуникации, но все же в основном для решения специальных управленческих задач. Здесь следует упомянуть о системе (ИСОД), которая позволяет ввести электронный документооборот в правоохранительную деятельность, осуществлять с помощью аппаратно-программных комплексов передачу необходимых данных для осуществления служебной деятельности.

В заключение хотелось бы отметить, что уголовно-правовая сфера видоизменяется под влиянием цифровых технологий. УК РФ дополняется отдельными статьями, новыми составами преступлений, тем самым регулируя и защищая вновь возникшие правовые отношения. Внедрение искусственного интеллекта в уголовное судопроизводство все еще выступает предметом на ученых исследований ученых-правоведов. Появление компьютерного алгоритма, помогающего при квалификации преступления, с одной стороны, конечно, облегчает работу правоприменителей, но с другой – будет ли решение, вынесенное искусственным интеллектом, отвечать требованиям справедливости, гуманизма и законности?

Список литературы

1. Зуев С. В. Цифровая среда уголовного судопроизводства: проблемы и перспективы Сибирский юридический вестник. 2018. № 4 (83). С. 118–124.
2. Итоги работы Единого портала госуслуг в 2021 году // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. URL: <http://government.ru/department/387/events/O>
3. Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С. Цифровая криминология. Москва: Академия управления МВД России, 2021. 224 с.

4. Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Российской Федерации от 09.05.2017 № 203 // Гарант.ру: информационно-правовой портал. URL: [http:// www.garant.ru](http://www.garant.ru)

5. Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» от 12.11.2018 № 410-ФЗ // Российская газета. 2018. 14 ноября.

И. Д. Викторов,
магистрант,
Московский государственный
юридический университет имени О. Е. Кутафина

ЦИФРОВЫЕ ПЛАТФОРМЫ: ПРОБЛЕМЫ АНТИМОНОПОЛЬНОГО РЕГУЛИРОВАНИЯ И МЕРЫ ПО ИХ УСТРАНЕНИЮ

Аннотация. Цель: проанализировать нормы действующего законодательства о защите конкуренции, с помощью которых можно бороться с доминированием цифровых платформ, предложить способы его модернизации. Предмет: антиконкурентная практика цифровых платформ, предложения по его изменению. Методология исследования заключается в критическом анализе разумности вносимых изменений пятым антимонопольным пакетом. Результаты: установлено, что внедряются новые высокотехнологичные способы злоупотребления цифровыми платформами своим доминирующим положением, что приводит к развитию цифровой монополии. Попытки законодателя усилить ответственность влекут развитие новых форм недобросовестной конкуренции. Для борьбы с антиконкурентной практикой цифровых платформ предлагается ввести систему оценки компаний по различным параметрам на основе технологии больших данных, направленных на стимулирование развития технологий, а не на подавление конкуренции.

Ключевые слова: изменение антимонопольного законодательства, цифровые платформы, маркетплейсы, пятый антимонопольный пакет, защита конкуренции онлайн-платформ, большие данные

DIGITAL PLATFORMS: ANTITRUST PROBLEMS AND MEASURES TO ADDRESS THEM

Abstract. Objective: To analyse the current competition law provisions that can be used to fight the dominance of digital platforms and to propose ways to modernise it. Subject: anti-competitive practices of digital platforms and proposals for its amendment. The methodology of the research consists in the critical analysis of the reasonableness of the changes introduced by the Fifth Antimonopoly Package. Results. It was found that new high-tech ways for digital platforms to abuse their dominant position are being introduced, leading to the development of a digital monopoly. Attempts of the legislator to increase liability entail the development of new forms of unfair competition. In order to combat the anti-competitive practices of digital platforms, it is proposed to introduce

a system of evaluation of companies according to various parameters based on big data technology, aimed at stimulating technology development rather than suppressing competition.

Keywords: Antitrust law changes, Digital platforms, Marketplaces, Fifth antitrust package, Competition protection for online platforms, Big data.

Развитие современного ландшафта цифровой экономики характеризуется взрывным ростом актуальности цифровых сервисов, в частности цифровых платформ и рынка электронной коммерции. Однако вместе с развитием лидеров национального рынка обостряется и необходимость выбора надлежащей модели по его регулированию. 2021 г. связан с активным обсуждением ряда законопроектов, направленных на регулирование данной сферы. Был опубликован проект «Концепции общего регулирования деятельности групп компаний, развивающих различные цифровые сервисы на базе одной «экосистемы» [8], разработанный Минэкономразвития.

Необходимо признать, что Российский рынок в целом никогда не был однородным и справедливым, предприниматели обладают различными ресурсами и возможностями для его развития. Но коронавирусная инфекция только усилила разрыв между аналоговым и цифровым рынком.

По результатам аналитического исследования агентства INFOline, совокупный доход крупнейших ретейлеров за 2021 г. вырос на 22,3 % до 16,4 млн руб. [5].

Повсеместное развитие цифровой экономики привело к необходимости трансформации бизнеса в цифровую среду, актуальность маркетплейсов, агрегаторов, цифровых платформ, возросла как никогда. Использование модели онлайн-продаж стало единственной возможностью для выживания традиционной модели бизнеса. Поэтому высокотехнологичные компании только укрепили свои позиции, ограничив доступ на рынок конкурентов.

Между тем использование алгоритмов в созданных бизнес моделях также может служить инструментом для сговора, как в горизонтальных, так и в вертикальных соглашениях. Выбор использования цифрового алгоритма в качестве механизма для увеличения прибыли позволяет избежать ответственности, предусмотренной законодательством, поскольку на сегодняшний день у антимонопольных органов нет никакого опыта по его регулированию. Устаревшие методы по пресечению нарушений не достаточно эффективны в фиксации нарушений при использовании сложных и гибких механизмов: отсутствует необходимость длительных переговоров и при этом почти полностью исключается человеческий фактор. Максимизация прибыли достигается за счет ущерба конечных потребителей.

При этом в современных условиях найти доказательств по установлению картельного сговора и так затруднительно, поскольку позиция антимонопольного органа основывается, в большинстве своем, на совокупности косвенных доказательств. Рассмотрим реальный кейс применения антимонопольного законодательства из сложившейся практики. В одном из решений управления федеральной антимонопольной службы по городу Москве факт договоренностей между субъектами был установлен судом с помощью одного и того же адреса при подаче заявок:

«Использование разными хозяйствующими субъектами единой инфраструктуры и совместная подготовка заявок на аукцион возможны только в случае кооперации

и консолидации для достижения ими единой цели. Подобное возможно только вследствие достигнутых договоренностей, поскольку коммерческие организации, преследуя цель извлечения прибыли, конкурируют между собой, а не действуют в интересах друг друга [9]. Поэтому выявление картельного сговора представляет собой комплексную процедуру, требующую детализированного анализа множества фактов и доказательств.

При этом необходимо констатировать, что если с регулированием деятельности традиционных компаний уже имеются устоявшиеся методы и практика по их регулированию, то в отношении цифровых платформ нет никакого единого понимания. Однако компании столкнутся с реальными прецедентами, вынуждающих продавцов участвовать в акциях, проводимых маркетплейсами. В качестве санкции установлена ответственность в виде дополнительной комиссии для продавцов, отказывающихся принять в них участие [7].

Так происходит формирование новой рыночной власти, которая навязывает свои условия на рынке и дискриминирует другие компании. В условиях отсутствия опыта и сложности доказывания данных категорий дел, формирование методов и способов по пресечению подобных нарушений для антимонопольного органа видится сложной задачей.

А. В. Бычков и Д. В. Шрам в связи с этим пишут: «Сформировавшие новую экономическую реальность технологические компании превратились в IT-гигантов (Big Tech), степень экономической концентрации которых настолько велика, что они конкурируют лишь между собой, что позволяет говорить о такой преобладающей форме конкуренции, как олигополия, а в ряде случаев, как, например, в ситуации с магазинами приложений Apple и Google, – и о дуополии» [1. С. 78–92].

Проблема обостряется затруднением доступа для выхода новых участников рынка, в том числе стартапов. Они в большинстве случаев лишены финансовых возможностей для создания нового продукта, что создает уникальные условия по сравнению с традиционным аналоговым рынком.

Применяемые технологии позволяют существенно оптимизировать транзакционные и иные операционные расходы, что оказывает положительный эффект на конечном потребителе. При этом потребитель оказывается так же уязвим, поскольку при предоставлении своих данных получает возможности по контролю потребительского поведения со стороны экосистем. Концентрация персональных данных в базах цифровых платформ и их чрезмерное использование приводит к развитию новых форм недобросовестной конкуренции.

Имеющийся огромный потенциал возможностей собственникам платформ позволяет выйти на международный рынок, но при этом сохраняются риски по усилению монополии. Не контролируемое развитие онлайн-платформ приводит к сбоям в рыночной системе, повышаются требования к необходимости оперативного реагирования со стороны государства. Как пишет О. В. Жевняков: доминирующие цифровые платформы захватывают смежные рынки путем создания новых бизнесов, успешность которых они проверяют, используя информацию о клиентах платформы и их транзакции (т. е. через недобросовестную конкурентную практику). Захват происходит и через приобретение смежных бизнесов [3. С. 3].

В сентябре 2022 г. в ответ на вызовы и размытость правового статуса цифровых платформ в Государственную Думу был внесен пятый антимонопольный законопроект, затрагивающий регулирование «цифровых» рынков [6].

При выборе указанной модели регулирования Федеральный Антимонопольный орган избрал путь до цифровой эпохи, в данном случае изменяются только критерии: с территориального на количественный. Логика в установлении доминирующего положения в зависимости от трафика посещения конкретной онлайн-платформы. Понятие цифровой платформы, указанное в законе также имеет неоднозначное толкование, под его определение могут подпадать различные агрегаторы, сайты страховых компаний и другие смежные сервисы. Двойственность интерпретационного понимания цифровых платформ вводимого пакета поправок приведет к избыточному регулированию, возрастет количество антимонопольных споров.

Основной проблемой сохранившегося законодательства является отсутствие детализации форм проявления недобросовестной конкуренции, использование старых категорий применительно к новым технологиям видится не лучшим решением. В долгосрочной перспективе это может привести к подрыву экономики Российской Федерации, поскольку не будет единообразного понимания, как у контролирующих органов, так и у бизнеса. Любые маркетинговые и стратегические задачи по развитию могут рассматриваться в качестве акта недобросовестной конкуренции.

На информационном рынке сейчас происходит неопределенность, с одной стороны, власти страны не хотят допустить монополизацию рынка цифровых экосистем, но с другой стороны, сдерживание их развития не позволит обеспечить сохранность цифрового суверенитета Российской Федерации. Отсутствие единого понимания цифровой монополии только осложняет сохранение цифрового роста страны, что требует рационального обсуждения. Поэтому для восполнения пробела предлагается добавить в федеральный антимонопольный закон следующее определение, цифровая монополия – это состояние рынка информационных товаров или услуг, на котором создание конкурентной среды становится не возможным, ввиду влияния одного лица, группы лиц или государства на весь рынок в целом. Законодательное закрепление понятия цифровой монополии является необходимым шагом в обеспечении здоровой конкуренции.

При этом нельзя не согласиться с R. W. Crandal, что более важным для нынешних дебатов по поводу использования антимонопольного законодательства для ограничения власти гигантских цифровых компаний является не вопрос о квалификации антиконкурентного поведения и введении его запрета, а о том, какие эффективные средства государство может использовать для борьбы с новыми монополистами, простое запрещение антиконкурентных практик может не повлиять на монопольную власть [11. С. 627–649].

Антимонопольная практика складывается таким образом, что происходит лоббирование интересов корпораций, дискредитируются мелкие цифровые компании и конкуренция. Цифровое и информационное неравенство приводит к разрушению демократического режима правления, процветанию цифрового капитализма. Поскольку вред монополии очевиден, то при чрезмерной защите корпораций от антимонопольного вмешательства и равномерного развития конкурентоспособного рынка цифровых технологий может привести к его стагнации.

Основной объем нарушений со стороны цифровых платформ все так же подпадает под категории недобросовестной конкуренцией или злоупотреблением доминирующим положением, однако борьба вокруг этих нарушений должна выстраиваться с учетом специфики и особенностей их работы в условиях цифровой экономики. Усиление административной ответственности, установление отягощающих обстоятельств, увеличение сумм штрафов только приводит к возникновению необоснованных расходов и подавлению информационной конкурентоспособности страны.

Неверно выбранная стратегическая политика антимонопольных органов и бездумное форсированная разработка массива законодательной базы для регулирования новых информационных отношений без учета их специфики, ограничивает разумное состояние конкуренции, вредит наращиванию цифрового потенциала компаний. Е. В. Холодная пишет, что «технологический прогресс опережает действующие в этой сфере правовые регуляторы» [10. С. 1], а по мнению А. В. Минбалеева перспективным направлением является трансформация права в «новые сложноорганизованные юридико-технические механизмы регуляции уже не общественных отношений, а отношений, обусловленных программно-инженерным программированием функционирования системы искусственного интеллекта» [4. С. 2]. Поэтому невозможно построить экономику страны будущего, используя слабо адаптированные и консервативные методы регулирования правоотношений.

В случае недобросовестного поведения онлайн-платформ сегодня применяется система наказания, когда нарушение права уже состоялась и антимонопольный орган работает только с последствиями такого нарушения. В то же время мы не можем никак не регулировать деятельность цифровых платформ, это может привести к их доминированию.

Технологии больших данных, искусственного интеллекта, используемые в высокотехнологичных компаниях заточены для максимального извлечения прибыли, а не для развития технологий. Ссылаясь на удобство и функциональную необходимость внедрения программных продуктов, компании изобретают все более технологичные способы антиконкурентных манипуляций. Такой подход посягает на свободу рыночной экономики, устраняет процесс развития технологий.

М. А. Егорова поддерживает точку зрения, что в России необходимо подготовить законодательные предложения, которые будут направлены на предупреждение монополизации товарных рынков в сфере цифровых технологий [2. С. 7–10]. Поэтому для реального предотвращения нездорового рыночного поведения целесообразным представляется применение ряда превентивных мер.

Предлагается ввести систему оценки по различным параметрам компаний, имеющих доминирующее положение на цифровом рынке онлайн-платформ. Использование технологии больших данных для анализа добросовестности поведения информационных компаний позволит использовать поощрение в качестве механизма стимулирования и пресекать применение цифровых технологий в антиконкурентных целях. В рамках реализации системы компании с высоким рейтингом будут пользоваться большим количеством льгот и привилегий, в то время как использование алгоритмов в обход закона должно служить основанием для понижения рейтинга и установления дополнительных ограничений и проверок в отношении их деятельности со стороны надзорных органов.

В подобной ситуации акты злоупотребления доминирующим положением и недобросовестной конкуренции будут невыгодны для цифровых корпораций, что выведет их деятельность в правовое поле. Это важный момент для построения гармоничного и демократического устройства нашей страны, руководство компаний будет направлять свои силы на совершенствование и стимулирования технологий и прогресса, а не только на коммерческие ценности.

В тоже время по борьбе с монополистами эффективным способом является развитие программного обеспечения по автоматизированному выявлению картелей и других антиконкурентных действий, например, «большой цифровой кот». Развитие цифровых технологий и сервисов в Федеральной антимонопольной службе позволит на основе технологии больших данных и машинного обучения выявлять картели и формировать доказательственную базу. В данном случае исключается человеческий фактор и коррупционная составляющая, поэтому дальнейшее развитие данных сервисов позволит быстро и эффективно пресекать нарушения антимонопольного законодательства.

Таким образом, социальный спрос на цифровые онлайн сервисы и цифровые продукты растет с каждым днем, рынок электронной коммерции неустанно расширяется в масштабах. При рассмотрении пятого антимонопольного пакета органами государственной власти достигнуты определенные успехи, но сохраняются риски по монополизации рынка. Введение в закон понятий сетевых эффектов и ценовых алгоритмов частично ограничивают их монопольную власть, но не решают системных проблем.

Наша страна находится на этапе стратегических возможностей ускорить внедрение собственных методов развития, происходят глубокие организационные изменения. Уровень правосознания руководства цифровых компаний остается на низком уровне, их деятельность направлена на поиск решений по созданию альтернативного программного обеспечения, формально соответствующее букве закона, но не его духу.

Поэтому внедрение прозрачной системы оценки деятельности информационных компаний на основе технологии больших данных является важной предпосылкой для развития цифрового потенциала нашей страны. Перестройка методов работы цифровых сервисов и онлайн платформ, укрепление социальной искренности, стимулирование взаимного доверия является насущным требованием для разрешения социальных противоречий, укрепления и обновления управленческих методов, построения гармоничного общества.

Список литературы

1. Бычков А. В., Шрам Д. В. Проблемы правоприменительной практики антимонопольного регулирования на цифровых рынках как показатель необходимости реформирования законодательства о защите конкуренции // Пролог: журнал о праве. 2021. № 2. С. 78–92.
2. Егорова М. А. Особенности нормативного регулирования цифровой экономики и проблемы антимонопольного регулирования на цифровых рынках как средство защиты национальных интересов // Юрист. 2018. № 11. С. 7–10.
3. Жевняк О. В. Антиконкурентная практика цифровых платформ и меры реагирования по российскому и зарубежному законодательству // Право и политика. 2021. № 5 (205). С. 14–41. URL: https://nbpublish.com/library_read_article.php?id=33888 (дата обращения: 17.09.2022).

4. Минбалеев А. В. Трансформация регулирования цифровых отношений // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 12 (64). С. 31–36.
5. Маркетплейсы рвутся вверх: за счет чего выросли обороты крупнейших ретейлеров России. URL: <https://www.forbes.ru/biznes/467927-marketplejisy-rvutsa-vverh-za-schet-sego-vyrosli-обороты-krupnejsih-retejlerov-rossii> (дата обращения: 17.09.2022).
6. О внесении проекта Федерального закона «О внесении изменений в Федеральный закон «О защите конкуренции» от 07.07.2022 № 7759п-П13 // СПС Консультант Плюс.
7. Продавцы пожаловались в ФАС на политику маркетплейсов. URL: <https://www.kommersant.ru/doc/5424588> (дата обращения: 17.09.2022).
8. Проект «Концепции общего регулирования деятельности групп компаний, развивающих различные цифровые сервисы на базе одной «экосистемы»// СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_387363/ (дата обращения: 17.09.2022).
9. Решение Московского УФАС России от 13.02.2020 по делу № 077/01/11–12363/201 // СПС «КонсультантПлюс». URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=RGSS&n=65640#mQfunHTac4Opbwx7> (дата обращения: 17.09.2022).
10. Холодная Е. В. Правовые механизмы преодоления административных барьеров в сфере цифровых экспериментальных инноваций // Право цифровой среды: монография / под ред. Т. П. Подшивалова, Е. В. Титовой, Е. А. Громовой. Москва: Проспект, 2022. С. 276–279.
11. Crandall R. W. The Dubious Antitrust Argument for Breaking Up the Internet Giants // Review of industrial organization. 2019. № 54 (4). С. 627–649. URL: <https://link.springer.com/article/10.1007/s11151-019-09680-y> (дата обращения: 17.09.2022).

А. А. Виноградова,
студент,

Казанский инновационный университет имени В. Г. Тимирязова

Л. Р. Хайрутдинова,
старший преподаватель,

Казанский инновационный университет имени В. Г. Тимирязова

КИБЕРВИКТИМНОСТЬ ЖЕРТВ КИБЕРСТАЛКИНГА

Аннотация. Отсутствие общепринятого определения киберсталкинга, законодательного закрепления нормы и ответственности привело к тому, что цифровые технологии дали возможность преследовать или запугивать интернет-пользователей различными способами, не неся за это наказания. Представляется необходимым научно определить киберсталкинг (киберпреследование) и его законодательное закрепление. В настоящее время количество жертв киберсталкинга возрастает, это связано с рядом факторов и причин кибервиктимности, хотя законодательство ряда стран уже содержит нормы об уголовной ответственности за киберсталкинг, чего нет в Уголовном кодексе РФ.

Ключевые слова: виктимность, виктимизация, жертва, информационные технологии, кибервиктимность, киберсталкинг, киберпреследование, преступление

CYBERVICTIMITY OF CYBERSTALKING PEOPLE

Abstract. The lack of a generally accepted definition of cyberstalking, legislative consolidation of responsibility has led to the fact that digital technologies make it possible to intimidate people in various ways. It is necessary to give the concept of cyberstalking and fix it in law. Currently, the number of victims of cyberstalking is increasing, this is due to the causes of cybervictimization. The legislation of countries already contains provisions on criminal liability for cyberstalking, which is not in the Criminal Code of the Russian Federation.

Keywords: victimization, victimization, victim, information technology, cybervictimization, cyberstalking, crime

Открытое цифровое пространство предоставляет возможности для социального взаимодействия во всех сферах и направлениях. С каждым годом государство, общество развивается, используя информационно-коммуникационные технологии. С одной стороны Интернет – это уникальные возможности в доступности получения образования, личностного развития, ведение бизнеса, поиска нужной информации и развлечений, а с другой стороны Интернет – это место, способ совершения преступлений.

Исследований вопросов, причин киберпреступлений и их жертв в России немного, но при этом такие проблемы поднимаются в научной среде и имеют на сегодняшний день особую актуальность.

Согласимся с утверждением Д. В. Жмурова о том, что между современной и старой преступностью существует не только антагонизм, но и существенная разница в методах воздействия на потерпевших, так как сейчас используются незнакомые ранее приемы, принципиально новые подходы к поиску, отбору и контакту с потенциальными жертвами.

Постоянное развитие компьютерных технологий и все большее их внедрение во все сферы жизни человека, несомненно, способствует росту киберпреступлений, а соответственно недостаточная разработанность действующего уголовного законодательства РФ приводит к высокому показателю латентности. Следовательно, к киберпреследованию следует относиться так же серьезно, как и к тем преступлениям, указанным в УК РФ.

Одним из ряда негативных последствий является киберсталкинг, определяемый как форма преследования, домогательства, сопровождающиеся систематическими угрозами, травлей через СМС, форумы, чаты, социальные сети, т. е. при котором используются электронные инструменты и виртуальная среда для контроля, манипулирования и принуждения жертвы к чему-либо. Киберсталкинг (киберпреследование – это поведение пользователей (это отдельные лица, группы или организации), которые используют информационные технологии для преследования одного или нескольких человек в своих интересах, но с возможными последствиями для жертв. Жертвами киберсталкинга становятся не только знаменитые люди, но и обычные граждане.

В качестве преследователей чаще всего выступают люди, страдающие от неразделенной любви, бывшие мужья или жены, желающие отомстить, подрост-

ки, издевающиеся над одноклассниками. Причем большинство преследователей психически нормальны и действуют по строго продуманному плану. Многие киберсталкеры даже объединяются в группы, которые учат друг друга преследовать жертву и нанести ей наибольший вред.

Что происходит, это использование социальных сетей и других виртуальных групп для сбора информации о жертве, частая отправка нежелательных сообщений, рассылка вирусов или взлом учетных записей, выдача себя за кого-то другого, размещение ложной информации о себе, что заставляет других пользователей доверять или верить этому человеку.

Киберпреследование или киберзапугивание может привести к психологическим (например, депрессивным симптомам, нарушениям сна), финансовым и социальным последствиям для жертв киберсталкинга.

Факторы влияющие на виктимность жертв киберсталкинга:

- 1) социально-демографические признаки: пол, возраст и семейное положение;
- 2) профессиональная деятельность или учеба;
- 3) вовлеченность в социальные сети;
- 4) потерпевшие от преступлений;
- 5) отсутствие документов, гражданства.

Виды кибервиктимизации могут быть следующие: троллинг, оскорбление, унижение, харассмент, социальное игнорирование, обращение внимания на свою личность и т. д.

Само поведение киберпреследователя не обязательно должно быть преступным, и что возможно виртуальный преследователь не преследует цель причинить именно вред жертве. Но в какой степени такое поведение будет социально приемлемо или каков порог между приемлемым и преступным поведением?

Исходя из этого, возникающие вопросы указывают на необходимость дополнительных исследований, посвященных киберпреследованию, определению, какой вред или ущерб может нанести конкретный субъект, и формирование механизма виктимологической защищенности лиц подвергшихся киберсталкингу.

Список литературы

1. Жертв интернет-преследований защитит закон: что такое киберсталкинг? // URL: https://informatio.ru/news/society/zhertv_internet_presledovaniy_zashchitit_zakon/
2. Жмуров Д. В. Кибервиктимность как новая категория виктимологии постмодерна // Азиатско-Тихоокеанский регион: экономика, политика, право. 2021. № 2. URL: <https://cyberleninka.ru/article/n/kiberviktimnost-kak-novaya-kategoriya-viktimologii-postmoderna> (дата обращения: 15.09.2022).
3. Кабанов П. А. Современная криминологическая виктимология: тенденции и некоторые перспективные направления развития // Виктимология. 2017. № 3 (13). URL: <https://cyberleninka.ru/article/n/sovremennaya-kriminologicheskaya-viktimologiya-tendentsii-i-nekotorye-perspektivnye-napravleniya-razvitiya> (дата обращения: 15.09.2022).
4. Сафуанов Ф. С., Докучаева Н. В. Особенности личности жертв противоправных посягательств в Интернете // Психология и право. 2015. Т. 5, № 4. С. 80–93.
5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

А. Ю. Виноградова,
студент,

Казанский инновационный университет имени В. Г. Тимирязова

АКТУАЛЬНЫЕ ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЦИФРОВОГО ПРОФИЛЯ

Аннотация. В статье рассматриваются основные подходы к пониманию дефиниции цифрового профиля в законодательных нормах, а также в положениях научной литературы. Сделан вывод, что цифровой профиль – это совокупность официальных, актуальных и подтвержденных данных о физическом или юридическом лице, содержащиеся в государственных информационных системах, информационных системах муниципальных органов и организаций, которые используются для качественного и эффективного предоставления государственных, муниципальных и иных услуг. Проводится анализ инфраструктуры цифрового профиля и его правового регулирования в рамках использования в сфере государственного управления и финансовых услуг.

Ключевые слова: цифровой профиль, профилирование, персональные данные, цифровая экономика, идентификация, аутентификация, социальное ранжирование, цифровые технологии, цифровая трансформация

CURRENT FEATURES OF THE LEGAL REGULATION OF THE DIGITAL PROFILE

Abstract. In the article, the author examines the main approaches to understanding the definition of a digital profile in legislative norms, as well as in the provisions of scientific literature. The author comes to the conclusion that a digital profile is a set of official, up-to-date and confirmed data about an individual or legal entity contained in state information systems, information systems of municipal bodies and organizations that are used for high-quality and effective provision of state, municipal and other services. The analysis of the infrastructure of the digital profile and its legal regulation in the framework of use in the field of public administration and financial services is carried out.

Keywords: Digital profile, Profiling, Personal data, Digital economy, Identification, Autism, Social ranking, Digital technologies, Digital transformation

В современном мире все чаще цифровые технологии встраиваются в общественные отношения, затрагивая все сферы общества. Помимо системы государственного управления, цифровая трансформация также не обошла стороной финансовую сферу, систему здравоохранения, страхования и т. д.

Стоит отметить, что на данный момент не сложилось единое понятие цифрового профиля как на законодательном уровне, так и в научной литературе.

Так, определение цифрового профиля было дано в отклоненном законопроекте № 747513–7, согласно которому цифровой профиль представляет собой «совокупность сведений о гражданах и юридических лицах, содержащихся в информационных системах государственных органов, органов местного самоуправления и организаций, осуществляющих в соответствии с федеральными законами

отдельные публичные полномочия, а также в единой системе идентификации и аутентификации» [7].

Также имеется несколько иная трактовка от органов исполнительной власти в «Сценарии использования инфраструктуры Цифрового профиля. Версия 1.14», которая определяет цифровой профиль как «совокупность цифровых записей о гражданине, содержащихся в информационных системах государственных органов и организаций» [8].

Переходя к изучению научных определений, автор обращает внимание на позицию А. К. Жаровой, согласно которой, цифровой профиль представляет собой многоуровневую сложную систему, которая формируется за счет проанализированных данных, берущих свое начало в информационных системах, а также в информационно-телекоммуникационных сетях [1. С. 61].

В свою очередь, А. М. Кондаков и А. А. Костылева придерживаются позиции, что «цифровой профиль – это информационный электронный носитель, в котором будут храниться все данные о гражданине», с целью обеспечить доступ через портал государственных услуг к данным о лице, содержащимся в других государственных информационных системах [2. С. 212].

В целом, исходя из данных определений, мы можем сделать вывод, что цифровой профиль представляет собой совокупность официальных, актуальных и подтвержденных данных о гражданине или юридическом лице, содержащиеся в ГИС, ИС муниципальных органов и организаций, осуществляющих публичные функции, а также в информационно-телекоммуникационных сетях, и используемые для качественного и эффективного предоставления государственных, муниципальных и иных услуг.

Стоит отметить, что, несмотря на то, что упомянутый законопроект был отклонен, в РФ была создана инфраструктура цифрового профиля граждан в рамках эксперимента, проводимого на основании постановления Правительства № 710 [5].

Согласно данному Постановлению цифровой профиль на данный момент включает в себя около 38 видов сведений о гражданине, начиная с ФИО, пола, даты рождения, заканчивая сведениями о доходах по форме 2-НДФЛ, сведениями из электронной трудовой книжки, деловой репутации и т. д. Как мы можем заметить, цифровой профиль включает в себя полный спектр сведений о гражданине, затрагивающий не только основные данные, но в целом все сведения о жизнедеятельности гражданина.

Исходя из методических рекомендаций Минцифры РФ, сбор, хранение и обмен указанными сведениями о гражданине будут осуществляться с помощью Единой системы идентификации и аутентификации (ЕСИА), в качестве которой уже выступает Портал государственных услуг, а также посредством системы межведомственного электронного взаимодействия (СМЭВ) [8]. В 2021 г. Минцифры также разработали методические рекомендации по использованию ЕСИА в рамках реализации инфраструктуры цифрового профиля [3].

В рамках реализации предоставленных полномочий государственные органы уже обладают самостоятельными цифровыми профилями граждан. Так, ФССП имеет базу данных относительно наличия задолженностей и исполнительного производства у граждан. МВД также имеет ИС ТОР, в которой находятся объективные данные на гражданина.

Обратим внимание, что помимо государственных органов (МВД, ПФР, ФССП и т. д.) в качестве участников проводимого эксперимента выступают кредитные, страховые, микрофинансовые организации, операторы финансовых платформ. В частности, согласно письму Банка России № 35-3-3-2/213 к августу 2020 г. к инфраструктуре цифрового профиля уже подключились 11 банков, 8 банков находились на стадии подключения [4]. Отсюда можно сделать вывод, что наиболее активное использование цифрового профиля, помимо государственных структур, подразумевается именно в финансовой, в частности, в банковской сфере.

В декабре 2021 г. Банк России представил Проект Основных направлений цифровизации финансового рынка на период 2022–2024 гг. [6], в котором особое внимание было уделено развитию и регулированию инфраструктуры цифрового профиля. В данном же проекте указывается, что с окончанием эксперимента планируется принятие упомянутого законопроекта, который законодательно определит и закрепит правовой статус Цифрового профиля гражданина, а также создаст необходимую законодательную базу для последующего формирования цифрового профиля юридического лица.

Согласно Проекту, предполагается расширение организаций, имеющих доступ к цифровым профилям. К уже имеющимся участникам присоединятся страховые организации, негосударственные пенсионные фонды, профессиональные участники рынка ценных бумаг, управляющие компаниями, бюро кредитных историй, Агентство по страхованию вкладов, а также операторы связи. Таким образом, будет значительно расширен круг сведений о гражданине, например, данными о его финансовой состоятельности, здоровье и т. д.

Помимо указанных сведений цифровой профиль предполагается расширить путем сбора биометрических данных граждан в банках и МФЦ в Единой биометрической системе (ЕБС) (в планах также самостоятельная регистрация в защищенном мобильном приложении в рамках эксперимента). Предполагается, что с помощью биометрических данных клиент сможет без личного присутствия получить финансовые услуги в банках, пройдя удаленную идентификацию на сайте или в мобильном приложении с помощью ЕБС. Также с помощью биометрических данных возможна будет и аутентификация, например, отмена или подтверждение сомнительных операций. На данный момент конкретный список собираемых биометрических данных не указан, однако уже сейчас в некоторых банках (например, ПАО «Сбербанк») используются биометрические данные, а именно изображение лица и запись голоса, для осуществления ряда финансовых услуг, например, для получения кредита.

На наш взгляд, ЕБС также будет активно и эффективно использоваться в различных государственных структурах. Так, в рамках СК РФ сократиться объем выполняемой работы и значительно ускорится процесс расследования, а именно органы предварительного следствия смогут получать в кратчайшие сроки необходимую следствию информацию в отношении подозреваемого, обвиняемого или свидетелей.

Данная система также будет весьма эффективна при проведении выборов. В виду того, что на данный момент предусмотренная электронная форма голо-

сования, использование биометрических данных (изображение лица) позволит идентифицировать личность избирателя.

В связи с большим объемом преступлений, совершаемых в финансовой сфере, планируется также создание соответствующих систем для проверки граждан и юридических лиц на предмет криминогенности. Так, в случае физических лиц будет создана Единая информационная система проверки сведений об абоненте (ЕИС ПСА), благодаря которой появится возможность проверки принадлежности номера телефона у оператора связи к конкретному лицу, а также определения степени риска соответствующего клиента на основе характера, объема и параметров совершаемых им операций. Данная система также позволит осуществлять обмен данными между различными финансовыми организациями, коллекторами, Банком России, ФСБ, Росфинмониторингом и Минцифры России. В рамках юридических лиц и ИП планируется создание сервиса «Знай своего клиента», с помощью которого клиенты также будут соотнесены к различным группам риска, исходя из совершаемых ими финансовых операций. Несомненно, данные системы позволят предотвратить значительное количество преступлений, совершаемых в финансовой сфере еще на ранних этапах. Однако, это также представляет собой определенную форму социального ранжирования клиентов по различным уровням риска. Исходя из того, к какой группе относится клиент (низкий уровень риска, высокий уровень риска и т. д.), будет доступен или ограничен определенный круг предоставляемых финансовых услуг, например, ограничение в совершении сомнительных операциях.

Однако, несмотря на все перечисленные плюсы цифрового профилирования, имеется также ряд важных и острых проблем, требующих значительного внимания.

Во-первых, встает вопрос относительно безопасности и защиты столь обширного объема имеющихся сведений о гражданах, использование которых осуществляется не только государственными органами, но и рядом коммерческих организаций, в связи с чем также остро встает вопрос относительно социального инжиниринга.

Также, несмотря на то, что при формировании цифрового профиля, в частности, в финансовой сфере, предусмотрена система согласий, при которой обмен данными может осуществляться только при наличии соответствующего согласия от клиента, которое может быть отозвано в любой момент, возникают риски, связанные с соблюдением конституционных прав и вмешательством в частную жизнь граждан.

Тем не менее цифровое профилирование является достаточно перспективной отраслью общественно-правовой деятельности, которая должна служить государственно-общественным интересам.

Список литературы

1. Жарова А. К. Вопросы обеспечения безопасности цифрового профиля человека // Юрист. 2020. № 3. С. 55–61.
2. Кондаков А. М., Костылева А. А. Цифровая идентичность, цифровая самоидентификация, цифровой профиль: постановка проблемы // Вестник РУДН. Серия: Информатизация образования. 2019. № 3. С. 207–218.

3. Методические рекомендации по использованию Единой системы идентификации и аутентификации. Версия 3.0: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации от 18.08.2021. URL: <https://digital.gov.ru/ru/documents/6186/> (дата обращения: 08.08.2022).

4. Письмо Банка России от 31.09.2020 № 35-3-3-2/213 «О получении сведений ФНС России» // СПС «Гарант». URL: <https://www.garant.ru/products/ipo/prime/doc/74512452/> (дата обращения: 10.09.2022).

5. Постановление Правительства РФ от 03.06.2019 № 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» // Собрание законодательства Российской Федерации. 10 июня 2019 г. № 23. Ст. 2963.

6. Проект Основных направлений цифровизации финансового рынка на период 2022–2024 гг.: Разработан Банком России от 10.12.2021. URL: https://www.cbr.ru/Content/Document/File/131360/oncfr_2022-2024.pdf (дата обращения: 09.09.2022).

7. Проект Федерального закона № 7475513-7 «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)». URL: <https://sozd.duma.gov.ru/bill/747513-7> (дата обращения: 09.09.2022).

8. Сценарии использования инфраструктуры Цифрового профиля. Версия 1.14: Методические рекомендации Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 29.12.2021. URL: <https://digital.gov.ru/ru/documents/7554/> (дата обращения: 08.09.2022).

И. С. Вишняков,
магистрант,

Институт законодательства и сравнительного правоведения
при Правительстве Российской Федерации

ЗАКОНОДАТЕЛЬНЫЕ ПРЕДЛОЖЕНИЯ США В СФЕРЕ РЕГУЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ЦИФРОВЫХ ПЛАТФОРМ

Аннотация. Столкнувшись с трудностями в формировании судебных прецедентов, ограничивающих рыночную власть платформ в рамках текущих законов, американскими законодателями был предложен ряд новых законов, направленных на создание равных и справедливых условий на цифровых рынках и на обеспечение защиты данных пользователей платформ. В статье анализируются текущие законопроекты, внесенные в Конгресс США и направленные на правовое регулирование деятельности цифровых платформ.

Ключевые слова: цифровые платформы, цифровая экономика, антимонопольное законодательство.

US LEGISLATIVE PROPOSALS IN THE FIELD OF REGULATION OF DIGITAL PLATFORMS

Abstract. Faced with difficulties in forming judicial precedents that limit the market power of platforms within the framework of current laws, American legislators

have proposed a number of new laws aimed at creating equal and fair conditions in digital markets and ensuring the protection of platform users' data. The article analyzes the current bills submitted to the US Congress and aimed at the legal regulation of digital platforms.

Keywords: Digital platforms, Digital economy, Antimonopoly legislation.

Распространение цифровых технологий влечет все более глубокие изменения во всех сферах общественной жизни, и особенно в сфере экономики, что требует инноваций и в сфере права, а именно – разработки адекватных мер правового обеспечения цифровой экономики. Развитие цифровой экономики становится приоритетным направлением для многих стран, и от успехов в этом направлении зависит конкурентоспособность отечественных фирм и государства в целом как на внутреннем рынке, так и на мировом.

С возникновением цифровой экономики возникла специфическая для этого хозяйственного уклада бизнес-модель – онлайн-платформы или цифровые платформы. Ключевым фактором производства в цифровой экономике являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг. Наиболее важной для новой бизнес-модели цифровых платформ является способность извлекать и контролировать огромное количество данных.

Начало «эры платформ» принято отсчитывать от 2008 года, когда был основан сервис Airbnb [6. Р. 94]. Возникшую на основании новых цифровых технологий экономическую модель называют по-разному: гигэномика, шеринговая экономика, экономика «по требованию», экономика тотального надзора, экономика мобильных приложений, экономика впечатлений и внимания, экономика доступа, сетевая экономика и т.д. [6. Р. 89; 15. С. 36].

Главный ресурс, которым оперируют платформы – данные. Английский математик и предприниматель Клайв Хамби называл данные «новой нефтью» [16]. Н. Срничек выражает эту особенность следующим образом: «Развитый капитализм двадцать первого столетия постепенно выстроился вокруг задачи извлечения и использования особого типа сырья – данных» [15. С. 37]. Данные как ресурс использовались и в «доплатформенных» бизнес-моделях, однако в гораздо меньших масштабах и только в вопросах, касающихся организации и координации производственных и логистических процессов. Возникновение и развитие новейших цифровых технологий открыло возможности сбора и регистрации огромных новых массивов данных, на основании чего «выросли новые отрасли, занятые их извлечением и использованием для оптимизации производственных процессов, детального анализа потребительских предпочтений, контролирования работников, понимания востребованных характеристик для разработки новых продуктов и услуг» [15. С. 39].

В связи с ключевым значением данных в деятельности платформ, противодействие антиконкурентным практикам платформ становится проблемой не толь-

ко антимонопольного законодательства, но также и законодательства в информационной сфере и в сфере персональных данных. В Федеративной Республике Германия антимонопольное ведомство возбудило дело в отношении Facebook (социальная сеть, которая в России признана экстремистской и запрещена), так как компания включила в пользовательское соглашение несправедливые условия обработки данных.

Одним из флагманов в сфере законодательных предложений по регулированию деятельности цифровых платформ являются Соединенные Штаты Америки. В США широкое обсуждение антимонопольного регулирования цифровых рынков началось после публикации доклада Комитета Стиглера по цифровым платформам [7] в сентябре 2019 года. В докладе констатировались недостатки американских антимонопольных законов и рекомендовалось создать Цифровое управление (Digital Authority), задачей которого должно стать создание общих благоприятных условий конкуренции на цифровых рынках.

В июне 2019 года юридический комитет Палаты представителей начал расследование по вопросам состояния конкуренции на цифровых рынках. 29 июля 2020 года главы Google, Apple, Facebook и Amazon были приглашены на слушания в Конгресс США, проводимые юридическим подкомитетом по антимонопольной политике. Глава подкомитета Дэвид Сисиллин указывал, что эти компании объединяет схожее поведение на рынке – они являются «узким горлышком» («bottleneck») в основных каналах дистрибуции, и за счет этого имеют возможность извлекать данные пользователей [1]. Amazon был обвинен в злоупотреблении своей ролью в качестве ритейлера и одновременно держателя платформы для иных продавцов. Apple обвинили в несправедливом использовании магазина приложений App Store для блокирования своих конкурентов и принуждения разработчиков к выплате высокой комиссии. Конкуренты Facebook уличили его в монопольном положении на рынке социальных сетей. Материнская компания Google – Alphabet – сталкивается с значительным количеством обвинений в нарушении антимонопольного законодательства в связи с доминирующим положением на рынке цифровой рекламы, поисковых систем и программного обеспечения для смартфонов. Кульминацией расследования стал выпущенный в октябре 2020 года отчет Палаты представителей, в котором выражалась серьезная озабоченность состоянием конкуренции, указывалось, что Amazon, Apple, Facebook и Google получили контроль над ключевыми каналами дистрибуции и функционируют как привратники. В качестве ответа на сложившуюся ситуацию на цифровом рынке авторы отчета рекомендовали широкий набор законодательных реформ.

Внесению законопроектов предшествовала большая судебная кампания против американских технологических гигантов. Начало «антимонопольному крестовому походу» против цифровых платформ положили иски Epic Games против Apple [4] и Google [3]. Иски стали развитием конфликта между Epic Games, как разработчиком, и Apple и Google, как владельцами магазинов приложений, из-за высоких (по мнению Epic Games) 30-процентных сборов с транзакций внутри приложений.

Вскоре после этого цифровыми платформами заинтересовались антимонопольные органы США. Федеральная торговая комиссия подала иск против Facebook, в ко-

тором пыталась доказать монопольное положение компании на рынке «услуг межличностного сетевого взаимодействия». Окружной суд округа Колумбия отказал в удовлетворении требований антимонопольного органа в связи с тем, что истцу не удалось обосновать расчет рыночной доли Facebook [2]. Комментируя решение суда, член Палаты представителей Конгресса США Кен Бак заявил, что решение «показывает крайнюю необходимость в реформе антимонопольного законодательства» [5].

7 июля 2021 года прокуроры 36 штатов США и столичного округа Колумбия подали коллективный иск к Google в связи с нарушениями антимонопольного законодательства, указывая, что Google контролирует 90% рынка приложений для Android [10].

Следуя рекомендациям отчета, американские законодатели представили в июне 2021 года серию законопроектов о регулировании цифровых рынков, а именно: 1) Закон «Об американском выборе и онлайн-инновациях» (Bill H. R. 3816 – The American Choice and Innovation Online Act) [11], нацеленный на запрет использования дискриминационных практик большими онлайн-платформами; 2) Закон «Об искоренении монополии платформ» (Bill H. R. 3825 – The Ending Platform Monopolies Act) [12], нацеленный на разрешение конфликтов интересов, с которыми сталкиваются определенные операторы онлайн-платформ; 3) Закон «Об улучшении совместимости и конкуренции через внедрение переключения между сервисами» (Bill H. R. 3849 – The Augmenting Compatibility and Competition by Enabling Service Switching Act, the ACCESS Act) [14], нацеленный на развитие конкуренции через снижение входных барьеров и издержек на смену сервисов для пользователей и предпринимателей.

Ключевым для всех трех законопроектов является понятие «охватывающей платформы» (covered platform). Данный статус присваивается платформам Федеральной торговой комиссией или Министерством юстиции. Платформе может быть присвоен статус «охватывающей», если она соответствует определенному количественному критерию: 1) имеет не менее 50 миллионов пользователей в США или не менее 100 тысяч пользователей-предпринимателей и 2) ей владеет или ее контролирует лицо с размером чистой годовой выручки или размером рыночной капитализации не менее 600 миллиардов долларов США. Помимо соответствия количественному критерию, фирма должна быть «критическим торговым партнером» в сфере продажи или предоставления товара или услуги, предлагаемых на платформе или напрямую связанных с ней. В зависимости от законопроекта, на лицо, управляющее платформой, налагаются определенные обязанности:

– The American Choice and Innovation Online Act запрещает лицу, управляющему платформой, «неправомерное дискриминационное поведение», а также ряд других дискриминационных практик. К таким практикам законопроект относит: создание преимуществ для собственных товаров и услуг платформы по сравнению с товарами и услугами других лиц, пользующихся платформой; вмешательство в установление цен на товары и услуги лиц, пользующихся платформой; непредоставление пользователям платформы допуска к данным, собираемым на основании их действий на платформе.

Платформа может избежать ответственности, если докажет, что ее поведение было безвредным для потребителей и для конкурентных отношений.

Законопроектом также предложено учредить Бюро цифровых рынков в составе Федеральной торговой комиссии, которая будет уполномочена контролировать соблюдение положений закона.

– The Ending Platform Monopolies Act направлен на недопущение возможности для операторов платформ владения коммерческой организацией, наличия контроля или выгоды в бизнесе, который использует платформу для продажи или предоставления товаров и услуг, если это может повлечь конфликт интересов. Аналогично предыдущему законопроекту, требования данного акта нацелены на недопущение приоритизации собственных товаров и услуг владельца платформы по сравнению с товарами и услугами пользователей.

– The Access Act налагает различные обязанности в вопросах переносимости и совместимости данных. В отличие от предыдущих проектов, предназначенных для обеспечения равных и справедливых условий пользования платформой, The Access Act направлен на защиту данных пользователей платформы и обеспечения безопасного переноса данных с одной платформы на другую.

В августе 2021 года американские законодатели внесли дополнительный законопроект, нацеленный именно на магазины приложений – Закон «Об общедоступных рынках приложений» (Bill H. R. 5017 – The Open App Markets Act) [13]. Предназначенный для «развития конкуренции и сокращения власти привратников в экономике приложений», закон применяется к лицу, владеющему или контролирующему магазин приложений, число пользователей которого составляет не менее 50 миллионов в США.

The Open Markets Act налагает ряд обязанностей на операторов магазинов приложений, включая:

– запрет принуждения к использованию внутренней платежной системы платформы под условием размещения приложения в магазине (такой запрет уже установлен законодательством Республики Корея [8]);

– запрет требовать от лиц, размещающих приложения в магазине, установления равных или более низких цен по сравнению с другими магазинами приложений;

– обязанность не вмешиваться в коммуникации разработчиков с пользователями;

Оператор магазина приложений не подлежит привлечению к ответственности за действия, которые 1) необходимы для обеспечения конфиденциальности данных пользователей или цифровой безопасности; 2) были предприняты для предотвращения спама или мошенничества; или 3) были предприняты для предотвращения нарушения (или в целях обеспечения соблюдения) федерального законодательства или законодательства штата. Надзор за исполнением Закона возлагается на Федеральную торговую комиссию, Генерального прокурора США и генеральных прокуроров штатов.

Вывод. Правовое регулирование деятельности цифровых платформ в США находится на стадии формирования. Столкнувшись с трудностями в формировании судебных прецедентов, ограничивающих рыночную власть платформ в рамках текущих законов, американскими законодателями был предложен ряд новых законов, направленных на создание равных и справедливых условий на цифровых рынках и на обеспечение защиты данных пользователей платформ.

Список литературы

1. Apple, Google и Facebook допросили об «уничтожении конкурентов». Главное // «РБК» от 30.07.2020. URL: https://www.rbc.ru/technology_and_media/30/07/2020/5f21f8e59a79470797bd8904. [дата обращения: 10.09.2022]
2. Case No. 1:20-cv-03589-JEB. State of New York, et al., v. Facebook, Inc. URL: https://ag.ny.gov/sites/default/files/state_of_new_york_et_al._v._facebook_inc._-_filed_public_complaint_12.11.2020.pdf [дата обращения: 10.09.2022]
3. Case No. 3:20-cv-05671. Epic Games, Inc., v. Google LLC. URL: <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3299&context=historical> [дата обращения: 10.09.2022]
4. Case No. 4:20-cv-05640-YGR. Epic Games, Inc., v. Apple Inc. URL: <https://www.cand.uscourts.gov/wp-content/uploads/cases-of-interest/epic-games-v-apple/Epic-Games-20-cv-05640-YGR-Dkt-410-Apple-Proposed-Findings-of-Facts-and-Conclusions-of-Law.pdf> [дата обращения: 10.09.2022]
5. Federal court tosses antitrust suits against Facebook, in huge blow to D.C.'s fight with tech // Politico, 28.06.2021. URL: <https://www.politico.com/news/2021/06/28/federal-court-dismisses-ftcs-antitrust-case-against-facebook-496764> [дата обращения: 10.09.2022]
6. Lobel O. The Law of the Platform // Minnesota Law Review, 2016, San Diego Legal Studies Paper No. 16-212. URL: <https://ssrn.com/abstract=2742380> [дата обращения: 10.09.2022]
7. Stigler Committee on Digital Platforms: Final Report // The University of Chicago Booth School of Business Official Website. URL: <https://www.chicagobooth.edu/research/stigler/news-and-media/committee-on-digital-platforms-final-report> [дата обращения: 10.09.2022]
8. Telecommunications Business Act // Korea Legislation Research Institute URL: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=59855&lang=ENG [дата обращения: 10.09.2022]
9. US Congress official website (Электронный ресурс) / URL: <https://www.congress.gov> [дата обращения: 10.09.2022]
10. Больше половины американских штатов подали в суд на Google // «РБК» от 08.07.2021. URL: https://www.rbc.ru/technology_and_media/08/07/2021/60e666689a7947c6e84d3889. [дата обращения: 10.09.2022]
11. Закон «Об американском выборе и онлайн-инновациях» (Bill H. R. 3816 – The American Choice and Innovation Online Act) // US Congress official website. URL: <https://www.congress.gov/bill/117th-congress/house-bill/3816/text> [дата обращения: 10.09.2022]
12. Закон «Об искоренении монополии платформ» (Bill H. R. 3825 – The Ending Platform Monopolies Act) // US Congress official website. URL: <https://www.congress.gov/bill/117th-congress/house-bill/3825/text> [дата обращения: 10.09.2022]
13. Закон «Об общедоступных рынках приложений» (Bill H. R. 5017 – The Open App Markets Act) // US Congress official website. URL: <https://www.congress.gov/bill/117th-congress/house-bill/3816/text> [дата обращения: 10.09.2022]
14. Закон «Об улучшении совместимости и конкуренции через внедрение переключения между сервисами» (Bill H. R. 3849 – The Augmenting Compatibility

and Competition by Enabling Service Switching Act, the Access Act) // US Congress official website. URL: <https://www.congress.gov/bill/117th-congress/house-bill/3849/text> [дата обращения: 10.09.2022]

15. Срничек Н. Капитализм платформ [Текст] / пер. с англ. и науч. ред. М. Добряковой; Нац. исслед. ун-т «Высшая школа экономики». – 2-е изд. – М.: Изд. дом Высшей школы экономики, 2020. – 128 с.

16. Цифровой взгляд в скважину // «Коммерсантъ» от 18.12.2020. URL: <https://www.kommersant.ru/doc/4616681>. [дата обращения: 10.09.2022]

В. Д. Гаврилова,
студент,

Волгоградский государственный университет

ВНЕДРЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМУ ПРАВОВОГО РЕГУЛИРОВАНИЯ: АНАЛИЗ ОТЕЧЕСТВЕННОГО И ЗАРУБЕЖНОГО ОПЫТА

Аннотация. В статье рассматривается внедрение системы искусственного интеллекта в принятие решений, вытекающих из различных общественных отношений, особое внимание уделено оценке предполагаемого и реального участия данной системы в выполнении публичных функций: осуществление правосудия, рассмотрение обращений граждан и т. д. Утверждается, что при внедрении искусственного интеллекта в различные сферы необходимо руководствоваться тем, что именно человек должен принимать конечные решения, поскольку он обладает сознанием и совестью и способен дать оценку, основанную на традиционных ценностях, вместе с тем новые технологии должны играть исключительно инструментальную роль. Методом моделирования выявлены вероятные недостатки использования искусственного интеллекта в правоприменении. Затрагиваются вопросы оформления системы регулирования соответствующих отношений, «отраслевого» подхода и выбора формы единого правового документа. Рассмотрен положительный опыт РФ по внедрению соответствующих технологий в сферу здравоохранения при достаточном контроле человека, затронут вопрос об экспериментально-правовых режимах в РФ.

Ключевые слова: искусственный интеллект, правовое регулирование, публичные функции, правоприменение, доказательства, судопроизводство, суд, фундаментальная ошибка

IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE INTO THE SYSTEM OF LEGAL REGULATION: ANALYSIS OF DOMESTIC AND FOREIGN EXPERIENCE

Abstract. The article is devoted to the implementation of an AI into decision-making, special attention is paid to the assessment of the intended and real participation of this system in the public functions: justice, consideration of appeals. The author thinks that the implementation of AI in various spheres requires person to make final decisions, because he has consciousness and is able to give an assessment based on traditional

values, and new technologies should play an instrumental role. The modeling revealed possible disadvantages of using AI in proceedings. The author also refers to the criminal case, which shows that it is necessary to approach AI solutions carefully. The author explores the “branches” approach in the execution of the system and chooses a single legal document. The positive experience of the RF in healthcare with sufficient human control is considered, the question of experimental legal regimes in the RF is raised.

Keywords: Artificial intelligence, Legal regulation, Public functions, Law enforcement, Evidence, Legal proceedings, Court, Fundamental error

Введение. Цифровизация сопровождается развитием цифровых технологий и использованием системы искусственного интеллекта (далее – AI) в различных сферах. Технологии AI отличаются непредсказуемым характером и недостаточной изученностью последствий, что требует соблюдать осторожность при внедрении и использовании данных механизмов. В юридической и философской литературе наблюдаются разные прогнозы относительно развития AI: как упрощение и улучшение жизни при сохранении контроля со стороны человека, так и стирание границ между человеческим и виртуальным миром, наделение AI способностью мыслить и даже управлять определенными аспектами общественных отношений.

Очевидно, что стирание границ между миром человека и миром AI не является желательным, поскольку это может привести к нивелированию значения человека как субъекта, который обладает сознанием, способностью к мыслительной деятельности и к оценке, основанной на таких традиционных ценностях, как жизнь, права и свободы человека и гражданина, гуманизм, справедливость.

Данные риски обуславливают необходимость тщательной правовой регламентации использования системы AI. На мой взгляд, необходимо внедрить эту систему так, чтобы минимизировать соответствующие риски и защитить традиционные ценности. Только таким образом данные технологии будут целостно и гармонично интегрированы в систему правового регулирования.

Цель исследования – рассмотреть процесс внедрения AI в систему правового регулирования и проанализировать отечественный и зарубежный опыт.

Для достижения выбранной цели поставлены следующие задачи: 1) рассмотреть подходы и теории к изучению и пониманию AI; 2) показать вероятные недостатки использования системы AI в правоприменении, используя метод моделирования; 3) найти пример юридического дела из зарубежной практики, в решении которого была допущена фундаментальная ошибка ввиду доверия человека решению AI; 4) изучить подходы к оформлению правового регулирования отношений по использованию AI при принятии решений, вытекающих из различных общественных отношений; 5) сделать выбор в пользу соответствующей формы закрепления и обосновать его; 6) рассмотреть отечественный опыт внедрения AI.

В статье используются формально-юридический, сравнительно-правовой, методы анализа и синтеза, моделирование.

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

Основная часть. Вопросы взаимодействия человека с технологиями AI и функционирования данной системы в целом сопряжены с комплексом правовых и этических проблем, что раскрывается в Национальной стратегии развития искусственного интеллекта на период до 2030 г. (далее – Стратегия), утвержденной Указом Президента Российской Федерации от 10.10.2019 № 490 [5].

В п. 49 Стратегии упоминаются направления, позволяющие сформировать систему регулирования общественных отношений, возникающих в связи с развитием и внедрением технологий AI. Взят курс по преобразованию правовой реальности в соответствии с потребностями развивающегося информационного общества с использованием правовых форм, методов и цифровых решений [2. С. 18]

Одно из них – регламентация процедур упрощенного тестирования AI и делегирование данной системе возможности принимать отдельные решения в сфере публичной власти, кроме тех, что могут ущемлять права и законные интересы граждан.

Данное направление представляется достаточно спорным ввиду сущности AI и значимости публичных функций. На мой взгляд, при внедрении AI в процессы принятия решений по вопросам, вытекающим из различных общественных отношений, необходимо руководствоваться тем, что конечное решение должно оставаться за человеком как за субъектом, способным дать оценку, основанную на традиционных ценностях, и учесть те факторы, которые мог не принять во внимание AI.

Прежде чем затрагивать факторы, которыми обусловлена данная позиция и перейти к практическим аспектам работы, необходимо разобраться в подходах к пониманию проблемы внедрения AI в процессы принятия соответствующих решений. Это позволит понять, почему исследователи и законодатель на данный момент не нашли однозначного решения данной проблемы.

Так, можно рассматривать данный процесс с точки зрения следующих подходов: футуристического и реалистического [10].

Представители футуристического подхода изучают AI, делая акцент именно на перспективы развития данной системы, и большинство из них соглашается с теорией сильного AI, предполагая, что данный механизм можно запрограммировать так, чтобы он мыслил, как человек.

Представители реалистического подхода изучают AI, основываясь на той информации, которая есть на данном этапе, и чаще всего придерживаются теории слабого AI, ограничивая возможности этого механизма лишь воспроизведением отдельных положений и отвергая его способности к когнитивной деятельности.

Разумеется, допустимо изучать рассматриваемое явление с точки зрения как футуристического, так и реалистического подхода, поскольку это позволит раскрыть проблему со всех сторон. При этом, на мой взгляд, следует согласиться с представителями теории слабого AI, а также учитывать риски использования данной системы. Так, данный механизм не является и не будет достойной альтернативой человеку, необходимо ограничить его использование инструментальной ролью. Соглашаясь на нечто большее, человек допускает возникновение огромных рисков и их реализацию, что может иметь много негативных последствий.

Итак, ранее была обозначена позиция автора о том, что при использовании AI в принятии решений, особенно в юридической сфере и в сфере реализации

публичных функций, конечное решение должно оставаться за человеком. Такой подход обусловлен следующими факторами.

Во-первых, сущность человека и его способность дать оценку, основанную на традиционных ценностях, и учесть те факторы, которые мог не принять во внимание AI. Одним из наиболее ярких примеров является предусмотренная процессуальными законами оценка доказательств по внутреннему убеждению, что является неотъемлемой составляющей процесса доказывания и принятия решения по юридическому делу. Закреплено, что доказательства не имеют для суда заранее установленной силы и что суду необходимо оценивать их по определенным критериям.

Так, ставится вопрос о возможности осуществления AI такой деятельности. Разумеется, в силу уникальности каждого человека, его сознания и мировоззрения в оценке доказательств может присутствовать доля субъективности. И, на первый взгляд, это исключается при оценке доказательств AI, поскольку в данном случае преобладает рациональность, логические и математические расчеты. Однако проблема возникает в связи с тем, что: а) при принятии решений AI не руководствуется такой этической категорией, как совесть. У данной системы отсутствует нравственное самосознание, говорить об оценке на основании внутреннего убеждения в таком случае невозможно; б) при составлении команд определяются последовательность и направление шагов AI в рамках осуществления данной деятельности. Так, в подобных условиях доказательства вполне могут иметь заранее установленную силу, что противоречит свободе оценки доказательств и демонстрирует, что даже при «рациональном подходе» AI субъективность не исключается.

Обратим внимание на то, что в судебной практике зарубежных стран уже известны случаи использования AI, о которых справедливо говорить в качестве посягающих на традиционные ценности и не соответствующих закону. Приведем дело Эрика Лумиса, который стал жертвой предвзятости программы для оценки рисков COMPAS [6]. Исходя из сущности функционирования программы, понимаем, что она установила высокие риски ввиду преобладания статистических данных, согласно которым принимаются во внимание пол и расовая принадлежность подсудимого. Подобная дискриминация незаконна и несопоставима с такими традиционными ценностями, как справедливость, гуманизм, права и свободы человека.

Данное резонансное дело демонстрирует, что результаты работы AI, с которыми человек безотлагательно согласился, привели к допущению фундаментальных ошибок при осуществлении правосудия – публичной функции, которую осуществляет соответствующий орган публичной власти – суд. Подобные ошибки неприемлемы и недопустимы, и для того чтобы избежать их человек должен относиться к работе AI с осторожностью. В любом случае, судье необходимо самостоятельно изучить дело, далее решить, принять во внимание результаты функционирования AI или не согласиться с ними, и только после этого выносить соответствующий судебный акт.

Обратим внимание, что в правоприменении с использованием AI может возникнуть ситуация, когда данный механизм оценил большинство фактических обстоятельств верно и в целом сопоставил их друг с другом, однако не принял во внимание отдельные смягчающие или отягчающие обстоятельства, которые влияют на назначение наказания. Например, AI может не принять во внимание, что

отдельные аспекты в поведении потерпевшего можно считать аморальными до такой степени, что они стали поводом для преступления. При этом подобная аморальность со стороны потерпевшего, согласно п. «з» ч. 1 ст. 61 УК РФ, признается смягчающим наказанием обстоятельством.

Моделируя ситуации в рамках концепции цифрового правоприменения, отметим, что AI может недостаточно подробно рассмотреть фактические обстоятельства дела для установления оценочных признаков, достаточно часто фигурирующих в системе уголовного закона: например, существенное нарушение прав и законных интересов объектов уголовно-правовой охраны. малозначительность деяния.

Следует согласиться с Гарри Сурденом, отметившим, что AI достигает успеха в направлениях правовой деятельности, связанных с чисто механическими или повторяющимися действиями, но не с абстракцией и концептуализацией [9. С. 1331].

Развивая данный тезис, отметим, что можно говорить и о таких аспектах, как форма и содержание. Затронем процесс рассмотрения обращений граждан. Так, можно использовать цифровые технологии с целью ускорения обработки обращений и реагирования на них. При составлении ответа могут использоваться шаблонные фразы, однако каждое обращение должно быть рассмотрено тщательно, поскольку каждая ситуация индивидуальна, следовательно, решения проблем так или иначе будут отличаться друг от друга. Получается, цифровые технологии могут помочь в «форме», но само «содержание» должно формироваться с учетом особенностей дела и проверяться человеком. В подобных процедурах мы используем AI именно как инструмент.

На мой взгляд, фактором, обуславливающим принятие конечного решения человеком и инструментальную роль AI, является и наличие несовершенств в структуре системы. Например, буквальное понимание команд, сопряженное с крайностями. Достаточно вспомнить тестирование беспилотного автомобиля в США, результатом которого стало то, что механизм причинил смерть переходившей дорогу женщине. Условием данного несчастного случая стал заданный механизму режим: при распознавании объектов чувствительность к «опасным» снижалась во избежание ошибочных реакций [3]. Оценка данной ситуации неоднозначна. С одной стороны, этот режим допустил человек, он проявил легкомыслие или вовсе небрежность, что стоило жизни другому человеку. С другой стороны, данная ситуация показывает опасность для человеческой жизни как фундаментальной ценности буквального понимания роботом команд. Отсутствуют гарантии, что даже при максимально уточненном и выверенном комплексе команд беспилотный автомобиль справится со сложным участком дороги.

Из вышеперечисленного очевидно, что при регламентации применения AI должен быть установлен четкий порядок, основанный на этических стандартах: «новые цифровые ценности» должны имплементироваться в современное общество в той мере, в какой они не вытесняют охраняемые правом традиционные человеческие ценности [1. С. 625].

Вместе с тем представляется интересным и вопрос оформления системы соответствующего законодательства. По этой проблеме подробно высказывался профессор Джеймс Демпси. Он считает оптимальным поручить руководителям отдельных сфер, в которых будет применяться система AI, принять положения, ре-

гламентирующие применение системы AI. По мнению Демпси, отраслевой подход при регулировании соответствующих процессов будет наиболее эффективным, нежели принятие единого закона [8. С. 14]. Реализация данной идеи позволит в рамках конкретной сферы предусмотреть регулирование конкретных ситуаций без бланкетных норм. Вместе с тем остается нерешенным вопрос об общих принципах регулирования применения AI как наборе минимальных стандартов, соблюдение которых позволит минимизировать установление противоречащего традиционным ценностям и закону порядка применения AI в конкретной сфере. Можно повторять данные принципы в разных документах, однако представляется оптимальным перечислить и раскрыть их в едином документе. Более того, регулирование отношений, связанных с применением AI в различных сферах, с учетом научно-технического прогресса и динамики общественного развития в целом имеет огромное значение, поэтому принятие единого закона выделит данную группу общественных отношений, «соберет» особенности применения AI в разных сферах. Это позволит не искать положения, связанные с применением AI, в разных подзаконных актах, а найти все в одном документе, что представляется рациональным.

В целом справедливо говорить о том, что Россия придерживается позиции об инструментальной роли AI. Показателен опыт России по внедрению технологий AI в сферу здравоохранения. Например, если в 2015 г. получение результата лучевого исследования длилось несколько дней, то сейчас с использованием системы AI это осуществляется быстро, при этом медики: а) могут обращаться как к оригинальным снимкам, так и к изображениям, обработанным алгоритмами AI; б) могут не согласиться с проведенным анализом, отправить на повторное исследование или осуществить это самостоятельно [4].

Ранее мы обращались к стратегии развития AI в РФ на период до 2030 г. Так, в пп. «а» п. 49 Стратегии упоминается создание экспериментального правового режима (далее – ЭПР) как средства обеспечения благоприятных правовых условий с целью получения доступа к «преимущественно обезличенным» данным, включая те, которые собираются федеральными органами и медицинскими организациями. Подобный ЭПР был установлен в Москве с 1 июля 2020 г. сроком на пять лет [7], предусмотрено, что AI используется участниками ЭПР как инструмент.

Закключение. Таким образом, исходя из изученной информации, можно положительно охарактеризовать опыт РФ в данном направлении, поскольку государство ответственно подходит к применению AI и не зафиксировано негативных ситуаций, вызванных новыми технологиями и неоперативной реакцией на них. Россия использует AI как инструмент, что представляется верным.

Установлено, что использование AI в правоприменении сопряжено с комплексом проблем: а) система не может оценивать доказательства по внутреннему убеждению; б) даже при «рациональном подходе» AI субъективность при принятии решений не исключается; в) AI может не принять во внимание некоторые смягчающие и отягчающие наказание обстоятельства; г) могут возникнуть проблемы при анализе системой AI фактических обстоятельств дела на предмет установления оценочных понятий уголовного закона.

При оформлении правового регулирования общественных отношений, связанных с применением AI в принятии отдельных решений, следует сделать выбор в пользу единого правового документа, поскольку это: а) позволит выделить эти общественные отношения, к которым будут применимы соответствующие принципы (приоритет традиционных ценностей и т. д.); б) представляется рациональным – возможность найти все соответствующие положения в одном документе, а не искать это в подзаконных актах, которые могут противоречить друг другу.

Выполнение поставленных задач способствовало достижению цели исследования – рассмотреть внедрение AI в механизм правового регулирования и проанализировать отечественную и зарубежную практику.

Представляется правильным исследовать и применять системы AI в таком направлении, чтобы данный механизм играл исключительно инструментальную роль, а конечное решение оставалось бы за человеком как за субъектом, способным оценивать ситуацию с позиции традиционных ценностей и предусмотреть ряд факторов, которые может упустить AI при функционировании. Если человек не будет относиться к функционированию AI с осторожностью, то возникнут негативные последствия: например, фундаментальные ошибки при осуществлении правосудия, причинение смерти другому человеку.

Список литературы

1. Гаврилова Ю. А. Проблема смысла права в цифровом обществе // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2020. Т. 24, № 3. С. 608–628.
2. Гаврилова Ю. А., Рыбакова О. С. Трансформация правовой политики в условиях цифровизации правовой реальности // Правовая парадигма. 2020. Т. 19, № 4. С. 17–23.
3. ИИ посоветовал пациенту умереть: самые крупные ошибки машинного обучения. URL: <https://hightech.fm/2021/09/02/ai-failures> (дата обращения: 18.09.2022).
4. Московские врачи начали применять искусственный интеллект для диагностики инсульта и легочной гипертензии. URL: https://www.mos.ru/news/item/105220073/?utm_source=search&utm_term=serp (дата обращения: 18.09.2022).
5. 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. URL: http://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 18.09.2022).
6. Решение Верховного Суда штата Висконсин от 2016 г. по делу «Штат Висконсин против Эрика Лумиса (апеллянта)» [State of Wisconsin v. Eric L. Loomis / Decision of the Supreme Court of Wisconsin No. 2016 WI 68 of 2016]. URL: <https://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/> (дата обращения: 18.09.2022).
7. Федеральный закон от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных». URL: <http://publication.pravo.gov.ru/Document/View/0001202004240030> (дата обращения: 18.09.2022).

8. Dempsey J. X. Artificial Intelligence: An Introduction to the Legal, Policy and Ethical Issues. USA, Berkeley: Berkeley Center for Law & Technology. 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2020/08/Artificial-Intelligence-An-Introduction-to-the-Legal-Policy-and-Ethical-Issues_JXD.pdf (дата обращения: 18.09.2022).

9. Surden H. Artificial Intelligence and Law: An Overview // Georgia State University Law Review. 2019. № 4. Pp. 1305–1337. URL: <https://readingroom.law.gsu.edu/cgi/viewcontent.cgi?article=2981&context=gsulr> (дата обращения: 18.09.2022).

10. Темірбеков Ж. Р. Құқық пен жасанды интеллект арақатынасы: кейбір зерттеулер // Құқық және мемлекет. 2022. № 2 (95). Pp. 83–99. URL: https://km.kazguu.kz/uploads/files/6_Темірбеков_Ж.Р..pdf (дата обращения: 18.09.2022).

Т. А. Гашимов,
аспирант,

Институт законодательства и сравнительного правоведения
при Правительстве Российской Федерации

ВЛИЯНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА ВЗАИМОДЕЙСТВИЕ ГОСУДАРСТВА И ГРАЖДАНСКОГО ОБЩЕСТВА

Аннотация. В настоящей статье рассматриваются теоретические основы и практические примеры взаимодействия государства и гражданского общества посредством сети Интернет. Приводится сравнение социологического и юридического подхода к цифровым правам, а также практика иностранных государств по различным вопросам реализации традиционных прав человека посредством сети Интернет.

Ключевые слова: цифровые права, право на объединение, гражданское общество, взаимодействие государства и гражданского общества, Интернет, теория сетевого общества, право на доступ в Интернет

THE IMPACT OF DIGITAL TECHNOLOGIES ON THE INTERACTION BETWEEN THE STATE AND CIVIL SOCIETY

Abstract. The article reviews the theoretical framework and practical examples of interaction between the state and civil society through the Internet. Compares the sociological and legal approach to digital rights, as well as the practices of foreign states on various issues of realising traditional human rights through the Internet.

Keywords: Digital rights, Right to association, Civil society, Interaction between state and civil society, Internet, Theory of the networked society, Right of access to the Internet

Введение. С развитием современных технологий происходит все больше изменений в сфере взаимодействия институтов гражданского общества и государства. Традиционные формы участия представительства граждан и обратной связи между государством и гражданами, такие как политические партии, процедура выборов и другие, постепенно теряют популярность и доверие во многих странах мира.

При этом нарастает популярность сетевых форм коммуникации между гражданами и государством: онлайн-петиций, объединений жителей в социальных сетях и др.

В настоящей работе рассматриваются теоретические аспекты цифровых прав, а также конкретные практические примеры реализации взаимодействия гражданского общества и государства посредством современных сетевых технологий.

1.1. Ключевой теоретической основой идеей о гражданском обществе в информационно-цифровую эпоху является теория Мануэля Кастельса [1. С. 214] о сетевом обществе, в котором ключевые социальные структуры и деятельность его членов организованы вокруг сетей электронных коммуникаций. При этом в отличие от традиционных социальных структур, которые основаны на иерархии и относительной устойчивости функций их членов, сетевые структуры отличаются автономией отдельных членов и неформальным лидерством.

Этот подход отражает социологическую сущность данного явления. При этом с юридической точки зрения использование сети Интернет является лишь формой, возможностью реализации любого права, в том числе права на объединение.

1.2. При этом право на доступ в Интернет выступает в юридической доктрине и практике как самостоятельное, новое право человека [2. С. 110].

Конституции или законодательство некоторых государств содержат прямые или косвенные положения о праве на доступ в сеть Интернет как право человека.

Так Конституция Греции в части 2 статьи 5А содержит норму схожую на право на доступ в Интернет: «Облегчение доступа к информации в электронной форме, а равно ее производства, обмена и распространения является обязанностью государства» [3].

Часть 2 ст. 10 Конституции Непала 2015 г. содержит следующее положение: «Радио, телевидение, Интернет или другие формы цифрового или электронного оборудования, пресса или любые иные средства коммуникации и распространения информации, эфирного вещания или передачи любых новостей... не могут быть закрыты, изъяты или лишены регистрации в связи с произведенными публикациями, трансляцией или изданием таких материалов на аудио-, аудиовизуальном или электронном оборудовании» [4].

Закрепление права на доступ в Интернет предполагалось и в проекте Конституции Чили 2022 г. [5].

Схожие нормы, но на уровне решения высшей судебной инстанции или отраслевого законодательства содержатся в законодательстве Франции [6], Эстонии [7].

1.3. Далее будут рассмотрены примеры использования сети Интернет при взаимодействии государства и гражданского общества в различных сферах общественной жизни.

Так, в сфере трудового права широко дискуссионным является вопрос об объединении в профессиональные союзы работников электронных платформ (сервисы такси, доставки и пр.). Различные страны по-разному решают данный вопрос [8. С. 94]: в Германии таких работников принимают в «традиционные профсоюзы», в Италии – признают исполнителями по гражданско-правовому контракту.

В сфере электорального процесса приводятся примеры, как в авторитарных странах использование оппозиционными кандидатами социальных сетей позволяет им нивелировать контроль правящих политических платформ над традиционными СМИ и выигрывать выборы (Турция и выборы мэра Стамбула) [9].

В сфере решения вопросов местного значения широкое распространение получили домовые и районные чаты, в которых обсуждаются вопросы управления общей собственностью и развития отдельных территорий. При этом аналогичные информационные площадки также иногда используются для протестной активности, например чаты по противодействию введению ограничений в связи с пандемией COVID-19 [10. С. 62].

Таким образом, использование современных технологий является дополнительным инструментарием к «традиционному» набору прав и возможностей объединений граждан для реализации политических и гражданских прав.

При этом остается дискуссионным вопрос, образуется ли сетевое объединение с точки зрения Федерального закона об общественных объединениях, обладает ли такое объединение возможностями для судебной защиты своих прав, проведения мероприятий, получения пожертвований и помощи от государства.

Заключение. Таким образом, использование цифровых технологий является субсидиарной формой реализации права на объединение, не образует с юридической точки зрения новых прав, но при этом на практике поднимает множество вопросов, которые требуют осмысления и разрешения как в отраслевом законодательстве, так и на уровне теории и практики конституционного права.

Список литературы

1. Бобова Л. А. Мануэль Кастельс: Влияние сетевого общества на характер социальных коммуникаций // Вестник МГИМО – Университета. 2013. № 5. С. 213–220.
2. Хуснутдинов А. Право на доступ в Интернет – новое право человека? // Сравнительное конституционное обозрение. 2017. № 4 (119). С. 109–123.
3. The Constitution of Greece. URL: <https://www.hellenicparliament.gr/en/Vouli-ton-Ellinon/To-Politevma/Syntagma/> (дата обращения: 13.09.2022).
4. The Constitution of Nepal. URL: <https://lawcommission.gov.np/en/wp-content/uploads/2021/01/Constitution-of-Nepal.pdf> (дата обращения: 13.09.2022).
5. Project of Constitution of Chile. URL: <https://guiaconstitucional.cl/wp-content/uploads/2022/07/Texto-Definitivo-CPR-2022-Tapas.pdf>. (дата обращения: 13.09.2022).
6. Décision n° 2009-580 DC du 10 juin 2009. URL: <https://www.conseil-constitutionnel.fr/decision/2009/2009580DC.htm> (дата обращения: 13.09.2012).
7. Public Information Act. URL: <https://www.riigiteataja.ee/en/eli/514112013001/consolide> (дата обращения: 13.09.2022).
8. Избиенова Т. А., Безина А. К. Реализация права на объединение работников, занятых через интернет-платформы, в европейских странах и в Российской Федерации // Актуальные проблемы российского права. 2021. № 2 (123).
9. Кривошеев К. Стамбул не дал себя переголосовать // Коммерсант. URL: <https://www.kommersant.ru/doc/4010867?ysclid=18932v441a614022609> (дата обращения: 15.09.2022).
10. Лебедева Е. В. «Право на город» и локальные сообщества: возможные сценарии развития // Социологическая наука и образование: современные вызовы и риски: материалы Междунар. науч.-практ. конф., посвящ. памяти проф. Г. П. Давидюка. Минск, 10 нояб. 2021 г. Минск: БГУ, 2021. С. 61–65.

Т. С. Гладкова,

аспирант,

Российская академия народного хозяйства и государственной службы

при Президенте Российской Федерации

ОБ УЧАСТИИ ГРАЖДАН В УПРАВЛЕНИИ ВЫЗОВАМИ ЦИФРОВОЙ ЭКОНОМИКИ КОНСТИТУЦИОННЫМИ ПРАВООТНОШЕНИЯМ

Аннотация. Показана актуальность участия граждан Российской Федерации в управлении вызовами цифровой экономики конституционными правоотношениями. Рассмотрен подход демократии соучастия в контексте объединения усилий для нивелирования стоящих вызовов. Проанализированы условия эффективной реализации подхода демократии соучастия. Подчеркнута важность и определены способы формирования проактивного общества.

Ключевые слова: цифровая экономика, вызовы цифровой экономики, конституционные правоотношения, формы прямой демократии, представительная демократия, демократия соучастия

ABOUT THE IMPORTANCE OF CITIZENS' PARTICIPATION IN MANAGING THE CHALLENGES OF THE DIGITAL ECONOMY TO CONSTITUTIONAL RELATIONSHIPS

Abstract. The purpose of the study is to show the relevance of citizens' participation in managing the challenges of the digital economy to constitutional legal relations. The article considers the approach of participatory democracy in the context of joining efforts to level the challenges. The conditions for the effective implementation of the participatory democracy approach are analyzed. The importance is emphasized and ways of forming a proactive society are determined.

Keywords: Digital economy, Digital economy challenges, Constitutional legal relations, Forms of direct democracy, Representative democracy, Participatory democracy

Сегодня в Российской Федерации осуществляется переход к цифровой экономике. Это переход на новый уровень развития, при котором осуществляется широкое применение информационных технологий и целью которого является повышение качества жизни человека.

Вместе с тем цифровая трансформация несет в себе не только возможности, но и вызовы, в том числе и для конституционных правоотношений: вызовы, связанные с обеспечением конституционного права на защиту от безработицы; вызовы, связанные с обеспечением конституционного права на образование и гарантий равных прав и свобод человека и гражданина; вызовы, связанные с обеспечением гарантий свободы конкуренции; вызовы, связанные с обеспечением гарантий свободы мысли и слова; вызовы, связанные с обеспечением права на неприкосновенность частной жизни, личную и семейную тайну, защиту своих чести и доброго имени [3].

Представляется важным участие всех субъектов конституционных правоотношений в управлении вызовами. Основная цель нам видится в объединении усилий для нивелирования стоящих вызовов. Граждане Российской Федерации

имеют право участвовать в управлении делами государства как непосредственно, так и через своих представителей [1]. При этом целесообразно использовать новый подход – переход от представительной демократии к демократии соучастия, в рамках которой важнейшие решения принимаются в интерактивном режиме путем вовлечения в обсуждение и принятие решений широких слоев населения, которые коммуницируют между собой и с органами государственной власти [4].

Для эффективной реализации такого подхода необходимы в первую очередь понимание гражданами стоящих вызовов и готовность к проактивному участию. Но проактивное общество, которое будет понимать стоящие вызовы и будет готово вместе с государством решать их, надо формировать. В связи с этим представляется важным:

- 1) формирование дополнительных каналов коммуникации,
- 2) целенаправленное взаимодействие органов государственной власти с населением (прямая и обратная связь) по вопросам цифровой трансформации экономики,
- 3) информирование о стоящих вызовах,
- 4) постоянное обучение населения новым формам социально-политической активности и их внедрение.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Российская газета. 2020. 4 июля.
2. Гладкова Т. С. Цифровая экономика как правовое понятие. Нормативные основы цифровой трансформации экономики в России и за рубежом // Мир юридической науки. 2018. № 5. С. 5–16.
3. Гладкова Т. С. Вызовы конституционным правоотношениям в условиях перехода Российской Федерации к цифровой экономике (в аспекте исторического материализма) // Конституционное и муниципальное право. 2021. № 12.
4. Нэбит Дж., Эбурдин П. Что нас ждет в 90-е годы. Мегатенденции. 2000. М.: Республика, 1992.

Н. В. Глотов,

студент,

Приволжский филиал Российского государственного
университета правосудия

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Аннотация. В статье рассмотрены проблемы внедрения искусственного интеллекта в уголовное судопроизводство. Процесс повышения эффективности уголовного судопроизводства с помощью перспективных информационных технологий позволит обеспечить реализацию принципа разумного срока уголовного

судопроизводства при соблюдении условия процессуальной экономии, повысить качество отправляемого правосудия и уменьшить нагрузку на судей.

Ключевые слова: юриспруденция, уголовный процесс, уголовное судопроизводство, искусственный интеллект, информатизация, цифровые технологии, информационное общество

FEATURES OF THE USE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL PROCEEDINGS

Abstract. Within the framework of this article, the author tried to consider the problems of introducing artificial intelligence into criminal proceedings. The process of increasing the efficiency of criminal proceedings with the help of advanced information technologies makes it possible to ensure the implementation of the principle of a reasonable time in criminal proceedings, while observing the condition of procedural economy, to improve the quality of justice administered and to reduce the burden on judges.

Keywords: Jurisprudence, Criminal procedure, Criminal proceedings, Artificial intelligence, Informatization, Digital technologies, Information society

Перспектива широкого применения и внедрения искусственного интеллекта (далее – ИИ) является одним из наиболее актуальных векторов развития деятельности всех ветвей государственной власти. Заинтересованность в использовании таких технологий присутствует как со стороны общественности, так и со стороны, научного и бизнес-сообщества [10]. Некоторые исследователи относятся скептически к ИИ, настаивая на том, что, несмотря на рост вычислительной мощности и совершенства программного обеспечения ЭВМ, никаких принципиальных прорывов в решении фундаментальных проблем ИИ не произошло [15. С. 91–107].

Первой проблемой правового регулирования искусственного интеллекта во всех сферах жизнедеятельности, а не только в уголовном процессе является отсутствие универсальной дефиниции. Такой пробел порождает некоторую неопределенность в самых базовых вопросах нормативного регулирования. Единственное данное законодателем определение искусственного интеллекта содержится в «Национальной стратегии развития искусственного интеллекта на период до 2030 года». Так, искусственный интеллект – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений [6]. Однако данное определение создано специально для целей описанной выше стратегии.

Доктринальные определения искусственного интеллекта так же сильно различаются. Ученые выбирают разные методы исследования этого термина: используется этимологический подход; применяется взгляд на ИИ как на систему задач [7. С. 512–516] или как компьютерно-программную систему [9. С. 91–109].

По нашему мнению, для регулирования ИИ необходимо избрать иной уровень правового регулирования, например, Федеральный закон «Об искусственном интеллекте». Предметом выступят отношения, возникающие при внедрении, применении и обеспечении деятельности информационных систем, использующих искусственный интеллект. Также необходимо дать определение основным понятиям, используемым в данной сфере, установить общую систему принципов применения на уровне национального законодательства ИИ, предусмотреть иные источники правового регулирования. Остановившись подробнее на нормативных источниках для регулирования искусственного интеллекта в уголовном судопроизводстве, наиболее предпочтительным является специальный федеральный закон с небольшим объемом регулирования.

ИИ может быть лишь помощником профессионального судьи или судебной коллегии, поскольку само законодательство ссылается на личные качества судьи. В первую очередь необходимо обратиться к Закону РФ от 26.06.1992 № 3132-1 «О статусе судей в Российской Федерации». Он содержит в себе положения о том, что судебная власть в Российской Федерации принадлежит только судам в лице судей и представителям народа. При трактовке этой нормы, устанавливающей исчерпывающий перечень лиц, наделенных полномочием по осуществлению власти, становится ясно, что на сегодняшний день искусственный интеллект не может быть наделен соответствующим полномочиями. Аналогичные положения содержит в себе Конституция РФ (ст. 32, 118). Кроме того, процессуальное законодательство нередко обращается к таким категориям, как формирование внутреннего убеждения, разрешение вопросов по совести, по справедливости. Вопрос об алгоритмизации данных процессов остается открытым и на сегодняшний день.

Если рассматривать ИИ как помощника судьи, перспектива его применения становится более реальной, и уже существует в некоторых странах постсоветского пространства [14]. В Азербайджане и Казахстане ИИ помогает судье в части подбора и анализа необходимого законодательства, в области изучения судебной практики, подготовки проекта судебного акта, определении круга участников по делу, включая их извещение. В Китае запущена пилотная программа, использующая информацию содержащуюся в ранее вынесенных судебных актах, помогает судьям определить доказанность обвинения и предлагает наиболее подходящий вид и размер наказания. Кроме того, в процессе доказывания ИИ анализирует речь участников процесса, письменные доказательства по делу. ИИ уведомляет судью в случае выявленных противоречий и недочетов. Применение ИИ в Китае принесло положительные плоды в виде унификации отправляемого правосудия [8. С. 119–120].

Особое значение имеет зарубежный опыт США в части применения прогнозирования рецидива преступления. Система COMPAS помогает судьям избирать меру пресечения и оказывает влияние при решении вопроса об условно-досрочном освобождении. Применение ИИ в данном случае влечет за собой неблагоприятные последствия в виде неверного определения риска рецидива для подсудимого или осужденного на основании его расовой принадлежности. Система работает на основании многих факторов, заложенных в нее человеком, например, «образовательных дефицитов», «профессиональных дефицитов», «дефицита социальных навыков достижения результатов», антисоциальных и криминальных контактов,

дисфункций брачно-семейных отношений. Предполагается, что из-за изначально неправильных условий, установленных авторами этой системы, система рекомендовала применять к темнокожему населению более строгие меры пресечения [4].

По результатам статистических исследований системы COMPAS было установлено, что прогнозы, которая разрабатывает система, оказались малоэффективными. Точность общих прогнозов составила 65 %, индивидуальных прогнозов обычных граждан – 63 %, коллективных прогнозов – 67 %. Следует отметить, что это даже лучше показателей ИИ [5]. Данный пример демонстрирует, что необходимо относиться с осторожностью к принимаемым ИИ решениям. Кроме того, такие решения обязательно необходимо предоставлять на всестороннюю проверку профессиональному юристу. Достижение высокой эффективности ИИ в современный период возможно только при соблюдении принципов превалирования решений человека и ограниченности вмешательства ИИ.

Говоря о принципах использования искусственного интеллекта в судебной деятельности и при осуществлении правосудия, стоит упомянуть Европейскую этическую хартию об использовании искусственного интеллекта в судебных системах и окружающих их реалиях. В ней содержится пять принципов об использовании ИИ в судебных системах и окружающих реалиях [1]:

1. Принцип уважения основополагающих прав.
2. Принцип недискриминации.
3. Принцип качества и безопасности.
4. Принцип прозрачности.
5. Принцип контроля пользователем.

Перспектива включения аналогичных принципов в различные источники правового регулирования кажется наиболее благоприятным решением, которое существенно улучшит отправляемое правосудие без рисков наступления неблагоприятных последствий для участников процесса как, например, с системой COMPAS.

Необходимо отметить, что для уголовного судопроизводства в доктрине предлагается собственная система, использующая ИИ – «Электронные весы правосудия» [12. С. 8–14.]. Ее отличительной чертой видится помощь в выборе наиболее оптимального выбора наказания. В алгоритмы программы закладываются следующие условия, влияющие на наказание:

- Категория преступления.
- Рецидив или совокупность преступлений.
- Умышленность совершенного деяния.
- Стадия преступления.
- Возраст субъекта преступления.
- Вердикт присяжных.
- Порядок рассмотрения уголовного дела.
- Формы и виды соучастия.

Однако на назначении наказания также сказываются иные субъективные характеристики лица, совершившего преступления, например, имущественное и семейное положение, наличие на иждивении третьих лиц, поведение в быту, состояние его здоровья и др. [3]

В 2021 г. у мировых судей Белгородской области появилась возможность использовать искусственный интеллект для подготовки судебного приказа по заявлению ФНС. Эксперимент оказался удачным. За календарный год время, затраченное на подготовку судебного акта, уменьшилось на 84 %. Заинтересованность в применении аналогичного ПО (программного обеспечения), но уже в рамках деятельности арбитражных судов, проявил заместитель председателя арбитражного суда Московской области [13]. По нашему мнению, помощь в подготовке судебного акта на основании поступающей корреспонденции и предоставленных документов поможет существенно уменьшить нагрузку на судей, которая уже на протяжении нескольких лет остается одной из наиболее актуальных проблем российской судебной системы. Отечественные исследователи так же предлагают использовать метод *predictive justice* («прогностическое правосудие») [10]. Однако, по нашему мнению, этот метод является несоответствующим международным стандартам в области применения искусственного интеллекта в судебных системах. Данная позиция поддерживается ученым, считающими, что соблюдение четвертого принципа Европейской этической хартии об использовании искусственного интеллекта в судебных системах и окружающих их реалиях в системах ИИ прогностического типа, основанных на технологиях многослойных нейронных сетей является утопией [15. С. 91–107].

Еще одной новеллой применения ИИ в уголовном процессе РФ является создание суперсервиса «Правосудие онлайн» в рамках интернет портала «Госуслуги». В рассматриваемом случае будут задействованы технологии слабого искусственного интеллекта. Основное преимущество для лиц, подающих заявление в суд – это обеспечение доступности правосудия и облегчение подачи иска в суд, а также оперативное извещение о назначенном заседании. Кроме того, будет реализована возможность присутствовать на заседаниях с использованием средств видеоконференцсвязи. Однако основной задачей именно искусственного интеллекта выступает подготовка проектов судебных решений, включая постановления, определения и приказы; а также расшифровка аудиопротоколов; создание поисковой системы для судей, позволяющей систематизировать и анализировать судебную практику.

Говоря о возможности применения искусственного интеллекта в судебной статистике, стоит обратить внимание на описанную ранее в исследовании систему «*predictive justice*» («прогностическое правосудие»), которая в сфере статистики может себя раскрыть в полной степени. Обращаясь к данным Судебного департамента при Верховном Суде РФ, можно говорить о множестве социально значимых статистических показателей, учитываемых в различных отчетах. В отчете о числе привлеченных к уголовной ответственности и видах уголовного наказания (форма 10.1) содержится следующая информация: социально значимые персональные данные о половой принадлежности осужденных, степени тяжести совершенных преступлений, о повторности привлечения к уголовной ответственности и др. Основываясь на этих показателях за определенное количество отчетных периодов, можно прогнозировать, например, нагрузку на судей определенной инстанции, в будущем.

Досудебные стадии уголовного процесса нуждаются в информатизации не менее уголовного правосудия в силу высокой бюрократической загруженности. Использование искусственного интеллекта при составлении процессуальных доку-

ментов позволило бы частично разрешить эту проблему. Позитивный опыт лишний раз доказывает это. Однако для использования таких технологий необходимо производить формирование цифрового уголовного дела. Занося в специализированную информационную систему данные о участниках процесса позволило бы создавать форму обвинительного заключения, уже содержащего в себе данные, заранее занесенные в такую систему.

По результатам проведенного исследования становится ясно, что применение искусственного интеллекта в уголовном судопроизводстве, включая сферу правосудия, предполагает множество положительных моментов. Однако, в силу сложности нормативного регулирования, остается достаточно дискуссионным вопрос о возможности широкого применения искусственного интеллекта в уголовно-процессуальной деятельности. Остается особенно проблематичным использование искусственного интеллекта в деятельности районных судов и мировых судей.

Список литературы

1. Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях (СЕРЕJ(2018)14) (принята г. Страсбурге 03.12.2018–04.12.2018 на 31-м пленарном заседании Европейской комиссии по эффективности правосудия). URL: <https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4> (дата обращения: 12.09.2022).
2. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // СПС «КонсультантПлюс».
3. Постановление Пленума Верховного Суда РФ от 22.12.2015 № 58 «О практике назначения судами Российской Федерации уголовного наказания» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_190932/ (дата обращения: 12.09.2022).
4. Angwin J., Larson J., Mattu S., Kircher L. Machine Bias // ProPublica. 2016. 23 May.
5. Yong Ed. A Popular Algorithm Is No Better at Predicting Crimes Than Random People // The Atlantic. 2018. 17 Jan.
6. Лагутенков А. Место искусственного интеллекта в мире людей и место людей в мире искусственного интеллекта // Наука и жизнь. 2018. № 2. С. 66–69. URL: <https://www.nkj.ru/archive/articles/33323/> (дата обращения: 12.09.2022).
7. Латфуллина Д. Р. Человеческий разум и искусственный интеллект // Ученые записки Казанского филиала «Российского государственного университета правосудия». 2018. Т. 14. С. 512–516.
8. Ли К.-Ф. Сверхдержавы искусственного интеллекта. Китай, Кремниевая долина и новый мировой порядок. Москва, 2019.
9. Понкин И. В., Редькина А. И. Искусственный интеллект с точки зрения права // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2018. Т. 22, № 1. С. 91–109.
10. Поскряков Р. С. Использование искусственного интеллекта в судебной деятельности // Огарев-Online. 2019. № 16 (137). С. 2. URL: <https://cyberleninka.ru/article/n/ispolzovanie-iskusstvennogo-intellekta-v-sudebnoy-deyatelnosti> (дата обращения: 12.09.2022).

11. Правовое регулирование искусственного интеллекта в условиях пандемии и инфодемии / под ред. В. В. Блажеева, М. А. Егоровой. Москва: Проспект, 2020. 240 с.
12. Рагимов И. М., Аликперов Х. Д. «Электронные весы правосудия» (цели, возможности, преимущества) // Уголовное судопроизводство. 2019. № 3. С. 8–14.
13. Робот-судья: реальность или фантастика – решали на ПМЮФ-22. URL: <https://pravo.ru/lf/story/241675/> (дата обращения: 12.09.2022).
14. Судейское усмотрение: сборник статей / Е. В. Авдеева, Г. А. Агафонова, М. Д. Беляев и др.; отв. ред. О. А. Егорова, В. А. Вайпан, Д. А. Фомин; сост. А. А. Суворов, Д. В. Кравченко. Москва: Юстицинформ, 2020. 76 с.
15. Цветков Ю. А. Искусственный интеллект в правосудии // Закон. 2021. № 4. С. 91–107.

Т. В. Горина,
студент,

Казанский инновационный университет имени В. Г. Тимирязова

ЦИФРОВЫЕ ТЕХНОЛОГИИ В ИНДУСТРИИ ТУРИЗМА В СИСТЕМЕ ПРАВОВЫХ ОТНОШЕНИЙ

Аннотация. Цифровизация стала неотъемлемой частью современного туризма. Туризм напрямую зависит от развития технологического прогресса, поэтому в статье рассматривается туристская отрасль в условиях цифровизации в системе правового регулирования. Отмечается, что цифровизация – это новая форма коммуникационного взаимодействия между производителями и потребителями туристических услуг. Дается характеристика новейшим цифровым технологиям, применяемым в туризме в настоящее время. Представлена информация о цифровых технологиях в системе правовых отношений, выявлены проблемы правового регулирования цифровых технологий в России. Предложены сценарии развития при выявленных проблемах в правовом регулировании.

Ключевые слова: туризм, трансформация туризма, цифровизация, цифровые технологии в туризме, цифровой туризм, правовое регулирование, право

DIGITAL TECHNOLOGIES IN THE TOURISM INDUSTRY IN THE SYSTEM OF LEGAL RELATIONS

Abstract. Digitalization has become an integral part of modern tourism. Tourism directly depends on the development of technological progress, therefore, the article deals with the tourism industry in the context of digitalization in the system of legal regulation. It is noted that digitalization is a new form of communication interaction between producers and consumers of tourism services. A characteristic is given to the latest digital technologies currently used in tourism. Information about digital technologies in the system of legal relations is presented, problems of legal regulation of digital technologies in Russia are identified. Development scenarios are proposed for identified problems in legal regulation.

Keywords: Tourism, Transformation of tourism, Digitalization, Digital technologies in tourism, Digital tourism, Legal regulation, Law

Цифровая трансформация – это главное направление развития экономики в XXI веке. Оно основано на переходе к цифровому формату представления информации с целью повышения эффективности экономики и улучшения качества жизни. Использование цифровых технологий помогает повысить скорость, доступность и безопасность обмена информацией во всех областях жизни. На нынешнем этапе развивать цифровую экономику необходимо для обеспечения конкурентоспособности нашего государства. Мировая эпидемия (COVID-19) является отличным примером того, как быстро может измениться образ жизни всего общества – с «аналогового» на «цифровой».

Туризм считается одной из самых активно развивающихся векторов экономики. Туризм привлекает довольно большие инвестиции, на его долю приходится более 30 % объема мировой торговли услугами. Развитие туристской отрасли во многом будет зависеть от успехов его оцифровки.

Одной из наиболее перспективных цифровых технологий является обработка Больших данных Big Data, блокчейн (Blockchain).

В настоящее время технологии «Больших данных» уже широко используются в индустрии туризма. Так, туристическая компания FUN&SUN переместила все свои данные на блокчейн. Технология Blockchain используется для создания платформ, предназначенных для отслеживания в режиме реального времени информации о свободных номерах в различных отелях без услуг посредников, оплаты проживания без комиссии, бронирования туристических услуг без посредников, управления идентификацией клиентов. Такая информация необходима всем представителям туристической индустрии, поскольку знание истинных предпочтений туристов дает возможность предвидеть их желания и, следовательно, повышать собственную конверсию [2. С. 16; 3].

На сегодняшний день в регулировании отношений в области «Больших данных» основными документами считаются Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О защите персональных данных» и Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В 2017 г. в нашей стране была утверждена Программа «Цифровая экономика», которая направлена на популяризацию инновационного потенциала Российской Федерации. «Большие данные» стоят на первом месте в качестве прорывных цифровых технологий.

Однако в законодательном регулировании Российской Федерации имеются проблемы в применении «Больших данных». Ранее в российском законодательстве в целом отсутствовало понятие «Большие данные». Их регламентировали как «персональные данные». Недавно, 13 июля 2021 г., был утвержден первый национальный стандарт, касающийся «Больших данных». Это ГОСТ Р ИСО/МЭК 20546–2021 «Информационные технологии. Большие данные. Обзор и словарь», в котором представлены основополагающие термины, а также предложено толкование термина «Большие данные» [4].

В зависимости от стран существует разница как правовом регулировании, так и моральном подходе к «Большим данным», как к предмету регулирования. Например, в Европейском союзе «Большие данные» изучаются через права (например, права

на неприкосновенность частной жизни, права на информацию и др.), а в США они изучаются в качестве оборотоспособного и коммерциализируемого актива.

На данный момент в России совершаются определенные попытки создать правовое регулирование «Больших данных». В настоящее время Российская Федерация ставит выбор в пользу создания собственной модели работы с данными. Эта модель будет обеспечивать полный сконцентрированный внутренний контроль за их использованием [9].

Следующим перспективным направлением в туризме считается интернет вещей (Internet of Things). Там туристические компании могут продвинуть свои предложения на фоне конкурентов. Эта технология используется в индустрии гостеприимства для создания комфортабельных условий поездки, которые будут соответствовать индивидуальным предпочтениям путешественников. Так, туристы с телефона могут регулировать температуру в номере, заказывать обслуживание и т. д. [7. С. 497].

Но у этой технологии наблюдаются огромные минусы, связанные с идентификацией пользователей, конфиденциальностью и безопасностью личных данных. Уже не первый год собирают собрания и ведут дискуссии о необходимых законодательных изменениях, поскольку Россия вступает в новый этап. Данный этап предусмотрен Стратегией развития туризма в Российской Федерации на период до 2035 года, принятой в 2019 г. В Стратегии термин «Интернет вещей» трактуется одним из важнейших научно-технологических направлений. Сразу стоит указать, что российские законодательные изменения вносятся постепенно, более медленными шагами.

Если говорить об идентификации, то здесь государством была реализована система ЕСИА. Подобная система обеспечивает авторизованный доступ к информационным системам. Но в настоящий момент данная система функционирует не в полную силу: например, использование ЕСИА для идентификации пользователя, использующего сеть Wi-Fi в общественных местах, только запланировано на реализацию в ближайшие пару лет. Вопрос идентификации невозможно рассматривать сам по себе, так как здесь все взаимосвязано. По этой причине вопрос безопасности передаваемых личных (паспортных) данных остается актуальным по сей день. Вследствие этого наблюдается схожая связь интернета вещей с технологией «Больших данных», которая заключается в отсутствии законодательного урегулирования процесса передачи конфиденциальных данных. У людей нет уверенности в защищенности данных. Следовательно, необходимо внести изменения правовых норм, регулирующие сбор и обработку личных данных [5].

Мобильные приложения – это тоже одна из цифровых технологий в туризме. Они специализируются в качестве приложений для путешествующих лиц. Сейчас эти приложения активно развиваются, что помогает предоставлять онлайн – доступ к покупке авиабилетов, аренде транспорта, бронированию отелей, навигации по местности. Помимо этих функций, мобильные приложения предоставляют справочную информацию о туристских дестинациях, об отзывах и рейтингах средств размещения, питания и т. д.

Если говорить об урегулировании правоотношений в мобильных приложениях, то в России не существует правового регулирования электронной торговли. Были многочисленные попытки принять законодательный проект «Об электронной

торговле», но до сих пор этого не произошло. Так, в 2000 г. был представлен проект закона № 11081-3 «Об электронной торговле» в Государственную Думу, но в 2004 г. во время рассмотрения законопроекта во втором чтении Государственной Думой он был отклонен и снят с рассмотрения в дальнейшем. В настоящее время загрузка мобильного продукта происходит через платформы цифрового распределения (Google, Apple и Windows). Если отношения, связанные с загрузкой и установкой приложения, регулируются внутренними нормативно-правовыми актами в области защиты прав потребителя, то отношения, связанные с размещением разработчиками приложений на платформах, не урегулированы. Пробел в правовом регулировании цифрового распределения заполняется нормами, устанавливаемыми самими сайтами [10].

Sharing Economy радикально меняет роли между поставщиками туристских услуг и их потребителями. Благодаря подобной технологии, развиваются многие сервисы. Примером могут быть Airbnb, Booking (сервисы аренды жилья), Uber (транспортные услуги) [6].

Любое приложение для аренды недвижимости требует ввода личных данных и вступления в отношения с незнакомыми людьми, что подвергает пользователей определенным рискам. Использование приложений для сдачи недвижимости без посредников может быть опасно тем, что потребитель способен не заплатить или повредить предметы (например, в квартире). В таком случае риск состоит в том, что потребитель может не заплатить ущерб владельцу, нанесенный им. Основная проблема заключается в том, что государство не готово законодательно регулировать шеринговую экономику. В России постоянно происходит уклонение от уплаты налогов. Тем не менее, власти продолжают прилагать все усилия, чтобы ввести в законодательство такой термин, как «шеринговая экономика» или «экономика совместного потребления» [11].

Создание цифровых платформ изменяет отношения между субъектами туристского рынка. Они упрощают коммуникацию между ними и отодвигают посредников. Цифровые платформы открывают потребителям доступ к информации по всему миру, а туристическим компаниям обеспечивают возможность применять мировой опыт в своих фирмах, при этом расширяя рынок и привлекая потребителей туристских услуг. Например, это цифровая платформа Russpass. Она носит не только информационный характер, но и позволяет туристам спланировать путешествие по России, исходя из своих интересов и предпочтений. Использование подобной технологии допускает исключения посредников из цепочки «производитель – потребитель» и экономит на маркетинговых и коммуникационных затратах. Цифровые платформы способствуют международному сотрудничеству предприятий, осуществляя инновационный импульс по развитию цифровых технологий в компаниях [1. С. 71–80].

Отличительная черта и сложность в правовом регулировании на цифровых платформах – это пользовательское соглашение, потому что именно оно устанавливает отношения внутри площадки. Поэтому ему следует уделить особое внимание, чтобы оценить необходимость введения нового правового понятия и системы правовых норм, так как эти меры отвечают современным потребностям в обществе и способствуют техническому прогрессу. По всей видимости, такая ситуация свидетельствует о необходимости создания национального платформенного законодательства [8].

Подводя итог, отметим, что современные направления технического прогресса и высокая потребность общества в получении туристских услуг с помощью цифровых технологий, создают определенную необходимость в правовом регулировании цифровых платформенных решений. Так, можно предложить внести изменения в Федеральный закон «Об основах туристской деятельности в Российской Федерации». В ст. 1 рекомендуется внести такое понятие, как «Цифровизация в сфере туризма», в гл. 3 внести правовое регулирование, установить правоотношения и регулирование правовых технологий. Рекомендуется принять законопроект «Об электронной торговле», внести такие понятия, как «Шеринговая экономика» или «Экономика совместного потребления». Также на федеральном уровне необходимо внести понятие «Большие данные» в Федеральный закон «Об информации, информационных технологиях и о защите информации». Создание платформенного права как современного направления российского права, представляет национальный прогресс. Оно имеет очень большое социальное значение и позволит увеличить экономические возможности России на мировой туристической арене в качестве современной научно-технической и правовой трансформации.

Список литературы

1. Абдикеев Н. М., Морева Е. Л. Основные тренды развития методов и моделей использования цифровых технологий при создании цепочек воспроизводства добавленной стоимости // Мир новой экономики. 2019. № 13 (30). С. 71–80.
2. Ахметова А. С. Возможности практического применения технологии блокчейн // Инновации в науке: научный журнал. 2018. № 10 (86). С. 15–16.
3. Блокчейн. URL: <https://vc.ru/flood/85973-cifrovaya-transformaciya-v-turizme-trendy-2020> (дата обращения: 03.09.2022).
4. ГОСТ Р ИСО/МЭК 20546–2021. Информационные технологии. Большие данные. Обзор и словарь. Введен 01.11.2021. URL: <https://clck.ru/3238vb>
5. Интернет вещей. URL: http://www.siblegal.ru/articles/main_news/nekotorye-voprosy-pravovoy-reglamentatsii-interneta-veshchey/ (дата обращения: 11.09.2022).
6. Лучшие мировые практики цифровой трансформации. URL: <https://digitalbusinessmodel.ru/page7181064.html> (дата обращения: 03.09.2022).
7. Паршин В. Я., Паршина М. В. Цифровые технологии как инструмент, влияющий на потребительский выбор в сфере туризма // Образование и наука в России и за рубежом. 2019. № 2 (50). С. 497.
8. Правовая природа цифровых платформ. URL: <file:///C:/Users/Tatyana/Desktop/2709-5711-1-PB.pdf> (дата обращения: 11.09.2022).
9. Правовое регулирование Больших данных. URL: <http://teamgroup.ru/pravovoe-regulirovanie-big-data-v-rossii.html> (дата обращения: 11.09.2022).
10. Проблемы правового регулирования мобильных приложений. URL: <https://wiselawyer.ru/poleznoe/81098-problemy-pravovogo-regulirovaniya-rynka-mobilnykh-prilozhenij/> (дата обращения: 11.09.2022).
11. Экономика шеринга. URL: <https://tiesc.mgimo.ru/2022/2022-05/sharing-economy-pros-cons-prospects> (дата обращения: 11.09.2022).

М. А. Горшкова,

студент,

Белорусский государственный университет транспорта,

Д. С. Драгун,

студент,

Белорусский государственный университет транспорта

ЭЛЕКТРОННОЕ ПРАВОСУДИЕ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Аннотация. В статье представлен анализ формирования, развития и становления системы электронного правосудия в Республике Беларусь. Рассматриваются подходы к ведению судопроизводства с помощью цифровых технологий, проводится анализ доступных в различных режимах функций действующей информационной платформы электронного правосудия. Выявлены сильные и слабые стороны интерфейса, а также сформулированы направления совершенствования функционирования сайта.

Ключевые слова: электронное правосудие, Верховный Суд Республики Беларусь, экономический суд, судопроизводство, электронная документация, цифровые технологии, инновации

E-JUSTICE IN THE REPUBLIC OF BELARUS

Abstract. The authors present an analysis of the formation, development and formation of the electronic justice system in the Republic of Belarus. Approaches to conducting legal proceedings using digital technologies are considered, the analysis of the functions of the current electronic justice information platform available in various modes is carried out. The strengths and weaknesses of the interface are identified, as well as the directions for improving the functioning of the site are formulated.

Keywords: e-Justice, Supreme Court of the Republic of Belarus, Economic Court, Legal proceedings, Electronic documentation, Digital technologies, Innovations

Создание информационного общества является одним из основных направлений развития современности, в рамках которого ИТ-технологии охватывают все более широкие сегменты функционирования социальной среды. Ключевую роль обеспечения реализации прав и свобод субъектов в условиях трансформирующейся реальности как в глобальном мировом масштабе, так и в Республике Беларусь, играет непрекращающаяся разработка и модернизация системы электронного правосудия.

Электронное правосудие представляет собой способ осуществления правосудия, основанный на использовании информационных технологий, что способно стать одним из революционных прорывов в судопроизводстве.

Первые шаги в развитии электронного правосудия в Республике Беларусь относятся к 2010 г., когда в экономических судах начали применять информационные технологии: электронные расписания заседаний, возможность рассматривать некоторые категории дел по видеосвязи, если судья и ответчик находились в разных экономических судах, аудио- и видеозапись как альтернатива протоколу судебного заседания.

Активное развитие электронное правосудие получило в условиях распространения коронавирусной инфекции, когда в связи с массовой вынужденной изоляцией населения появилась необходимость расширения форм участия граждан в судебной деятельности и разработки новых функций системы, например, таких как внедрение конференцсвязи для опроса свидетелей и возможность принять дистанционное участие в судебном разбирательстве в режиме реального времени для лиц, участвующих в деле.

Кроме того, в настоящее время имеется возможность удаленного доступа к данным судебных заседаний и текстам судебных постановлений. На коммерческой основе имеется полный доступ к нормативным правовым актам, а также актам правоприменительной практики в поисковой системе «Эталон».

Специализированный сервис «Электронное судопроизводство» как часть сайта Верховного Суда Республики Беларусь (service.court.gov.by) на безвозмездных началах предоставляет ограниченный функционал (получить образцы документов для обращения в суд, дистанционно подать обращение, жалобу, ходатайство и отслеживать его движение, предоставить материалы, оказывающие влияние на доказательную базу в делах, находящихся в рассмотрении, с помощью сети Интернет). В онлайн-режиме осуществляется примерный расчет государственной пошлины с помощью сервиса «Калькулятор госпошлины».

Несмотря на все вышеперечисленные возможности и нововведения, на сегодняшний день существует множество ограничений в системе рассматриваемого программного компонента электронного правосудия. Один из них проявляется в том, что возникает необходимость подтверждения подлинности в суде электронной документации бумажными носителями либо заверенными копиями у нотариуса. В свою очередь, данная процедура увеличивает время рассмотрения документации и ее количественный объем.

Документация, представленная в электронной форме, считается подлинной, если имеет цифровую подпись или ее аналог. В другом случае документ является недействительным согласно положений Закона Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи».

Информация, которая находится в форме звуко- и видеозаписей, исследуется согласно нормативам, указанным в ст. 90 Хозяйственного процессуального кодекса Республики Беларусь: лица, которые предоставляют данную информацию, обязаны указать кем, когда и где были сделаны записи. Запрещается использовать доказательства, если они получены скрытым путем, исключая случаи, когда запись разрешается законодательством. Предоставленные звуко- и видеозаписи не возвращаются владельцу.

Для входа на сайт необходимо зарегистрироваться как юридическое лицо (субъект хозяйствования) или физическое лицо (представитель физического лица). Без подобной авторизации доступен только калькулятор госпошлины. После авторизации появляется доступ ко всему функционалу, перечисленному выше. Сайт доступен на русском и белорусском языках в любое время суток, ежедневно. Имеется версия сайта для слабовидящих в нескольких цветовых палитрах с возможностью изменить размер шрифта. Однако на сайте Верховного Суда Республики Беларусь

нет прямого доступа к сайту электронного судопроизводства, сайт непросто найти с помощью поисковых запросов известных браузеров.

Сайт имеет ряд несовершенств, таких как: сложная многоуровневая систематизация информации, интуитивно не понятная простому пользователю, ограниченное количество операций, продолжительное время рассмотрения электронных документов и их регистрации. Сайт не имеет поисковой строки и прямой связи с технической поддержкой.

В настоящее время платформа национального электронного правосудия продолжает свое развитие, и в качестве направлений последнего можно сформулировать следующие дополнительные возможности, введение которых позволит расширить получаемую пользователем информацию:

- о долгах, их оплате, исполнительном производстве;
- об ограничениях на въезд и выезд из Республики Беларусь, снятии данных ограничений при их наличии;
- о задолженности по уплате государственной пошлины;

Представляется также востребованным дистанционное получение справок об отсутствии судимости, возможность записаться на консультацию к судебному исполнителю.

Визуальная часть сайта должна привлекать пользователей, быть более красочной и понятной, обязательно должны быть представлены поисковая строка и обратная связь с техподдержкой.

Реализация указанных предложений поможет привлечь новых пользователей, что в свою очередь положительно скажется на времени обработки документации и уменьшит живую очередь, послужит катализатором для развития отдельных элементов электронного судопроизводства, что в итоге обеспечит абсолютную открытость ведения судебной деятельности и повысит эффективность работы судебной системы в целом.

Список литературы

1. Блинков И. А., Яковлева А. П. Плюсы и минусы электронного правосудия: поиск баланса // Вестник Поволжского института управления. 2019. Т. 19, № 6. С. 73–79.
2. Бойко В. К., Жук М. Г., Шулейко Е. И. Электронные документы как элемент «электронного правосудия» // Информационные технологии в юридических и экономических науках. 2020. С. 283–284.
3. Бурдин Е. В., Зуев С. В. Цифровые доказательства и электронная форма судопроизводства по гражданским делам // Электронное правосудие. 2021. С. 108–122.

К. И. Гришин,

студент,

Казанский инновационный университет имени В. Г. Тимирязова

РАЗВИТИЕ СЕМЕЙНОГО ПРАВА В РОССИЙСКОЙ ФЕДЕРАЦИИ В КОНТЕКСТЕ ЗАКЛЮЧЕНИЯ И РАСТОРЖЕНИЯ БРАКА В ОНЛАЙН-ФОРМАТЕ

Аннотация. Современное право едва успевает за стремительно развивающимся миром, сталкиваясь с актуальными вызовами общества. Развитие многополярного мира, пандемия и другие факторы приводят к вынужденным актам государственной власти, приводящим к замедлению межличностного взаимодействия. Лица, желающие вступить в брак, в ряде случаев не могут реализовать свое право в рамках семейно-брачных отношений по свободному вступлению в брак.

Ключевые слова: право, цифровые технологии, семейное право, заключение брака с иностранцем, интернет, коронавирус, семейно-брачные отношения

DEVELOPMENT OF FAMILY LAW IN THE RUSSIAN FEDERATION IN THE CONTEXT OF CONCLUSION AND DIVORCE OF MARRIAGE IN ON-LINE FORMAT

Abstract. Modern law barely keeps up with the rapidly developing world, facing the actual challenges of society. The development of a multipolar world, a pandemic, etc. lead to forced acts of state power, leading to a slowdown in interpersonal interaction. Persons wishing to marry in a number of cases cannot exercise their right within the framework of family and marriage relations to freely enter into marriage.

Keywords: Law, Digital technologies, Family law, Marriage with a foreigner, Internet, Coronavirus, Family and marriage relations

Процесс цифровизации правовых отношений является современным и необходимым этапом совершенствования механизма регулирования общественных отношений путем объединения цифровых технологий с нормами права.

А. Т. Карасев пишет, что «цифровизация общественных отношений в реализации конституционных прав – это процесс перевода информации с аналоговой формы в цифровую форму при реализации закрепленных в гл. 2 Конституции РФ фундаментальных прав человека» [1. С. 112].

При помощи цифровизации правовых отношений, для граждан значительно упрощается процесс реализации своих фундаментальных, конституционных прав, что не может не отвечать интересам Российской Федерации, как правового государства.

Федеральным законом № 147-ФЗ «Об актах гражданского состояния» [2], цифровизация постепенно интегрируется в процесс заключения брака, так, в частности, добавился новый вариант подачи заявления о заключении брака. Согласно ст. 26, брачующиеся имеют право подать заявление в формате электронного документа через единый портал государственных и муниципальных услуг и региональные порталы государственных и муниципальных услуг.

Такие нововведения отвечают общим тенденциям всемирной цифровизации права, которые необходимы в новых реалиях современного мира. Однако, Россия

существенно отстает в этой сфере от других зарубежных стран, которые уже сделали большой шаг к цифровизации правовых отношений и юридических процессов, в рассматриваемой сфере.

В ряде зарубежных стран (США, ОАЭ и др.) на фоне пандемии (COVID-19), начал широко применяться процесс заключения брака онлайн, путем использования видеоконференцсвязи. Питер Б. Мэггсотметил, что в штате Юта первыми в Соединенных Штатах разрешили любой паре вступать в брак через Интернет, находясь в любой точке мира (оба в одном месте или в разных местах). Особый порядок был принят в 2020 году, когда окружные офисы были закрыты для личных посещений из-за пандемии» [3. С. 40].

Реализация дистанционного заключения брака в России обсуждалась еще в марте 2020 года, когда премьер-министр Российской Федерации (далее – РФ) Михаил Мишустин заявил, «работа ЗАГСов приостановлена по определенным форматам, необходимо обеспечить условия, чтобы их услуги можно было получить дистанционно» [4].

Однако, данная инициатива не нашла своего законодательного закрепления и подразумевала лишь необходимость ограничить круг лиц, которые могут присутствовать на официальной части мероприятия и обеспечить возможность подключения их к видеоконференцсвязи.

Семейный кодекс РФ в ст. 11 закрепляет императивную норму, которая предусматривает исключительно очное присутствие будущих супругов в органах ЗАГС [5], что является нормативно-правовым барьером, препятствующим внедрению цифровых технологий в процесс заключения брака.

Официальный сайт мэра Москвы публикует информацию, что «с начала года в столичные органы ЗАГС поступило более 80 тыс. заявлений о заключении брака, из которых свыше 60 % было подано онлайн» [6]. Онлайн-подача заявления о заключении брака в 2022 г. в Москве стала еще более популярной – свыше 60 % молодоженов предпочли такой способ получения услуги, что на 15 % больше, чем за аналогичный период прошлого года.

На практике происходит так, что у населения России имеется большой спрос на цифровизацию правовых процессов, связанных с заключением и расторжением брака, но переступить нормативно-правовой барьер пока не удастся, что обусловлено несколькими объективными причинами. Во-первых, само наличие правовых актов, которые препятствуют преобразованию государственных услуг в электронную форму. Во-вторых, малая правовая обеспеченность работы систем электронного взаимодействия.

Мы считаем, что в условиях ужесточения визовых санкций, результатом которых является невозможность присутствия одного из супругов на территории другого государства, модернизация семейного права путем внедрения процесса заключения брака онлайн – является необходимой мерой обеспечения прав граждан на семью и на защиту института семьи в РФ, предусмотренных в ст. 38 Конституции РФ. Также осознавая сложность проведения описываемых процедур в рамках квазитерриторий России [7].

Мы предлагаем внести поправки в Семейный кодекс РФ ст. 11 и в Федеральный закон № 143-ФЗ «Об актах гражданского состояния» ст. 27, заключающиеся в возможности подачи онлайн-заявления будущих супругов на проведение бракос-

четания онлайн, т. е. без фактического личного посещения органов ЗАГС, путем подключения по видеоконференцсвязи двух заявителей и сотрудника ЗАГС, что позволит упростить процесс заключения брака, сделает его более экономичным, а главное – более доступным, разорвав территориальные препятствия.

Таким образом, цифровизация правовых отношений не только упростит реализацию гражданами своих фундаментальных прав на семью, но и будет отвечать публичным интересам Российской Федерации, как правового государства, исходя из того, что граждане РФ смогут в полном объеме реализовывать свои права и обязанности, несмотря на возникающие вызовы современного мира.

Список литературы

1. Карасев А. Т., Кожевников О. А., Мещерягина В. А. Цифровизация правоотношений и ее влияние на реализацию отдельных конституционных прав граждан в Российской Федерации // Антиномии. 2019. Т. 19, Вып. 3. С. 99–119.

2. Федеральный закон «Об актах гражданского состояния» от 15.11.1997 № 143-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_16758/ (дата обращения: 15.09.2022).

3. Мэггс П. Б. Трансформация права: онлайн-брак и нотариальное удостоверение без границ // Вестник Университета имени О. Е. Кутафина (МГЮА). 2022. С. 39–43.

4. Минюсту РФ поручили наладить дистанционную регистрацию браков. URL: <https://www.interfax.ru/russia/701914> (дата обращения: 15.09.2022).

5. Семейный кодекс Российской Федерации от 29.12.1995 № 223-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_8982/460a84ab74616e740d2581dd3d2140ee1af4b5d8/ (дата обращения: 15.09.2022).

6. Более 60 процентов молодоженов в Москве подают заявления о заключении брака онлайн. URL: <https://www.mos.ru/news/item/112744073/>

7. Гончарова Н. Н., Латыпова Э. Ю., Гончаров Н. Н. Проблемы проведения уголовно-процессуальных действий с участием иностранных граждан, на российской территории, а также в зданиях посольств и консульств России // Пробелы в российском законодательстве. 2021. Т. 14, № 4. С. 366–372.

Е. А. Губаева,

магистрант,

Московский государственный университет имени М. В. Ломоносова

ЭКСПЕРИМЕНТАЛЬНЫЕ ПРАВОВЫЕ РЕЖИМЫ ОСУЩЕСТВЛЕНИЯ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ЦИФРОВЫХ ИННОВАЦИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье рассматривается специфика правового регулирования экспериментальных правовых режимов. Проведен анализ экспериментальных правовых режимов на примере Российской Федерации и англосаксонских стран как прообраза нового регулирования. Обращено внимание, что подобный режим должен быть направлен на поддержку малого и среднего бизнеса. Делается вывод

о необходимости введения в законодательство антимонопольных механизмов в случае выхода технологии из экспериментального правового режима. Кроме того, отмечается, что создание экспериментальных правовых режимов в отношении проектов, связанных с цифровыми технологиями, позитивно скажется на развитии общества.

Ключевые слова: право, экспериментальный правовой режим, цифровые технологии, цифровая экономика, регуляторная песочница, малый и средний бизнес, искусственный интеллект

EXPERIMENTAL LEGAL REGIMES OF ENTREPRENEURIAL ACTIVITY IN THE FIELD OF DIGITAL INNOVATIONS IN THE RUSSIAN FEDERATION

Abstract. The article deals with the specifics of the legal regulation of experimental legal regimes. The analysis of experimental legal regimes is carried out on the example of the Russian Federation and Anglo-Saxon countries as a prototype of the new regulation is carried out. The author of the article draws attention to the fact that such a regime should be aimed at supporting small and medium-sized businesses. It is concluded that it is necessary to introduce antimonopoly mechanisms into the legislation in case of technology withdrawal from the experimental legal regime is made. In addition, it is noted that the creation of experimental legal regimes for projects related to digital technology will have a positive impact on the development of society.

Keywords: Law, Experimental legal regime, Digital technologies, Digital economy, Regulatory sandbox, Small and medium businesses, Artificial intelligence

«Нельзя объять необъятное», – гласит афоризм Козьмы Прутков. Зачастую эта фраза в полной мере соответствует современному законодательному процессу, активному принятию множества новых законов и поправок к старым. Тем не менее существуют определенные сферы, которые требуют внимания государства как регулятора общественных правоотношений, поскольку могут затрагивать права и свободы граждан, что является высшей ценностью.

В современном мире сложно найти ту сферу жизни, которая была бы не затронута тенденцией цифровизации. Соответственно, ни представители бизнеса, ни научное сообщество, ни государство не вправе игнорировать те изменения, которые диктует развитие технологий.

На сегодняшний день цифровая экономика представляет собой особо значимый сектор. Под ней принято понимать «хозяйственную деятельность, ключевым фактором производства которой является обработка больших объемов, что позволяет повысить эффективность технологий» [11]. В результате указанных процессов возникает огромное количество инновационных идей, которые могут качественно улучшить функционирование систем, а также обеспечить конкурентоспособность государства в мировой гонке инноваций.

Для внедрения подобных разработок необходимо законодательное урегулирование, поскольку, как замечают многие эксперты, право не успевает и никогда не будет успевать за развитием новых технологий [16. С. 301]. По оценке Минэкономразвития, принятие федерального закона может занимать от двух до пяти

лет. Соответственно, традиционная процедура принятия законов законодательным органом будет тормозить процесс внедрения инноваций. Поэтому регулятором были предприняты некие шаги для создания правовых инструментариев, позволяющих более гибко и оперативно регулировать цифровые нововведения, а также устанавливать различные меры по созданию комфортных условий для их тестирования. В частности, предусматривается создание следующих институтов:

а) инновационные акселераторы (партнерские соглашения по предоставлению финансовых услуг с использованием новых технологий);

б) инновационные центры (осуществление комплексной юридической помощи стартапам);

в) регуляторные песочницы (допускающие возможность тестирования и ограниченного использования инновации с неким послаблением в правовом регулировании бизнеса в отношении разработок, апробации и внедрении цифровых технологий) [4. С. 61]. В рамках настоящего исследования автор предлагает рассмотреть последний инструментарий как возможность для развития технологических инноваций, выявить определенные проблемы при реализации экспериментальных правовых режимов, а также на примере зарубежного опыта проанализировать возможные последствия внедрения экспериментальных проектов в жизнь.

Для начала следует определиться, как работает экспериментальный правовой режим. Регуляторные песочницы являются изобретением Правительства и финансового регулятора Соединенного Королевства Великобритании. Под ними понимается режим, при котором инноваторам позволяется под контролем регулятора проводить эксперимент в изолированной среде с безопасным запуском [18. С. 1]. Песочницы необходимы для выполнения нескольких задач:

а) снижение правовой неопределенности;

б) обеспечение ясности в отношении необходимости подобной инновации на рынке и ее последующего правового регулирования;

в) поиск баланса между защитой прав потребителей, их персональных данных и продвижением инновационного продукта. Таким образом, регуляторная песочница в первую очередь позволяет восполнить нормативное правовое регулирование с учетом потребностей цифровой экономики, которая стремительно развивается.

Со стороны исследователей нередко возникает справедливый вопрос: какую же форму в идеале должно принять законодательное регулирование экспериментальных режимов? На международной научно-практической конференции «Цифровая трансформация экономических отношений: вызовы для права», организованной совместно МГУ и МГЮА, многие спикеры высказывали свои опасения по поводу складывающегося в России правового режима в отношении регуляторных песочниц. Так, А. В. Габов обратил внимание слушателей на этические проблемы существования экспериментальных правовых режимов. В частности, было высказано мнение с опорой на Федеральный закон № 258-ФЗ [12] о том, что при создании регуляторной песочницы регулятор вправе допустить даже нарушение принципов права, т. е. исходных начал, воплощающих закономерности права, природу и его социальное назначение [10]. Представляется возможным согласиться или опровергнуть указанный довод после анализа сложившегося правового регулирования и определения правовых проблем, из него вытекающих.

Для выявления комплекса мер, используемых регулятором в экспериментальном правовом режиме, Ю. С. Харитонов и Л. В. Санникова выделяют следующие модели правового регулирования:

- a) адаптация под существующие правовые нормы;
- b) фрагментарное внесение изменений в закон;
- c) экспериментальная модель при создании особой экономической зоны;
- d) принятие специальных правовых актов, призванных урегулировать новые правоотношения [8. С. 118].

Исходя из предложенной исследователями классификации следует, что регуляторная песочница будет новым параллельным правовым режимом со своей ответственностью субъектов, порождающим особые правовые последствия. Однако так ли нужен этот режим в современных российских реалиях с учетом многих рисков?

Во-первых, невозможно игнорировать факт того, что в случае реализации экспериментального правового режима начнется массовый сбор персональных данных граждан для последующей обработки и анализа. На сегодняшний день как в России, так и во всем мире не существует комплексного и эффективного инструмента, позволяющего надежно защищать персональные данные неопределенного круга лиц. Более того, многие регуляторы пытаются даже снять ответственность с субъектов регуляторной песочницы в случае нарушения законодательства о персональных данных.

Так, в Великобритании в рамках проектов песочницы участники не будут подлежать ответственности за нарушение акта о персональных данных, если при этом они взаимодействовали с уполномоченным органом и уведомяли о своих действиях [20].

Подобная позиция хоть и выглядит оправданной с точки зрения развития технологий, напрямую нарушает принцип неприкосновенности частной жизни, являющийся основным правом человека по основным законам государств. К такому выводу приходят и суды. Например, в недавнем правовом споре между ООО «В Контакте» и ООО «Дабл» [5] суд указал, что ответчик своими действиями нарушил исключительные права истца на базу данных, а также привел к ситуации, когда истец не может исполнять обязательства перед пользователями по защите их персональных данных.

Представляется, что регулятор в любом случае обязан получать согласия от объектов исследования, даже если это породит бюрократические сложности и удлинит процесс анализа данных.

Во-вторых, существует риск излишнего законотворчества в отношении тех правоотношений, которые функционировали и без режима регуляторной песочницы. Здесь показателен проект телемедицины, заключающийся в проведении онлайн-консультаций врача с пациентом, дистанционном медицинском наблюдении и удаленной идентификации пациента. По итогам телемедицинской консультации медицинский работник вправе поставить пациенту диагноз и назначить лечение.

Опуская обсуждение рисков при удаленной идентификации лица и защиты его персональных данных, отметим, что подобные разработки уже имеют активное применение в рамках проекта «Яндекс.Здоровье» [9]. Это коммерческий сервис онлайн-консультаций, где пациент может обратиться к квалифицированным врачам по многим направлениям. На момент начала работы сервиса для соответствия действующему

законодательству с пациентами заключался договор на оказание информационной услуги. То есть формально предметом договора являлась не медицинская, а информационная услуга по медицинским вопросам. После принятия Приказа Министерства здравоохранения РФ № 965н [6] медицина стала доступна и с применением онлайн-технологий, правда, без постановки окончательного диагноза, но с оценкой состояния здоровья и определения тактики медицинского лечения (что при всей витиеватости звучит синонимично действиям по установлению диагноза пациента).

Соответственно, можно сделать вывод, что в рамках некоторых проектов, подлежащих реализации в экспериментальном правовом режиме, вряд ли создаются новые правоотношения, поскольку они уже существуют в настоящее время без специального правового режима.

Наконец, стоит выделить риск выборочного допуска к экспериментальному правовому режиму субъектов с инновационными инициативами. При анализе проектов, выделенных Минэкономразвития для создания специального экспериментального правового режима, видно, что все субъекты – это крупные компании с уже готовым продуктом. По сути, единственным интересом для них является возможность протестировать свою разработку в условиях смягченного правового режима. Однако одной из целей регуляторных песочниц является еще и обеспечение развития науки и социальной сферы, работа на благо общества [12].

Тем самым возникает закономерный вопрос: возможно ли участие в экспериментальном правовом режиме субъектов малого и среднего бизнеса, преследующих как раз-таки вышеуказанные цели?

На круглом столе, проведенном 01.12.2021 в Совете Федерации [3], заместитель Министра экономического развития Российской Федерации В. В. Федулов отметил, что регулятор заинтересован в участии в экспериментальном правовом режиме именно крупных компаний. Был сделан вывод, что небольшие стартапы, для которых еще не сориентирован финансовый бизнес для дальнейшего развития и выпуска в конвейерное производство, пока не готовы к выводу в правоотношения «регулятор – субъект регуляторной песочницы» и «бизнес – общество».

Делать какие-либо преждевременные выводы относительно российского экспериментального правового режима пока что рано. Однако, опираясь на международный опыт, понятно, что подобные песочницы больше подходят для развития как раз-таки индивидуальных предпринимателей и небольших стартапов. Например, в Сингапуре работа Валютно-финансового управления показала, что 30 из 40 заявок на участие в регуляторной песочнице были отозваны, поскольку участники могли осуществить свои проекты без специального правового режима [19].

В Отчете по деятельности регуляторных песочниц регулятором Великобритании [15] отмечено, что преимущественно заявки на участие в регуляторной песочнице подаются субъектами малого и среднего бизнеса. Это не отменяет участия и крупных компаний, но их интерес должен объясняться не столько необходимостью в таком инструменте как экспериментальный правовой режим, сколько возможностями для ускорения роста своего бизнеса.

Соответственно, невозможно отрицать риск того, что крупные фирмы, давно функционирующие на рынке, могут быстро «вырасти» из предложенной регулятором

песочницы. Все инициаторы утвержденных проектов являются в каком-то смысле «монополистами» рынка. Так, «Яндекс», транснациональная компания в отрасли информационных технологий, получит возможность реализации на территории России проекта по коммерческому использованию беспилотного наземного транспорта. Иной пример: группа коммерческих организаций в области предоставления медицинских услуг, такие как «Медси», «СберЗдоровье», цифровой сервис «Доктор рядом» и сеть клиник «Ниармедик» смогут реализовывать услуги в формате телемедицины.

Как отмечают многие эксперты [1], «объективно, это зрелые технологии, уже частично реализованные в других юрисдикциях». Кроме того, у субъектов проектов достаточно финансовых ресурсов для реализации этого проекта вне искусственного режима песочницы. В таком случае, не будет ли разумнее дать шанс развития и тестирования новых технологий для индивидуальных предпринимателей и небольших стартапов, не имеющих достаточных правовых и экономических средств для выпуска своей разработки?

Известно, что меры поддержки малого и среднего бизнеса в России не являются настолько эффективными, чтобы обеспечить предпринимателей комплексной помощью. Получается, что с введением экспериментальных правовых режимов небольшие стартапы вновь остаются без внимания государства, несмотря на возможный потенциал разработанных ими инноваций. Кроме того, в случае успешного тестирования проектов в условиях регуляторной песочницы регулятор распространит режим на территорию всего государства путем внесения поправок в действующее законодательство. Тем самым компания, являющаяся монополистом в искусственной среде песочницы (поскольку она единственная тестировала свой продукт в комфортных для нее условиях), способна захватить лидерство и на реальном рынке, исключив из конкуренции остальных участников, желающих продвигать похожие технологии.

Таким образом, необходимо продумывать антимонопольные механизмы в случае выхода технологии из экспериментального правового режима, а также предусматривать возможность участия в режиме регуляторных песочниц мелкого и среднего бизнеса.

Подводя итог, следует отметить несколько важных тезисов. Экспериментальный правовой режим в России рассматривается регулятором как прообраз нового регулирования, т. е. в качестве параллельного правового регулирования в ходе проведения тестирования инноваций. Нельзя однозначно утверждать, что данная форма породит лишь негативные последствия. Тем не менее, важно помнить о соблюдении определенных принципов, обеспечивающих эффективное функционирование регуляторных песочниц и соответствие их целям создания.

Экспериментальный правовой режим должен преследовать, в первую очередь, цель блага для общества. Поэтому, насколько это возможно, требуется исключить лоббирование со стороны крупных компаний, которые продвигают свои проекты исключительно с целью удовлетворения собственных интересов, и, возможно, отдельных государственных структур.

На сегодняшний день научным сообществом выдвигаются интересные предложения, продиктованные потребностями бизнеса: например, регистрация результатов интеллектуальной собственности с помощью технологий распределенного реестра. Интерес со стороны общества в подобных технологиях прослеживается в связи с существованием факультативных регистраций объектов авторского права в неком-

мерческих организациях, ведением частных реестров коммерческих обозначений патентными поверенными [13]. Положительным моментом для выбора данного проекта будет возможность оценить эффективность технологий распределенного реестра, опираясь на позитивный иностранный опыт.

Так, в Великобритании широкую поддержку стабильно получают проекты, связанные с технологиями блокчейн. После первых отборов для участия в регуляторной песочнице около 39 % избранных проектов оказались связанными с технологиями распределенного реестра [14]. А, например, в Таиланде в рамках регуляторной песочницы подразделение Банка Таиланда стало использовать технологию блокчейн для удостоверения и сертификации документов [17].

Соответственно, для государства представляется важным считывать реальные запросы со стороны предпринимательства и реализовывать их в инновационных проектах.

Кроме того, необходим допуск в песочницы субъектов малого и среднего бизнеса, так как их разработки зачастую могут быть чрезвычайно полезными для общества, но предприниматели просто не имеют достаточно средств и поддержки со стороны государства для их реализации.

Наконец, нельзя забывать и про защиту прав и свобод лиц. Любая инновация должна быть нацелена на благо общества. О гуманистическом подходе напрямую указывается и в Концепции развития в сфере искусственного интеллекта [7], где одним из принципов провозглашается обеспечение защиты прав и свобод человека, повышение благосостояния граждан в результате развития технологий искусственного интеллекта и робототехники.

Необходимость введения специальных правовых режимов для создания комфортных условий для организаций, ведущих деятельность в приоритетных областях развития цифровой экономики, признается всеми экспертами [2]. Но первоочередной задачей государства, как регулятора возникающих правоотношений в сфере регуляторных песочниц, должно быть соблюдение баланса частных и публичных интересов, поскольку гармонизация и эффективность устанавливаемых режимов зависит именно от этих факторов.

Список литературы

1. Большим инновациям большие песочницы // Comnews. 2021 URL: https://www.comnews.ru/content/214484/2021-05-14/2021-w19/bolshim-innovaciyam-bolshie-pesochnicy?utm_source=telegram&utm_medium=general&utm_campaign=general (дата обращения: 26.08.2022).
2. Вайпан В. А. Правовое регулирование цифровой экономики // Предпринимательское право. Приложение «Право и Бизнес». 2018. № 1. СПС «Консультант-плюс».
3. Круглый стол Совета Федерации по теме «Оценка эффективности экспериментальных правовых режимов и возможности расширения сферы их применения». 2021. URL: <https://www.youtube.com/watch?v=UMX6rB%E2%80%AF4W>
4. Обзор финансовой стабильности Банка России № 2. II–III кварталы 2016. С. 61. URL: http://www.cbr.ru/collection/collection/file/7861/fin-stab-2016_2-3r.pdf
5. Постановление Девятого арбитражного апелляционного суда № 09АП-31545/2021-ГК от 08.07.2021 по делу № А40-18827/17.

6. Приказ Министерства здравоохранения РФ от 30.11.2017 № 965н «Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий» // СПС «Гарант». URL: <https://base.garant.ru/71851294/> (дата обращения: 26.08.2022).
7. Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // СПС «Гарант». URL: <https://www.garant.ru/products/ipo/prime/doc/74460628/> (дата обращения: 26.08.2022).
8. Санникова Л. В., Харитонов Ю. С. Цифровые активы: правовой анализ: монография // 4 Принт. 2020. С. 118.
9. Сервис «Яндекс.Здоровье». URL: <https://health.yandex.ru/consultation/> (дата обращения: 26.08.2022).
10. Теория государства и права: учебник для юридических вузов и факультетов / под ред. С. С. Алексеева. Москва: Норма, 2005.
11. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «Гарант». URL: <https://base.garant.ru/71670570/> (дата обращения: 26.08.2022).
12. Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // СПС «Гарант». URL: <https://base.garant.ru/74451176/> (дата обращения: 26.08.2022).
13. Харитонов Ю. С. Правовое значение фиксации интеллектуального права с помощью технологии распределенных реестров. Право и экономика. 2018. № 1 // СПС «Консультант-плюс».
14. Christopher C. Chen. Regulatory Sandboxes in the UK and Singapore: A Preliminary Survey. 2019. P. 12. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3448901 (дата обращения: 26.08.2022).
15. Financial Conduct Authority. Regulatory sandbox lessons learned report. // 2017. URL: <https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf> (дата обращения: 26.08.2022).
16. Hilary J. Allen, Sandbox Boundaries // 22 Vanderbilt Journal of Entertainment and Technology Law. 2020. Vol. 22 (2). P. 301.
17. Ivo Jenik, Kate Lauer. Regulatory Sandboxes and Financial Inclusion. // Working Paper. Washington, D.C.: CGAP, 2017. URL: <https://www.cgap.org/sites/default/files/Working-Paper-Regulatory-Sandboxes-Oct-2017.pdf>. P. 13 (дата обращения: 26.08.2022).
18. Jayoung James Goo, Joo-Yeun Heo. The Impact of the Regulatory Sandbox on the Fintech Industry, with a Discussion on the Relation between Regulatory Sandboxes and Open Innovation // Journal of Open Innovation Technology Market and Complexity. 2020. № 6 (2). P. 43.
19. Lin Lin. Regulating FinTech: The Case of Singapore. 2019. URL: https://www.researchgate.net/publication/335012999_Regulating_FinTech_The_Case_of_Singapore (дата обращения: 26.08.2022).
20. What is the Sandbox? 2020. URL: <https://ico.org.uk/for-organisations/regulatory-sandbox/the-guide-to-the-sandbox/what-is-the-sandbox/> (дата обращения: 26.08.2022).

Т. Р. Гуляев,

студент,

Байкальский государственный университет

И. А. Решетников,

студент,

Байкальский государственный университет

И. Д. Скрылев,

студент,

Байкальский государственный университет

О ПРИНАДЛЕЖНОСТИ ИСКЛЮЧИТЕЛЬНЫХ ПРАВ НА РЕЗУЛЬТАТЫ, СОЗДАННЫЕ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

Аннотация. Статья посвящена исследованию проблемы принадлежности исключительных прав на результаты, созданные искусственным интеллектом. Актуальность обусловлена активным технологическим развитием в области искусственного интеллекта, а также отсутствием правовых норм, которые могут урегулировать вышеупомянутую проблему. Цель научной работы заключается в анализе данной проблемы, изучении опыта ее решения в законодательстве других государств, а также разработке научно обоснованных положений по совершенствованию действующего российского законодательства и практики его применения в области исключительных прав на результаты, созданные искусственным интеллектом.

Ключевые слова: цифровые технологии, искусственный интеллект, нейросети, авторское право, исключительное право, технологическое развитие, разработка законодательства

ON THE OWNERSHIP OF EXCLUSIVE RIGHTS TO RESULTS CREATED BY ARTIFICIAL INTELLIGENCE

Abstract. The article is devoted to the study of the problem of ownership of exclusive rights to the results created by artificial intelligence. The relevance of this work is due to the active technological development in the field of artificial intelligence, as well as the lack of legal norms that can resolve the above-mentioned problem. The purpose of the scientific work is to analyze this problem, study the experience of its solution in the legislation of other states, as well as develop scientifically-based provisions to improve the current Russian legislation and practice of its application in the field of exclusive rights to the results created by artificial intelligence.

Keywords: Digital technologies, Artificial intelligence, Neural networks, Copyright, Exclusive right, Technological development, Legislation development

Современный этап развития человечества ознаменован активным созданием и использованием информационных систем и технологий. Вместе с тем законодатели различных государств стремятся распространить правовое регулирование на эти сферы в том числе. Так, одной из важнейших тем технологической повестки не только России, но и всего мира значится создание и функционирование искусственного интеллекта (далее ИИ). Представляется, что данный вектор развития одновременно

является современным, а также футуристичным. Однако с каждым новым витком освоения ИИ появляется все больше вопросов с правовым регулированием текущей траектории, наиболее интересным является проблема принадлежности исключительных прав на интеллектуальную собственность, изобретаемую ИИ. Так, например, в Гражданском кодексе Российской Федерации определено, что исключительное право принадлежит гражданину-автору произведения науки, литературы или искусства [1]. Таким образом, появляется коллизия, когда автором является ИИ, а не гражданин, чего не предусматривают нормы действующего Гражданского кодекса Российской Федерации. Можно однозначно сказать, что стремительное развитие технологий ставит перед законодателем сложные задачи, которые требуют грамотных решений, особенно в сфере регулирования деятельности ИИ.

Изучение этих вопросов в контексте технологии ИИ является в странах Западной Европы, США и Азии актуальным направлением юридической науки и практики. В настоящее время уже существуют прецеденты создания объектов исключительного права ИИ. В основном, речь идет о создании литературных и художественных произведений. В США, например, сложился свой определенный подход в этом вопросе. Необходимо соблюсти два условия: 1) работа должна быть осязаемой, 2) работа должна быть оригинальной. В англо-саксонской правовой системе уже имеются известные прецеденты по данному вопросу: *Burrow Gilles Lithographic Co. v. Sarony* [3], *Bleistein v. Donaldson Lithographing* [8], *Alfred Bell & Co. v. Catalda Fine Arts* [7].

В деле *Burrow Gilles Lithographic Co. v. Sarony* рассматривался вопрос о приобретении исключительных прав на создание фотографии ИИ. Итоговое решение суда весьма интересное. Суд признал исключительное право за создателем машины, объясняя это тем, что создание фотографии сугубо механический результат труда, отсутствует творчество создателя. Этим решением в США значительно сузилась защита исключительных прав ИИ на созданные им объекты. В деле *Alfred Bell & Co. v. Catalda Fine Arts* заметно более снисходительное отношение. Суд посчитал, что достаточно, чтобы произведение было оригинальным и не имело схожести с другими объектами исключительного права. Опираясь на данное решение, ИИ мог бы сохранить за собой все права.

В деле *Bleistein v. Donaldson Lithographing* рассматривался сходный вопрос с *Burrow Gilles Lithographic Co. v. Sarony*. Суд разделял работу созданную, самим человеком, и результатом, созданным ИИ. Исключительное право, по мнению суда, «что-то непреодолимое, которое принадлежит одному человеку».

Интересен также опыт Европейского союза. В последние десять лет страны ЕС активно инвестируют в разработку нейросетей и ИИ в целом. Это, в свою очередь, порождает необходимость в правовом регулировании объектов, созданных не человеком. Из ключевых нормативно-правовых актов можно выделить ст. 2 Директивы 2009/24/ЕС от 23 апреля 2009 г. «О правовой охране компьютерных программ», а также ст. 4 Директивы 96/9/ЕС Европейского Парламента и Совета от 11 марта 1996 г. «О правовой охране баз данных» [5]. В этих документах указывается, что обладателем исключительных прав может являться как физическое лицо, так и группа лиц. Если же сравнивать прецеденты в американском праве, касаемо фотографий, то п. 16 Директивы 2006/116/ЕС Европейского парламента и Совета

от 12 декабря 2006 г. «О сроке охраны авторских и некоторых смежных прав» указывает на «собственное интеллектуальное творчество автора» как единственный критерий оригинальности творческого труда.

Что касается практики азиатских стран, то тут все обстоит несколько иначе и это хорошо видно на примере судебного дела Tencent v. Shanghai Yingxun Technology Company (далее SYTC) [4]. Спор между двумя этими компаниями возник по причине того, что SYTC использовала и опубликовала на своем сайте экономический отчет, написанный программой Dreamwriter – ИИ созданный Tencent. Шэньчжэньский городской суд в своем решении не согласился с позицией SYTC о том, что текст, созданный ИИ является достоянием общественности и может свободно использоваться и распространяться. Суд обязал SYTC произвести компенсационные выплаты в пользу Tencent. Исходя из вышесказанного можно открыто заявить, что дело Tencent v. Shanghai Yingxun Technology Company стало первым в судебной практике, когда суд признал, что ИИ может обладать исключительными правами на созданные им произведения.

Таким образом, из примеров США и законодательства ЕС можно сделать вывод о том, что в этих странах отсутствует регулирование исключительного права в отношении результата творчества искусственного интеллекта. Все примеры говорят о том, что необходим человеческий фактор, который определяет оригинальность работы. Однако, в Китае практика пошла по другому пути и уже сейчас мы можем видеть решения, которые показывают всю важность защиты объектов, созданных ИИ.

Исключительное право в России является одним из быстроразвивающихся институтов гражданского права. Данная отрасль развита несколько хуже, чем в странах Европы и США. Этот фактор, в свою очередь, играет немаловажную роль и в защите прав ИИ на результаты интеллектуальной собственности.

В РФ, как и в предыдущих примерах, этот вопрос остается открытым. Относительно недавно поправки в существующий ГК РФ подготовил депутат Государственной думы РФ от «Единой России» Алексей Кобилев, 21 октября 2020 года их направили на согласование в Минэкономики [2]. Инициатор поправки предложил закреплять право на интеллектуальную собственность, созданную ИИ, за их разработчиками. Анализируя законы ЕС и прецеденты США по существующему вопросу, можно выдвинуть два решения проблемы, которые в будущем могут быть реализованы уже в российском гражданском праве.

Первым вариантом является возможность оставить законодательство в существующем виде, аргументируя это тем, что в настоящее время прогресс в области разработки и улучшения ИИ не достиг нужного порога. «Машина» и ее разум еще очень далек от человеческого. Они несамостоятельны и работают по командам людей. Соответственно можно говорить об отсутствии того самого «человеческого» фактора, о котором идет речь в законах ЕС. Компьютер создает объекты несамостоятельно, а по воли человека. К тому же, ст. 1257 ГК РФ гласит: Автором произведения науки, литературы или искусства признается гражданин, творческим трудом которого оно создано, т. е. законом не предусмотрено что ИИ может быть субъектом исключительных прав. Создателем выступает гражданин, и для того, чтобы закрепить право на интеллектуальную собственность за ИИ, необходимо ввести новый некий «квазисубъект», тем самым полностью

изменив не только правовую систему РФ, но и теорию права в целом. Соответственно, на данный момент времени объекты, созданные ИИ, признаются общественной собственностью. Это, в свою очередь, может значительно замедлить развитие технологии ИИ и нейронных сетей, так как корпорациям, не получающим прибыль от реализации своего продукта, нет смысла вкладывать ресурсы в его разработку.

Второй вариант предполагает, что права на объекты, созданные ИИ, будут оставаться у разработчика или правообладателя, но это может оказаться не самым рациональным решением. Такой подход может быть актуальным в течение ближайших лет, пока достаточно мало компаний, специализирующихся на разработке и использовании данных технологий. Однако, развитие IT сектора уже создает такую ситуацию, что в экономике почти не остается отраслей, где не был бы задействован ИИ [6]. Отсюда следует, что при передаче исключительных прав на ИИ от одной компании к другой будут возникать сложности относительно того, что работы, созданные ИИ до его продажи, будут принадлежать компании-продавцу, а работы, созданные после продажи, будут принадлежать компании-покупателю. Необходимо отметить, что рано или поздно такие переходы прав от одного субъекта к другому в больших количествах приведут к тому, что найти конкретного правообладателя произведения будет достаточно сложно.

Третий вариант кажется наиболее интересным и необычным. Он подразумевает наличие исключительного права ИИ на созданные им произведения. Приобретение ИИ правосубъектности, что конечно же не будет касаться исключительных прав на сам ИИ. Сторонники такого метода объясняют его тем, что мы уже имеем подобный опыт с институтом юридических лиц. Так, юридические лица могут иметь исключительные права на достижения науки и техники, изобретения, художественные произведения и многое другое. Решения, которые принимаются на советах и собраниях юридических лиц влияют на дальнейшую судьбу этих вещей. Следовательно, можно использовать эту практику относительно ИИ. Такой прием позволит легко находить правообладателя продукта и не будет огромного количества операций по передаче исключительных прав, а также многих других проблем.

Таким образом, технический прогресс ставит вызов правовым системам различных стран, в том числе и правовой системе Российской Федерации. С каждым днем развитие ИИ набирает новые обороты. Если еще относительно недавно созданные человеком механизмы лишь исполняли заложенную в них функцию, то теперь эти механизмы на уровне алгоритмов могут примитивно, но мыслить. Голосовые помощники, программы, самостоятельно генерирующие тексты и картинки, уже создают объекты, которые нельзя урегулировать текущим законодательством в области исключительного права. И если сейчас данная проблема в меру развития технологий не является крупной, то в обозримом будущем может произойти обратное.

Полагаем, что на данном этапе развития информационных технологий уже необходимо делать первые шаги в урегулировании вопроса принадлежности исключительных прав на созданные нейросетью объекты. В подобном ключе разумным является введение правосубъектности ИИ как носителя исключительных прав. Исходя из изученной и предложенной информации, данный вектор развития является не только передовым, но и наиболее практико-применимым. Безусловно,

данная мера является достаточно серьезной в рамках правового поля Российской Федерации, однако в настоящем и будущем периоде развития права это позволит снизить риски возникновения новых проблем на почве данного вопроса, а также представит перед мировым сообществом Российскую Федерацию как государство, активно вовлеченное в освоение и правовое регулирование передовых технологий.

Список литературы

1. Гражданский кодекс Российской Федерации от 18.12.2006 № 230-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_64629/7dde8dbb10c5ce94297e5eb859712be091044d70/ (дата обращения: 12.09.2022).
2. Шестоперов Д. Что написано софтом Газета – Коммерсантъ № 206 (6927) от 11.11.2020. URL: <https://www.kommersant.ru/doc/4566144>, свободный (дата обращения: 10.09.2020).
3. Alfred Bell & Co. v. Catalda Fine Arts, 191 F.2d 99 (2d Cir. 1951).
4. Bleistein v. Donaldson Lithographing, 188 U.S. 239 (1903).
5. Burrow Gilles Lithographic Co. v. Sarony, 111 U.S. 53 (1884).
6. CJ Observer. Tencent v. Yingxun Tech // Портал законов Китая. URL: <https://ru.chinajusticeobserver.com/law/x/2019-yue-0305-min-chu-14010> (дата обращения: 12.09.2022).
7. Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs. URL: <https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:111:0016:0022:EN:PDF> (дата обращения: 11.09.2022).
8. Omdia – Informa PLC // Искусственный интеллект. URL: <https://www.tractica.com/resources/white-papers/artificial-intelligence-10-key-themes-across-use-cases/> (дата обращения: 12.09.2022).

Э. Б. Дамдинова,
студент,

Новосибирский государственный университет экономики и управления

Ю. В. Тимошенко,
студент,

Новосибирский государственный университет экономики и управления

РАСПРОСТРАНЕННОЕ КИБЕРПРЕСТУПЛЕНИЕ СОВРЕМЕННОСТИ – ФИШИНГ

Аннотация. Данная статья посвящена способам хищения персональных данных в современном мире. В представленной работе исследован один из таких способов – фишинг. На данный момент природа киберпреступления «фишинг» малоизучена и отсутствует его упоминание в нормативно-правовых актах, поэтому возникает проблема квалификации преступлений, связанных с посягательством на персональные данные. Проанализирован зарубежный и отечественный опыт.

Ключевые слова: киберпреступление, безопасность, защита персональных данных, интернет, мошенничество, фишинг, подозрительные сайты, информация

A COMMON CYBERCRIME OF OUR TIME IS PHISHING

Abstract. This article is devoted to the methods of personal data theft in the modern world. In the presented paper, one of these methods of “Phishing” will be investigated. At the moment, the nature of cybercrime “Phishing” is poorly understood and there is no mention of it in regulatory legal acts, therefore, there is a problem of qualification of crimes related to encroachment on personal data. When researching this topic, foreign and domestic experience was analyzed.

Keywords: Cybercrime, Security, Personal data protection, Internet, Fraud, Phishing, Suspicious sites, Information

В современном мире важное место в механизме функционирования постиндустриального общества занимают инновации и знания, они являются основой в сфере деятельности государства и общества. С помощью их протекают процессы в информационном пространстве.

Так во Всемирной паутине – Интернет множество людей обладают возможностью общаться, знакомиться с различной информацией. С дальнейшим развитием киберпространства отдельная часть пользователей стала использовать его для реализации своих преступных умыслов с помощью махинаций. Рост киберпреступников увеличивается пропорционально числу пользователей сети Интернет. По данным Интерпола, динамика развития киберпреступности является самой стремительной [4. С. 149–151].

Одним из распространенных киберпреступлений является фишинг. Актуальность указанной темы обусловлена тем, что данное преступление становится все более глобальной проблемой в современном мире, так как нарушается информационная безопасность личности, предприятий, что приводит к потере персональных данных, денежных средств.

В первую очередь необходимо выявить природу и сущность фишинга. Фишинг (phishing) происходит от английского слова fishing обозначая выуживание или рыбная ловля [3. С. 60–66]. Механизм работы схож с процессом рыбалки. Изучая историю развития фишинга, то впервые термин «Phishing» был зарегистрирован 2 января 1996 г. в новостях Usenet под заголовком «AOHell» [6. С. 135–141]. Жертвой кибермошенников стала известная медийная организация AOL. Мошенники представились сотрудниками компании AOL, чтобы узнать у пользователей пароли и логины от аккаунтов используя для этого программу по отправки мгновенных сообщений. Такие письма содержали просьбу от сотрудников компании о предоставлении им доступ к аккаунтам для технических работ. Однако завладев аккаунтом его использовали для распространения спама. Затем в начале 2000-х гг. фишингу стали подвергаться не только аккаунты, но и платежные системы: eBay и PayPal. В 2006 г. кибератаке подверглась социальная сеть MySpace, и у пользователей были похищены их персональные данные.

В юридической литературе дается определение фишинга как одного из видов интернет-мошенничества, преследующего целью завладение конфиденциальными данными (пароли, логины, реквизиты, учетные записи) пользователей сети. Механизм работы заключается в рассылке электронных писем на почту от имени известных брендов, компаний, банков, а также рассылкой сообщений в социальных сетях

[1. С. 69–75]. В таких письмах содержится прямая ссылка на сайт-копию, например, налоговой службы, интернет-магазинов, где необходимо произвести оплату: указать реквизиты банковской карты. Часто создают сайт-копии социальных сетей и сервисов, требующие ввести логин и пароль от аккаунтов. Указанные действия позволяют мошенникам завладеть банковскими счетами и аккаунтами. Однако многие фишеры после получения конфиденциальных данных не пользуются ими, а продают их другим мошенникам, владеющим средствами и преступными схемами для обналичивания денег [2. С. 90–93].

Сложность данного преступления требует подробного его исследования. Для этого фишинг стоит рассмотреть с нескольких сторон:

1. С юридической, потому что происходит нарушение конституционных прав граждан (право на защиту персональных данных или личной информации).

2. С психологической, так как наблюдается непосредственное влияние на психику потерпевшего, определенная степень морального вреда, нанесенный жертве в результате кибератаки. Согласно Уитти, жертвы киберпреступлений чаще соответствуют следующим критериям: они старше, имеют повышенную виктимность из-за недостаточного интеллектуального развития, неопытности в использовании Интернета, доверчивости, рассеянности и невнимательности, при наличии которых мошенник может повлиять на них [9. С. 5–7].

3. С экономической – ущерб, причиненный фишером носит материальный характер, так как цель преступника получить определенные денежные средства с банковских счетов.

Обобщая выше сказанное, фишинг можно определить, как хакерство с целью завладение персональными данными для использования в корыстных целях, т. е. фишинг выступает инструментом в руках преступника, и он является одним из наиболее распространенных и эффективных кибератак, который использует человеческий фактор [10. С. 22–35].

Стоит отметить, что фишинг имеет свои основные виды. Первым видом можно назвать – классический фишинг (фишинг подмены) включающий в себя основные фишинг-атаки. Суть его состоит в том, что преступники от имени действующей, и реально существующей компании, например, от лица платежной системы, банка, интернет-магазина и т. п. отправляют электронные письма случайным пользователем, где убеждают перейти на сайт, который ни чем не отличается от оригинального сайта компании и сделать определенные действия, например, пройти регистрацию, чтобы получить какой-то бонус [8. С. 451–455]. Все это производится с целью хищения личных данных.

Целенаправленная фишинг-атака нацелена на как определенных людей, так и на компании. Как отмечают в юридической литературе, этот вид является более глубокой вариацией фишинга, которая требует особых знаний о структуре власти организации и о ней самой [7. С. 1645–1650]. Для достижения более успешных результатов киберпреступники используют личную информацию, собранную на просторах интернета, например, из социальных сетей, сайтов, где граждане оставляют свое резюме для дальнейшего трудоустройства, затем создают мнимые знакомства, для того чтобы входящее сообщение восприняли подлинным, обращаясь, например,

по имени, отчеству используют иные личные данные. Далее после установления доверия, целевые фишинговые компании просят предоставить некоторую информацию или войти на сайт, который является либо фальшивым, либо вирусным.

Фишинг против топ-менеджмента – данный вид направлен именно на руководителей компании, которые имеют полный доступ к информационным данным компании. После получения необходимых данных у злоумышленников открывается возможность в дальнейшем использовать ее для коммуникации с другими отделами предприятия. Например, реализация мошеннических банковских переводов.

Фишинговые рассылки от Google и Dropbox – в этом направлении целью является похищение логина и пароля от облачного хранилища, где традиционно хранится конфиденциальная или корпоративная информация. Принцип работы этого вида тот же, как и у других, т. е. они создают фишинговый сайт для входа в аккаунт и отправляют ее ссылку пользователю. Однако вместо веб – сайта могут прикрепить файл, при скачивании его киберпреступники в дальнейшем смогут иметь полный доступ к компьютеру пользователя, так как в данном файле содержатся вирусные программы (трояны, вирусы шифровальщики и т. д.).

Еще один основной вид фишинга – это фарминг, он является более эффективным, так как классический фишинг легче обнаружить в отличие от фарминга. Последний вид означает скрытое перенаправление на мошеннические сайты. Схема его действия состоит в том, что на компьютер потерпевшего тем или иным способом внедряют «троянскую программу», которую не так часто могут отследить антивирусы, она заменяет данные по IP-адресам, далее пользователь перенаправляется на фишинговый сайт, где и водит личные данные. Данный вид является наиболее опасным из-за того, что его трудно обнаружить.

Таким образом, разнообразие форм фишинга говорят лишь о том, что данный вид направления киберпреступления является весьма активным и с каждым днем растет количество обманутых пользователей.

Далее обозначим проблему, которая вытекает из нашей темы. Рассматриваемое нами киберпреступление – фишинг – является интернет-мошенничеством, бороться с которым современное общество еще не может, потому что уголовное законодательство не идет в ногу с информационными технологиями из-за их быстрого темпа развития. Также при совершении преступниками определенных действий они остаются анонимными, что затрудняет расследование и делает данное преступление скрытым и весьма опасным, так как в некоторых случаях затруднительно задержать злоумышленника из-за нехватки доказательной базы. Все это приводит к уменьшению эффективности работы правоохранительных органов.

Как отмечает генеральная прокуратура Российской Федерации из-за характера сложности данного вида преступления неквалифицированные следователи и дознаватели не возбуждают уголовные дела из-за того, что отсутствуют материальные следы, а также часто при расследовании дела следствие заходит в тупик из-за отсутствия должной переподготовки работников. Впоследствии чего возрастает уровень кибермошенничества из-за не раскрытия и не выявления данного нарушения.

Изучая статьи Уголовного кодекса Российской Федерации, можно заметить, что они не охватывают в полном объеме природу и суть компьютерных преступлений, потому что нет единого понимания, осмысления такого преступления, как фишинг. Поэтому одной из причин роста фишинговых атак является несовершенство уголовного законодательства, которое заключается в том, что имеющиеся статьи о киберпреступности сложны и запутанны для понимания как для сотрудников правоохранительных органов, так и судебного разбирательства. В гл. 28 УК РФ «Преступления в сфере компьютерной информации» содержится всего пять статей: ст. 272 «Неправомерный доступ к компьютерной информации»; ст. 273 «Создание, использование и распространение вредоносных компьютерных программ»; ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»; ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»; ст. 274.2 «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования».

Также в УК РФ был дополнен ст. 159.3 «Мошенничество с использованием электронных средств платежа» и 159.6 «Мошенничество в сфере компьютерной информации», стоит заметить, названные статьи не включены в гл. 28.

Мы считаем, что рассматриваемому виду преступлений не уделяется должного внимания, так как отсутствует всеобщее толкование в нормативных документах и актах о киберпреступлениях.

Предлагаем выделить факторы, влияющие на уровень раскрываемости киберпреступления – фишинг. Первым фактором будет являться ограниченное количество статей, которые затрагивают киберпреступления. Многие правоведы отмечают, что формулировка и содержание статей довольно трудны для понимания правоприменителями. Возникают сомнения в действиях правоохранительных органов, судей из-за затруднительного, запутанного и сложного содержания статей УК РФ.

Вторым фактором выступает то, что расследованием таких преступлений (фишинга) занимаются лица, имеющие юридическое образование. В этом заключается ошибка заставляя людей указанной деятельности, в которой они слабы. Данными киберпреступлениями должны заниматься специалисты в сфере IT-технологий. В настоящее время специалистов по таким преступлениям крайне мало, несмотря на то, что идет процесс цифровизации общества. Поэтому для полной квалификации сотрудников органов, помимо высшего юридического образования, необходим опыт в работе с компьютерными технологиями. Это будет способствовать раскрытию и борьбе с киберпреступлениями, например, фишингом.

Еще одним фактором выступает мягкие, условные сроки за киберпреступность законодательством Российской Федерации. Как показывает судебная практика, за преступление в сфере фишинга могут назначить в основном штраф [5. С. 265–267].

В то же время в зарубежной практике можно выделить следующие отличительные черты: законодательство Америки предусматривает ответственность лицу, которое осуждено за киберпреступление, но повторно совершившее несанкционированное проникновение к компьютерным данным – тяжкие последствия. Такими последствиями выступает тюремное заключение сроком до 20 лет. Для сравнения Российское законодательство предусматривает максимальное наказание до 7 лет лишения свободы (ст. 272 УК РФ).

Следует то, что фишинг представляет собой серьезное киберпреступление, борьба с которым неизбежна. Для этого необходимо быть ознакомленными с мерами борьбы, чтобы снизить рост преступности. В УК РФ выделяют статьи, предусматривающие наказание за мошенничество в сфере компьютерных технологий. Однако нет нормы, которая закрепляла бы фишинг как преступление и предусматривала ответственность за него. Поэтому стоит ознакомиться с зарубежным опытом в сфере антифишингового законодательства. Так, законодательство Америки гарантирует пользователям Сети, что преступников в названной сфере ожидает более жесткая мера наказания за их деятельность (лишение свободы и штрафы в крупном размере). Пользователи сети Интернет в Америке чувствуют себя более безопасно, так как они уверены в информационной системе государства.

Это говорит нам о том, что следует ужесточить санкцию за киберпреступность, чтобы преступники всерьез приняли во внимание, что за данную деятельность последует серьезное наказание, в таком случае они не будут чувствовать безнаказанность.

В дальнейшем для профилактики фишинга с целью разрешения проблем, следует, чтобы Пленум Верховного Суда дал всеобщее толкование, что может подразумеваться под таким киберпреступлением современности, как фишинг, в форме постановления. А также дал некоторые вспомогательные рекомендации по квалификации данного преступления, что в последующем приведет облегчение работы правоохранительных и судебных органов, а также законодательно утверждает это общественно – опасное деяние. Помимо этого будет целесообразным, если сотрудники занимающиеся расследованием в сфере киберпреступлений, пройдут профессиональную переподготовку в сфере IT-технологий. Обучение кадров правоохранительных органов должно происходить с учетом специфики киберпреступлений на всех уровнях. Все это поможет увеличить скорость и качество раскрытия преступления.

Еще одним способом защиты граждан является в просвещении населения о таком преступлении, как фишинг, через СМИ, а также проводить просветительные беседы в образовательных, государственных учреждениях, что необходимо с осторожностью относиться к различным рассылкам, не поддаваться провокациям, которые используют преступники для завлечения жертвы.

Таким образом, стало ясно, что киберпреступление современности – фишинг – является опасным и достаточно тяжело раскрываемым и что уголовное законодательство требует некоторых изменений, чтобы идти в ногу со временем. Указанные способы профилактики смогут предотвратить увеличение роста преступности, что в некотором понимании обеспечит безопасность пользователей от злоумышленников и усовершенствует уголовную политику Российской Федерации.

Список литературы

1. Антонова Т. С., Смирнов В. М. Фишинг как неизученное киберпреступление // Научный журнал: StudNet. 2021. № 6. С. 69–75.
2. Батюшкин М. В. «Фишинг» – компьютерное мошенничество? // Символ науки. 2021. № 1. С. 90–93.
3. Данько О. С., Медведева Т. А. Исследование техник Фишинга и методов защиты от него // Молодой исследователь Дона. 2021. № 3 (30). С. 60–66.
4. Ермакова А. Л., Чаплыгина В. Н. Фишинг как распространенное киберпреступление современности // Закон и право. 2022. № 2. С. 149–151.
5. Ильницкий А. А. Шичкин Д. А. Компьютерная преступность. Основные проблемы раскрываемости киберпреступлений // Молодой ученый. 2022. № 19 (414). С. 265–267. URL: <https://moluch.ru/archive/414/91468/> (дата обращения: 10.09.2022).
6. Могунова М. М. Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг) // Вестник СГЮА. 2020. № 4 (135). С. 135–141.
7. Прокопайло А. А. Целевой фишинг по компьютерным и информационным наукам // StudNet. 2021. С. 1645–1650.
8. Румянцев Е. П., Найденов Н. Д. Виды фишинга и способы защиты от него // Аллея науки. 2018. С. 451–455.
9. Ilchenko O. I, Chumak V. Fishing as a Cybercrime in the Internet Banking System: Economic and Legal Aspects // Journal of and Regulatory Issues. 2019. № 2. С. 7.
10. Giustppe Desolda, Lauren S. Ferro. Human Factors in Phishing Attacks: A Systematic Literature Review // ResearchGate. 2022. С. 35.

Л. Р. Данакари,

кандидат философских наук, доцент,
кафедра педагогики, психологии и социальной работы,
Волгоградский государственный университет

К. П. Ермоченко,

магистрант,
Смоленский государственный университет

С. И. Ивентьев,

юрисконсульт, теолог, специалист в сфере
национальных и религиозных отношений,
ДЭЛИЛ

ДУХОВНО-НРАВСТВЕННЫЙ И ПРАВОВОЙ АСПЕКТЫ СВОБОДЫ ЛИЧНОСТИ В ЦИФРОВУЮ ЭПОХУ

Аннотация. Сегодня агенты цифровой эпохи нашли свое непосредственное отражение и на функционировании фундаментальных духовно-этических, философских категорий, к числу которых относится свобода личности. В данной статье она выступает предметом исследования. Цель исследования заключается в рассмотрении вопроса духовно-нравственного и правового аспектов свобо-

ды личности в цифровую эпоху. Представлено авторское определение личности. Сделан вывод, что правовое закрепление цифровых прав человека и гражданина не решает проблему полной свободы личности.

Ключевые слова: человек, личность, цифровая эпоха, права человека, цифровые права, гражданское законодательство, душа и дух человека, свобода личности

SPIRITUAL, MORAL AND LEGAL ASPECTS OF INDIVIDUAL FREEDOM IN THE DIGITAL AGE

Abstract. Today, the agents of the digital age have found their direct reflection on the functioning of fundamental spiritual, ethical, philosophical categories, which include personal freedom. In this article, it is the subject of research. The purpose of the study is to consider the issue of spiritual, moral and legal aspects of individual freedom in the digital age. The article presents the author's definition of personality. Also, it is concluded that the legal consolidation of digital human and citizen rights does not solve the problem of complete individual freedom.

Keywords: Human, Personality, Digital age, Human rights, Digital rights, Civil legislation, Human soul and spirit, Personal freedom

Свобода – благо, неволя – зло.

Народная пословица

Введение. Сегодня в условиях стремительно меняющегося мира и всех его духовно-нравственных, социально-экономических, политических и культурных процессов, которые находятся под незримо объективно сильным давлением информационного общества, вопрос личности, понятие свободы этой личности приобретают усовершенствованный и дополненный вид и обновленное понимание.

Юридизация «мира цифры и информации» и конъюнктуры «рынка цифры» в виде закрепления цифровых прав вновь на повестку дня подняла извечную проблему свободы личности.

Основная часть. Чтобы рассмотреть всесторонне заявленную тему, нам необходимо раскрыть концепт «личность».

Понятие «личность» стали использовать с появлением христианства, и оно было чуждо античному мировоззрению, так как использовалось слово «ипостась», которое «обозначало все, что обладает действительным, но совсем не обязательно одушевленным существованием» [1. С. 36–37; 11. С. 122].

Непосредственно первой вехой в христианстве в вопросе понятия и принятия личности как социоэтической категории, по мнению Ю. Я. Крамаренко, явились триадологические споры. Они преследовали цель попытаться осмыслить и понять единую троичность Бога мировоззрения [11. С. 122].

В христианстве Бога часто именуют Личностью [14. С. 72–83].

В богословии под словом «личность» понимается богодарованное уникальное начало в человеке, которое формирует неповторимый образ существования природы конкретного человека. Учитывая, что Бог есть Личность (в христианстве – три единосущные Личности), то и человек является личностью именно

в связи со своей богообразностью. Считается, что эти два понятия («образ Божий» и «личность») взаимосвязаны, но не тождественны [14. С. 72–83].

В психологической науке личность – это организованно-стойкая система индивидуально-психологических и социальных характеристик, которые составляют базовую основу структуры человеческой сущности с точки зрения ее социально-психологической природы [6].

В философии личность – персона (от лат. *persona* – «маска, роль актера») [23. С. 240].

Согласно толковому словарю русского языка, личность – человек как носитель каких-нибудь свойств; лицо [16].

Из вышеизложенного видно, что понятие «личность» отождествляется с человеком, а также связано с персональными качествами (волевыми, нравственными и другими) и социальными характеристиками. При этом к большому сожалению, понятие «личность» не увязывается с душой и духом человека и его духовно-нравственными характеристиками.

В философии и религии понятие «личность» так или иначе увязывается с лицом или ликом человека.

Если рассматривать понятие личности в плоскости учения церкви, то, как указывалось выше, первая предстает как образ Божий, запечатленный в человеке. Так, личность недоступна познанию, стремящемуся всегда быть исчерпывающим и полным.

Изучение личности человека в фокусе объекта науки не имеет такой же алгоритм рассмотрения, применимый к объектам – предметам внешнего мира. Личность всегда глубинна, непостижима и сущностно наполнена. Она неповторима, ее проявление – это всегда сокровенно-недоступное сущностное единение всей духовной структуры. Ее нельзя определить к бытийной реальности [18. С. 17].

Русский советский философ, религиозный мыслитель А. Ф. Лосев, рассматривая проблему лика, отнес его к выражению личности. При этом лик, по мнению ученого, выступает не субстанцией личности, а ее смысловым явлением и образом [15. С. 484].

По нашему мнению, верно будет под личностью понимать человека, его духовную сущность, состоящую из души и духа, обладающего индивидуальными духовными, нравственными, психологическими, социальными, интеллектуальными, физическими и другими характеристиками, компетенциями и духовно-нравственным потенциалом.

Таким образом, под личностью мыслится человек и его духовная сущность. Следовательно, в настоящем исследовании будет рассматриваться свобода человека и духовной сущности (души и духа), что ново и необычно для философии права и юридической науки в целом. В этом заключается актуальность темы статьи.

В цифровую эпоху вопрос свободы личности для полного и объективно точного его изучения необходимо рассматривать одновременно и параллельно, исходя из нравственной составляющей данной проблемы и правовой.

Нужно уметь видеть и определять необходимое наличие, противоречивое отсутствие тождественных свойств и характеристик при изучении как правового аспекта свободы личности, так и духовного и нравственного.

Современная наука располагает достаточно большим количеством полных и точных трактовок, определений понятия «свобода личности», рассмотренных с позиций различных сфер человеческой жизни.

Так, в частности, энциклопедический словарь Ф. А. Брокгауза и И. А. Ефрона с философской точки зрения под свободой понимает «возможность проявления субъектом своей воли на основе осознания законов развития природы и общества» [2].

Обобщая весь имеющийся на сегодняшний день опыт по проблеме определения сущности, структуры свободы личности, ее характерных и отличительных черт, можно однозначно утверждать, что она принципиально необходима человеку, который всегда в своих действиях и стремлениях руководствуется собственными интересами и желаниями, т. е. проявляя свой самостоятельный выбор [4. С. 1070].

Согласно Толковому словарю живого великорусского языка В. И. Даля, свобода – это «возможность действовать по-своему; отсутствие стеснения, неволи, рабства, подчинения чужой воле» [10. С. 151].

В «Философско-правовых аспектах свободы личности» В. И. Коваленко предложил собственную трактовку понятия «свобода личности». Автор сравнил ее с охраняемым благом, внутренними компонентами которого выступают:

- свободно-осознаваемое желание человека;
- ощущаемое побуждение;
- возможность реализации свободы в действительности, т. е. физический критерий;
- свобода объективизации своего волеизъявления [12. С. 15].

Эти представленные определения понятия «свобода личности» и еще множество других, которые нашли свое отражение в словарях, учебных пособиях, научных трудах, должны в информационную эпоху не просто найти свое отражение и реальное применение, а показать, что современные реалии сегодняшнего дня, в том числе и «эпоха цифры» в целом, никаким образом не влияют ни на характер структурных характеристик этого понятия, ни на способ их реальной реализации.

Этому можно дать вполне логическое объяснение. Сегодня, как бы ни развивалось общество, все его структуры, главное первостепенное место занимали и будут занимать личность человека, ее безопасность и свобода.

Категория «личность» имеет исходно-ключевое значение для правоведения, где она рассматривается в качестве носителя прав и обязанностей [21. С. 165].

Согласно концепции четвертого и пятого поколений прав человека, духовная сущность человека, его душа и дух также наделяются определенными правами и свободами, в том числе правом на информацию, творчество и свободу выбора [5. С. 62–65].

Тогда сказал Иисус к уверовавшим в Него иудеям:

«Если пребудете в слове Моем, то вы истинно Мои ученики,
и познаете истину, и истина сделает вас свободными» (Иоанна 8:31–32).

В христианстве свободу человека увязывают с Истиной или с Богом, т. е. с Абсолютной свободой.

Как указывает иеромонах Иов (Гумеров), право выбора основано на свободе человеческой воли как неотъемлемом свойстве образа Божия в человеке [17. С. 216]. При этом автор конкретизирует, что эта воля может быть ослаблена и искажена грехом, но всегда остается свободной; чем выше человек стоит духовно, тем полней проявляется эта свобода [17. С. 216].

Современная трактовка и определение понятия «воля» действующими психологами следующие: непосредственная форма психического проецирования действительности.

При этом она позволяет самой личности преодолеть все трудности и препятствия и в итоге способна достичь всех поставленных целей, которые необходимы для возможности регулирования всех действий человека, его психических процессов. Таким способом создаются все необходимые условия для осуществления волевой регуляции личности [13. С. 18].

Под волей также можно подразумевать именно силу духа человека и его души.

Если рассуждать о непосредственных формах проявления свободы, то необходимо указать на такую нравственно-этическую и философскую категорию, как выбор. Эта категория применима исключительно к человеку, так, именно он благодаря своей воле, выступающей побудительной силой, способен сделать выбор при принятии решения. Выбор и разум – две взаимосвязанные категории [24. С. 142–143].

Российский философ Л. Е. Балашов справедливо отмечает, что воля выступает регулятором и контролером человеческого поведения, которая способна управлять им [3. С. 7].

Свободу человека можно подразделить на следующие виды: абсолютную, относительную, духовную, моральную (нравственную), социальную, физическую, личную (свобода передвижения, выбора занятия, возможность поступать по своему усмотрению и своему волеизъявлению), культурную, политическую (свобода активного и пассивного избирательного права (право избирать и быть избранным)) и др. [20. С. 297–301; 22. С. 93–98].

Следует отметить, что в современном мире, к большому сожалению, человек не может обладать всей полнотой свободы, т. е. абсолютной свободой, что подтверждается следующим.

Например, в религии отмечается, что человек, который грешит, не свободен в моральном и духовном плане. Государство через законы и силу ограничивает свободу человека для установления определенных правил поведения своих граждан, а также осуществляет наказание лиц, нарушивших закон. В экономическом плане человечество не свободно от денежной системы и находится в большой зависимости от нее. Интернет породил интернет-зависимых людей. С помощью цифровых технологий можно проследить перемещение людей и товаров по миру, а также манипулировать сознанием человека и общества. Подобных примеров зависимости человека от внешних условий и неполной его свободы – большое количество.

Таким образом, в наиболее общепринятом толковании свобода характеризуется всегда отсутствием давления и насилия в любом виде (физическом,

моральном, духовном и пр.). Всякого рода ограничения человека, его духовной сущности противоречат и идут вразрез с ней.

Цифровая эпоха не просто предлагает, а навязывает свои требования к процессу функционирования общества, его отраслей, структур, систем и подсистем. Это своего рода «вирус», который постепенно проникает во все, что создавал и продолжает создавать человек, причем очень стремительно наращивая темпы этого проникновения.

Юридическая наука еще недавно не была знакома с феноменом цифровых прав (digital rights). Сегодня это не просто феномен, это законодательная новелла, которая уже нашла способ частичной реализации.

По мнению В. Д. Зорькина, цифровые права могут быть истолкованы и пониматься как право любого человека на открытый доступ к цифровым произведениям, право на их создание и использование [19. С. 340–351].

Пользование всеми информационными каналами и механизмами передачи информации также для В. Д. Зорькина является проявлением реализации сущности цифровых прав. Таким образом, автор приравнивает цифровые права к необходимости обеспечения безопасности частной информационной среды [19. С. 340–351].

Цифровые права, по мнению Р. Б. Головкина и О. С. Амосовой, не являются мерами возможного предпочтительного поведения субъектов правоотношений, а выступают формой, выражающей субъективность прав, которые нашли свое отражение в действующем гражданском законодательстве [9. С. 165].

Это далеко не все толкования данного проблемного понятия, которые предлагают нам юридическая наука и научное знание в целом. Мы можем быть согласны или быть против данных интерпретаций, но все они имеют право на существование и в совокупности в последующем способны внести ясность и дать достаточно полное объяснение данному феномену, которое найдет свое место в системе гражданского законодательства.

А пока юридическая мысль, рассматривая феномен «информационных прав», может руководствоваться Гражданским кодексом Российской Федерации, который претерпел в текущем году важные изменения в части увеличения объектов гражданских прав.

В настоящее время так называемые цифровые права стали новым объектом гражданских прав.

Так, в силу ст. 128 Гражданского кодекса Российской Федерации от 30.11.1994 № 51-ФЗ (ред. от 25.02.2022) к объектам гражданских прав относятся вещи и иное имущество, в том числе имущественные права (включая в частности, цифровые права), результаты работ и оказание услуг, результаты интеллектуальной деятельности, нематериальные блага [8].

Гражданский кодекс РФ определяет цифровые права как определенные в соответствии с правилами и требованиями всей информационной среды законо-обязательные права, режим и исполнение которых подчинены общему законодательству. В этом определении цифровые права основываются на следующих принципах:

1. Осуществление и реализация цифровых прав, их залог или передача возможны исключительно без третьего лица только в информационной системе.

2. Если человек распоряжается информационными правами на требованиях, продиктованных информационной средой, то он является их законным обладателем.

3. Переход цифрового права на условиях сделки не требует одобрения лица, которое считается обязанным по такому цифровому праву.

Цифровые права привязывают человека и гражданина к той или иной правовой системе, корпорации, т. е. создают взаимозависимую связку «цифровые права – человек – государство (корпорация)».

В юридической науке сегодня в связи с этим ведутся дискуссии. Так, например, Л. Ю. Василевская считает, что некорректно и неправильно рассматривать цифровые права в одном фокусе и одной плоскости с имущественными правами [7. С. 3–14].

Указанный автор отмечает, что процессы цифровизации и деятельность ее агентов никоим образом не способны создать новый вид информационных прав. Цифровизация лишь способна дать «информационную жизнь» современному способу фиксации прав [7. С. 3–14].

Очевидно, что цифровые права базируются на правах человека и гражданина на информацию, творчество и свободу выбора. Можно сказать, что первые конкретизируют вторые права.

Заключение. Цифровые права не могут гарантировать человеку и его духовной сущности (душе и духу) полную свободу, т. е. проблема полной свободы личности в связи с юридическим закреплением информационных прав не решается.

В ходе исследования было выявлено, что цифровая эпоха на данном этапе развития человеческого общества не решает проблему полной или абсолютной свободы личности.

Список литературы

1. Армстронг А. Х. Истоки христианского богословия. Введение в античную философию. Санкт-Петербург: Издательство Олега Абышко, 2006. 256 с.

2. Брокгауз Ф. А., Ефрон И. А. Иллюстрированный энциклопедический словарь Ф. А. Брокгауза и И. А. Ефрона. Современная версия. Москва: Эксмо, 2009. 288 с.

3. Балашов Л. Е. Этика. Москва: Дашков и Кш, 2003. 137 с.

4. Большой энциклопедический словарь. Москва: БРЭ; Санкт-Петербург: НОРИНТ, 1998. 1434 с.

5. Боброва Н. А., Ивентьев С. И. Человеческая душа как главная духовно-нравственная ценность человека // Философия человека: материалы Второго научного симпозиума, 11–12 октября 2019 г., Таганрог / отв. ред. В. П. Рыжов. Таганрог: Типография Ступина С. А., 2019. С. 62–65.

6. Ведмеш Н. А. Структура личности. URL: <https://psihomed.com/strukturalichnosti/> (дата обращения: 05.09.2022).

7. Василевская Л. В. Цифровые права как новый объект гражданских прав: проблемы юридической квалификации // Хозяйство и право. 2019. № 5 (508). С. 3–14.

8. Гражданский кодекс Российской Федерации (часть первая) // Собрание законодательства Российской Федерации. 05.12.1994. № 32. Ст. 3301.
9. Головкин Р. Б., Амосова О. С. «Цифровые права» и «цифровое право» в механизмах цифровизации экономики и государственного управления // Вестник Владимирского юридического института. 2019. № 2. С. 165.
10. Даль В. И. Толковый словарь живого великорусского языка: В 4 т. Т. 4. Санкт-Петербург: ТОО Диамант, 1996. 688 с.
11. Крамаренко Ю. Я. Личность человека в православном богословии и в психологической науке // Вестник ПСТГУ IV: Педагогика. Психология. 2006. Вып. 2. С. 122–148.
12. Коваленко В. И. Философско-правовые аспекты свободы личности // Философия права. 2016. № 6 (79). С. 11–15.
13. Конюхов Н. И. Словарь-справочник по психологии. Москва: Б. и., 1996. 160 с.
14. Леонов В. Взаимосвязь понятий «личность» и «образ Божий» в православном богословии // Сретенский сборник. Научные труды преподавателей СДС. 2010. С. 72–83.
15. Лосев А. Ф. Диалектика мифа. Москва: Правда, 1990. 656 с.
16. Ожегов С. И. Толковый словарь русского языка. Москва: Мир и Образование; ОНИКС, 2012. 1375 с.
17. 1115 вопросов священнику // Православие.Ru. 11.11.2005. С. 216.
18. Платон (Игумнов), архимандрит. Православное нравственное богословие. Сергиев Посад: Свято-Троицкая Сергиева лавра, 1994. 240 с.
19. Понкин И. В., Редькина А. И. К вопросу о понятии и онтологии цифровых прав // Пермский юридический альманах. 2021. № 4. С. 340–351.
20. Строганова Н. И. Свобода человека: философская и правовая категория // Пробелы в российском законодательстве. 2002. № 3. С. 297–301.
21. Теория государства и права: учебник / под ред. В. К. Бабаева. Москва: Юристъ, 2003. 592 с.
22. Хомелев Г. В. Философский и религиозный смысл христианского учения о свободе человека // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2018. № 1 (87). С. 93–98.
23. Философский энциклопедический словарь. Москва: ИНФРА-М, 2009. 570 с.
24. Этика / под ред. Т. В. Мишаткиной, Я. С. Яскевич. Минск: Новое знание, 2002. 509 с.

М. В. Дементьева,

студент,

Ростовский филиал Российской таможенной академии

К ВОПРОСУ О ПРИВЛЕЧЕНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ

Аннотация. В статье поднимается проблема привлечения искусственного интеллекта к уголовной ответственности. На основании анализа концепции «классического» субъекта преступления рассматриваются теоретические аспекты концепции правосубъектности искусственного интеллекта.

Ключевые слова: цифровизация, инновационные цифровые технологии, искусственный интеллект, уголовная ответственность

TO THE QUESTION OF ATTRACTION OF ARTIFICIAL INTELLIGENCE TO CRIMINAL RESPONSIBILITY

Abstract. The article raises the problem of bringing artificial intelligence to criminal liability. Based on the analysis of the concept of “classical” subject of a crime, the author examines the theoretical aspects of the concept of the legal personality of artificial intelligence.

Keywords: Digitalization, Innovative digital technologies, Artificial intelligence, Criminal liability

В современных реалиях человеческая жизнь претерпевает изменения, которые обусловлены активным внедрением инновационных цифровых технологий, появившихся в результате четвертой промышленной революции.

Ключевым достижением являются роботизированные системы, обеспеченные искусственным интеллектом. Результаты исследований в области разработки и создания искусственного интеллекта применяются практически во всех сферах жизнедеятельности общества. Он настолько плотно вошел в нашу жизнь, что по праву обрел феноменальное значение и в ряде научных исследований его определяют как искин.

В законопроекте Соединенных Штатов «О будущем искусственном интеллекте» от 2017 г. искусственному интеллекту дали следующую дефиницию: «любые искусственные системы, выполняющие задачи в изменяющихся и непредсказуемых условиях без значительного надзора со стороны человека, либо способные учиться на своем опыте и повышать свою производительность» [1].

В последние годы вопрос о возможности привлечения искина к уголовной ответственности в качестве субъекта преступления является одной из актуальнейших тем в доктрине уголовного права. Эта тема является актуальной не только для отечественного, но и для зарубежного исследователя, так как необходима разработка соответствующих положений на уровне международного права.

Да, количество преступлений по вине самообучающейся системы невелико, да и внедрение самих искинов не достигло своего экватора, однако очевидно, что

в ближайшем будущем искусственный интеллект будет модернизирован и, скорее всего, станет всеобъемлющим по сфере его применения.

Так, Рэй Курцвейл, один из представителей трансгуманизма, полагает, что «человечество быстро приближается к «технологической сингулярности» – точке, где искусственный интеллект намного превзойдет человеческий разум и сможет решать задачи, которые мы прежде были не в состоянии решить, с непредсказуемыми последствиями для цивилизации и человеческой природы». Именно по этой причине следует выработать теоретическую базу, которая поможет законодателю в регулировании данной проблемы.

Зарубежными теоретиками было сформулировано следующее мнение: «С увеличением интенсивности использования искусственного интеллекта растет вероятность противоправной деятельности. Соответственно, развитие систем искусственного интеллекта влечет необходимость реструктуризации правовой системы» [2].

Отечественные ученые также отметили, что системные исследования в области регламентации общественных отношений в сфере робототехники в России практически отсутствуют, поэтому необходима разработка основ законодательства в данной области [3].

Нельзя не согласиться с приведенными позициями. Действительно, искусственный интеллект способен приносить не только пользу, но и существенный вред. Так, такие компании как AUDI, BMW, Tesla, Toyota, UBER представляют мировому сообществу автомобили, оборудованные системой автоматического управления. Пожалуй, их главное преимущество состоит в возможности свободного от человека передвижения. Однако весной 2018 г. в Темпе (штат Аризона, США) произошло дорожно-транспортное происшествие с участием беспилотного автомобиля компании UBER, повлекшее смерть человека. Национальный совет по безопасности на транспорте США в отчете о случившемся обозначил, что причиной аварии послужил тот факт, что система автоматического вождения не идентифицировала пострадавшего, как пешехода, по причине пересечения дороги в неполюженном месте, т. е. вне зоны пешеходного перехода. Эксперты относят этот прецедент к разряду первого зафиксированного случая причинения смерти человеку в результате наезда беспилотного автомобиля. Последствием аварии стало временное приостановление испытаний робомобилей.

Следует понимать, что самообучающиеся системы применяют и в вооруженных силах развитых стран и которые, как правило, имеют вид автоматизированных систем управления (АСУ), в основу деятельности которых положен специальный алгоритм. Предположим, АСУ при сдаче в эксплуатацию и при дальнейшей диагностике не показала сбоев и неисправностей, алгоритм был внесен верно, погрешностей со стороны человека также не было допущено. Но во время военных действий система дала сбой и совершила стратегическую ошибку. Назревает вопрос: кто будет нести ответственность за причиненный вред? Как должно измениться законодательство? Какие нормы должны появиться?

Поскольку законодатель сталкивается с данной сферой впервые, может возникнуть множество проблем, имеющих отношение к определению сущности таких явлений и направлений совершенствования законодательства [4].

Так, с отечественной теоретической точки зрения субъект преступления – это физическое лицо, совершившее запрещенное Уголовным кодексом РФ общественно опасное деяние в форме действия или бездействия, и способное нести за него ответственность. Следовательно, исходя из вышеприведенной интерпретации, можно сформулировать вопросы, получив ответ на которые, можно создать концепцию правосубъектности искусственного интеллекта.

Во-первых, в России субъектом преступления может быть только физическое лицо, так как уголовный закон нашей страны, в отличие от, например, французского, не предусматривает уголовную ответственность юридических лиц, а также предметов и вещей. Следовательно, необходимо выяснить каков статус искусственного интеллекта.

Во-вторых, искусственный интеллект самостоятельно понесет ответственность за совершенное им противоправное деяние в случае сбоя в работе или же его разработчик или программист?

В-третьих, в соответствии с принципом вины, провозглашенным в ст. 5 УК РФ, лицо подлежит уголовной ответственности в том случае, если установлена его вина. К какой форме вины из существующих целесообразно отнести вину искусственного интеллекта, если у него нет ни сознания, ни воли, присущих человеку? Следовательно, возникает сложность в установлении интеллектуального и волевого критериев, разграничивающих умысел и неосторожность.

В то же время ученые из лаборатории MIT Media Lab создали нейронную сеть, которую специально обучали «мыслить» как склонную к психическим расстройствам и тягу к разрушению [5]. Предполагается, что выработанная система не способна в полной мере причинить существенный вред охраняемым общественным отношениям ввиду ограниченности проводимого эксперимента, однако феномен создания такой сети дает основание обратить внимание на имеющиеся пробелы в области правового регулирования искусственного интеллекта.

В-четвертых, способность нести ответственность за общественно опасное деяние предполагает достижение возраста, с которого наступает уголовная ответственность. При попытке привлечения искусственного интеллекта, какой категорией нужно апеллировать? Или быть может не брать во внимание этот критерий?

Приведенные выше вопросы можно отнести к числу базовых, так как их происхождение основано на нормах, существующих сегодня в отечественном уголовном законе. Мы считаем, что пока роботизированные системы, обеспеченные искусственным интеллектом, не достигнут человеческого уровня сознания и образа жизни, то следует говорить о преступлениях, совершенных посредством искусственного интеллекта, к возможным субъектам которых можно отнести: разработчика; производителя; программиста; специалиста-техника и иных лиц. Презюмируется, что «операторы» не только ответственны за исправную работу искина, но и обязаны должным образом контролировать ее (например, водитель беспилотного автомобиля должен сохранять бдительность, чтобы в случае аварийной ситуации успеть отключить автономное управление).

Кстати, стоит разграничить два типа ситуаций, когда причиной преступления является искусственный интеллект:

1. Искусственный интеллект, самостоятельно совершивший преступление ввиду сбоя в работе или внезапно возникшей поломки.

2. Искусственный интеллект, совершивший преступление ввиду взлома его программного обеспечения и децентрализации работы системы.

Следует отметить, во втором случае в качестве специального субъекта преступления будет выступать лицо, именуемое в информационном пространстве «хакер».

Важно затронуть и вопрос об объективной стороне состава преступления. На наш взгляд, искусственный интеллект способен как в полной мере, так и частично выполнить ее, причем как в форме активного поведения, так и в форме бездействия.

В случае признания искусственного интеллекта субъектом преступления следует также обратить внимание и на аспект, касающийся выбора соответствующего наказания. Так, Уголовный кодекс РФ предлагает тринадцать вариантов вида наказаний для «классического» субъекта, однако очевидно, в отношении искина их применение нецелесообразно.

Итак, инновационные цифровые технологии совершенствуются, развиваются и, несомненно, нуждаются в правовом регулировании в зависимости от сферы применения. На основании анализа норм действующего Уголовного кодекса Российской Федерации мы видим, что пока законодатель не может надлежащим образом реагировать на противоправную деятельность искусственного интеллекта в силу отсутствия соответствующих составов преступлений и норм, определяющих основания (условия) ответственности за подобные деяния.

Вместе с тем в связи с активным развитием искусственного интеллекта и внедрения его в нашу жизнь, существует настоятельная потребность уже сейчас не только поднимать данную проблему, но и искать пути выхода из нее. Так, например, можно предложить подумать о дополнении УК РФ принципиально новой главой – гл. 281 «Преступления, совершенные искусственным интеллектом и другими саморазвивающимися системами, в том числе роботами или посредством них». Следует учитывать, что возможные дополнения Особенной части Уголовного кодекса РФ должны сопровождаться изменениями и Общей части, в которой необходимо установить: условия уголовной ответственности искусственного интеллекта, критерии его виновности и его наказуемость.

Список литературы

1. Future of Artificial Intelligence Act of 2017, 115th Congress. URL: <https://www.congress.gov/bill/115thcongress/house-bill/4625/text> (дата обращения: 28.08.2022).
2. Čerka, Paulius, Jurgita Grigienė, Girbikyte Sirbikyte. Liability for Damages Caused by Artificial Intelligence // Computer Law and Security Review. 2015. № 31. Pp. 376–389.
3. Архипов В. В., Наумов В. Б. Искусственный интеллект и автономные устройства в контексте права: о разработке первого в России закона о робототехнике» // Труды СПИИРАН. 2017. № 6 (55). Pp. 46–62.
4. Мосечкин И. Н. Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления // Вестник Санкт-Петербургского университета. 2019. С. 462.
5. Norman AI. n. d. Norman. URL: <http://norman-ai.mit.edu/> (дата обращения: 28.08.2022).

Д. В. Демиденко,

студент,

Одинцовский филиал Московского государственного института
международных отношений (университета) Министерства иностранных дел
Российской Федерации

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ РЕШАЕТ СУДЬБУ ЧЕЛОВЕКА: НАШЕ БУДУЩЕЕ ИЛИ ФАНТАЗИЯ?

Аннотация. В современном мире цифровизация постепенно проникает в судебную систему, где технологии позволяют заменить человека. Поэтому цель данного исследования состоит в изучении возможности использования искусственного интеллекта в роли судьи. Освещается мировой опыт инновационных разработок в этой области, оцениваются плюсы и минусы внедрения роботов-судей, а также предлагаются выводы о перспективах развития и использования цифровых технологий для замены живых судей. Это позволяет получить представления о будущей судебной системе и жизни общества, а также избежать совершения ошибок, учитывая последствия использования искусственного интеллекта в судах.

Ключевые слова: цифровизация, право, искусственный интеллект, судья, правоотношения в суде, роботизация человеческой деятельности, будущее судебной системы

ARTIFICIAL INTELLIGENCE DECIDES PERSON'S FATE: OUR FUTURE OR FANTASY?

Abstract. Nowadays digitalisation is being gradually developed in the judiciary, so that it becomes possible to substitute technologies for people. Thus the purpose of the scientific research is to study opportunities to use artificial intelligence as a judge. The article gives world instances of some innovative solutions in this field, contains the assessment of advantages and disadvantages of adopting robots as judges, as well as provides several conclusions concerning prospects of developing and using digital technologies in order to replace human judges. It helps predict future judicial system and people's life, along with avoid making mistakes by keeping in mind consequences of applying artificial intelligence in courts.

Keywords: Digitalisation, Law, Artificial intelligence, Judge, Legal relations in a court, Robotization of human activity, Future of the judiciary

Введение. XXI в. – век цифровизации и информационных технологий. Инновации проникают буквально во все сферы общественной жизни, и даже такая самостоятельная и независимая ветвь власти, как судебная, не является исключением. Рассмотрение дела по видео-конференц-связи, допросы в онлайн формате, автоматический подбор судебной практики с помощью компьютерных программ уже довольно обычные явления. Мир не стоит на месте, и процесс цифровизации происходит активнее. Наблюдая вектор развития новых технологий, невольно

задаешься вопросом: а возможно ли, что споры и конфликты в обществе будут разрешать не уполномоченные на то люди, а роботы-судьи?

Искусственный интеллект (ИИ) представляет собой созданные человеком систему, устройство или машину, которые способны имитировать деятельность человека в соответствии с заложенными в них алгоритмами. Подобные инновационные разработки уже активно используются в различных целях (в магазинах, на заводах и др.). Даже существуют примеры применения роботов в правоотношениях, например, роботы-юристы в банках (в Сбербанке). Помимо вспомогательных участников судебной системы, обязательно существует независимый арбитр, который сможет справедливо урегулировать возникший между людьми конфликт. Работа такого субъекта правоотношений трудоемка, сложна и предполагает наличие определенных навыков и знаний, поэтому в условиях цифровизации человечество всячески пытается облегчить процесс осуществления правосудия, перекладывая те или иные функции на инновационные технологии.

Целью данной статьи является изучить возможность использования искусственного интеллекта в роли судьи, а объектом исследования выступают правоотношения, возникающие в обществе в рамках разрешения спора в судебном порядке. Актуальность работы очевидна, так как с помощью полученных результатов может стать ясным, будет ли цифровизация двигаться в направлении использования роботов-судей и стоит ли к этому стремиться. Новизна заключается в рассмотрении имеющихся попыток такого процесса, осуществленных в разных странах, и формулировании выводов, касающихся проблемы применения искусственного интеллекта в качестве судьи. На данном этапе исследования будет выдвинута гипотеза, что в будущем роботы будут использоваться вместо человека-судьи повсеместно.

Современная жизнь. Сегодня наблюдается довольно большой прорыв в области цифровизации – все больше появляется программ и устройств, упрощающих жизнь человека, во многих сферах применяются роботы. Определенные достижения сделаны и в рамках использования инновационных технологий в судебной системе.

Изучая примеры внедрения цифровых разработок в судах, следует упомянуть Эстонию, страну с одной из самых инновационно развитых в Европе судебной системой [10]. Так, уже в 2005 году правительство страны начало реализовывать идею электронных судебных дел – была создана центральная информационная система e-File [10. Digitalisation of courts]. Она предоставляет обзор разных этапов уголовного, гражданского и административного судопроизводства, рассмотрения дел, относящихся к мелким правонарушениям, процессуальных действий и судебных решений для вовлеченных сторон [12]. Известно, что в 2018 году Министерство юстиции Эстонии поручило главному директору по данным Эстонии Отту Вельсбергу (Ott Velsberg) разработать «робота-судью» для использования вместо человека в рассмотрении исков на сумму меньше 7 тыс. евро [11]. Однако в 2022 г. Министерство юстиции Эстонии пояснило, что информация о создании искусственного интеллекта для замещения человека является ложной, так как у Министерства не было планов создания подобного устройства. Вместо этого государство развивает информационно-коммуникационные технологии для снижения рабочей нагрузки на судей [15]. В перспективе планируется автоматизировать национальный порядок проведения

процедуры оплаты, которая состоит из довольно простых процессуальных этапов, но которая осуществляется в единственном отделе одного конкретного здания суда. Также существует проект внедрения системы, предполагающей применение в судах машинного обучения – искусственного интеллекта, который решает задачи и обучается опыту без непосредственных инструкций. В результате на сегодняшний день Эстония преимущественно развивает ИКТ в судах, а в рамках искусственного интеллекта разрабатываются лишь планы и проекты, затрагивающие наиболее распространенные и относительно несложные судебные дела и процедуры.

В Великобритании цифровые технологии также проникли в судебную систему – уже несколько лет действуют программы для онлайн разрешения споров (eBay, Rechtwijzer 2.0, Online Schlichter, Cybersettle и др.) [19. С. 11–16]. В 2016 году профессор Майкл Легг выдвинул идею о внедрении цифровых технологий, представляющих собой простые, опирающиеся на законодательство системы с искусственным интеллектом [17. С. 3]. А в 2022 г. в Англии и Уэльсе разрабатывается трехуровневая цифровая система правосудия по гражданским и семейным делам, а также по делам, относящимся к компетенции органов административной юстиции (трибуналов) [20. С. 1–2]. Она будет включать веб-сайт и компьютерное приложение, на которых можно будет узнать, как подать претензию. Затем заявители будут направлены на ряд порталов предварительного рассмотрения дела, после чего дело будет переходить на стадию онлайн судебного процесса, реализуемого уже сейчас для онлайн-гражданских исков о денежных средствах (Online Civil Money Claims) и онлайн-исков о возмещении ущерба (Damages Claims Online). Однако стоит подчеркнуть, что правительство рассматривает варианты использования искусственного интеллекта в судебных целях исключительно в рамках несложных и наиболее часто встречаемых дел.

Наибольший успех в области цифровизации в судах наблюдается в Китае. Так, в 2022 г. в этом государстве уже активно работает интеллектуальная судебная система System of Systems (SoS) в качестве помощника и консультанта для судей [22]. В 2014 г. данное устройство было лишь базой данных, однако сейчас SoS автоматически сканирует судебные дела на наличие ссылок, дает судье рекомендации по необходимым законам и правилам, составляет юридические документы и исправляет в приговоре ошибки, сделанные человеком [2]. Китайская разработка System of Systems стала первым в мире «судьей» с искусственным интеллектом [17]. Верховный суд страны предписал судьям консультироваться с данной системой по каждому делу, а, если судья не согласен с решениями машины, он должен в письменной форме представить свое мнение, для того чтобы устройство зафиксировало его и могло использовать в будущем [22]. Разработчики информировали о способности SoS выносить обвинения по распространенным правонарушениям – опасное вождение, воровство и мошенничество с кредитными картами [9]. Инициатором создания такого искусственного интеллекта была Шанхайская прокуратура, считавшаяся самой загруженной в Китае, но за период с 2019 по 2021 г. с помощью System of Systems было сэкономлено 1,7 млрд рабочих часов для китайских граждан [22], что наглядно демонстрирует преимущества использования подобной технологии. Однако жители Китая отнеслись к ней скептически, после чего государственный

прокурор успокоил население, заявив, что, если искусственный интеллект выносит решения с 97 % точности, это не означает, что человеческие судьи будут заменены [18. An AI that dictates verdicts]. Было подчеркнуто, что даже система с безупречными результатами может столкнуться со сбоем в программе, что недопустимо в суде, цель которого обеспечить правосудие и справедливость. Таким образом, даже в такой быстро развивающейся стране, как Китай, где уже существует так называемый «робот-судья», еще в 2017 г. стали использовать в судах первого робота Хиаофа, функция которого объяснять людям сложные юридические термины простым языком, а также отвечать на возникшие вопросы [23], и широко используется мобильный мини-суд «Mobile MiniCourt», основанный на крупнейшей китайской социальной сети WeChat [13. I. What is the «Mobile MiniCourt»], судебная система не допускает полной замены человека в роли судьи на искусственный интеллект. Инновационные достижения используются в судебных целях в Китае только в той мере, которую позволяет несложность рассматриваемых дел, простая и однотипная форма некоторых процедур, а также меньшая ответственность за их проведение.

Наше государство также продвинулось довольно далеко в области цифрового развития судов. В 2019 г. был принят Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации», который утвердил Национальную стратегию развития искусственного интеллекта до 2030 г. и стал двигателем создания инновационных технологий в разных сферах [8]. Уже в 2021 г. в России начали внедрять на участках мировых судей Ижевска робота-стенографиста АПК «Нестор.ПРАВОСУДИЕ», который хранит аудио- и видеозаписи, распознает речь участников заседаний и составляет по ней текст протокола судебного заседания [7]. Успешное тестирование и полученные положительные результаты работы робота-стенографиста побудили российское общество к внедрению робота-судьи. Так, сотрудники «Мегафон Ритейла» создали систему с использованием искусственного интеллекта, которая за два месяца использования сократила время подготовки судебного акта на 84 %, а время заполнения карточки дела – на 96 % [3]. В 2021 г. это техническое достижение установили в качестве пилотного проекта на трех мировых участках Белгородской области [4]. Искусственный интеллект готовит судебные приказы по взысканию задолженностей по имущественному, транспортному и земельному налогам, подготавливая необходимые документы и проверяя реквизиты. Председатель Совета судей РФ Виктор Момотов пояснил, что данная система не выносит самостоятельно судебные приказы, а направлена на помощь судьям и экономию их рабочего времени. Следовательно, создавая данный проект, разработчики не намеревались заменить живых судей на роботов, а лишь облегчить тяжесть их работы. На 2022 г. известно, что разрабатывается программное обеспечение для приказного производства в арбитражных судах [3. Слова Андрея Соловьева]. Более того, глава практики юридических технологий (LegalTech) фонда «Сколково» Антон Пронин подчеркнул, что уже появились технические возможности для создания более продвинутых цифровых систем с искусственным интеллектом, способных предлагать судьям предварительные решения по рассматриваемым делам на основе анализа существующей судебной практики. Тем не менее окончательное судебное решение должен принимать именно человек, а не запрограммированная машина [3. Слова Антона Пронина].

Согласно опросу, сделанному в 2021 г., 15 % российских граждан полностью согласились на вынесение судебного приговора цифровым алгоритмом, 37 % – поддержали идею роботов-судей, но предпочли, чтобы их дела рассматривали уполномоченные на то люди, а 47 % – настаивали на живом человеке в роли судьи [1]. Следовательно, более половины опрошенных (52 %) были не против искусственного интеллекта в качестве судьи. Известно также, что некоторая часть российского общества даже считает, что появление цифровых технологий сделает судебную систему честнее и справедливее. Данное изучение общественного мнения показало, что не только практическая выгода следует за внедрением инноваций в судах, но и в какой-то степени увеличивается доверие людей к системе правосудия.

Таким образом, в Китае и России уже есть протестированные в жизни роботы-судьи. Однако в первом государстве искусственный интеллект предлагал уже готовое решение по судебному делу, а в нашей стране созданное устройство только подготавливало документы для вынесения судебного приказа. Также в Китае цифровое достижение уже активно используют в деятельности судов, а Россия провела только пилотный проект, однако он оказался успешными, поэтому, предположительно, его будут внедрять в российскую судебную практику. В обоих же случаях судьи могли не согласиться с решениями машины и вынести собственное, а также системы использовались в строго определенных делах, которые не были особо сложными и редко встречаемыми.

На сегодняшний день уже есть разработки искусственного интеллекта в качестве судьи. Процесс цифровизации играет важную роль для общества, включая судебную систему, так как использование цифровых технологий в судах имеет ряд преимуществ. Во-первых, машина способна обрабатывать большой объем информации гораздо быстрее человека. То есть в процессе рассмотрения дела судебная практика и законодательство будут изучены более подробно, а решение будет вынесено с большей правильностью и справедливостью. Во-вторых, внедрение искусственного интеллекта позволит сэкономить время судей, так как рутинная и однотипная работа будет выполняться устройством. Таким образом судьи смогут уделять больше внимания и времени более важным судебным делам. Более того, рассмотрение дела цифровым алгоритмом вызывает у людей надежды, что судебный процесс будет непредвзятым и справедливым. Так, было проведено исследование, которое показало, что степень тяжести судебного приговора зависит от того, как долго у судьи не было перерыва и перекуса [24]. В Израиле, например, оказалось, что более серьезное наказание назначалось в делах, рассматриваемых за час до обеда и за час до конца рабочего дня судьи [21]. Очевидно, что у робота нет усталости и чувства голода, поэтому судебные решения не будут зависеть от внешних и второстепенных факторов, а использование искусственного интеллекта приведет к осуществлению правосудия, которое может осуществляться в любое время, так как у цифровой системы не предполагается наличие законно установленного периода рабочего времени и ежегодных отпусков. Также робот-судья действительно выступает независимым арбитром в споре, так как он выносит решение преимущественно на основе фактов и положений законодательства. Использование механизма в качестве судьи исключает возможности, что судье просто станет жалко

виновного или он будет подкуплен. Стоит отметить, что искусственный интеллект как судья не нуждается в выплате ежемесячной заработной платы, что позволяет государству сэкономить государственные денежные средства, предполагаемые на зарплату судьям, и перенаправить их на улучшение жизни населения, на другие, не менее важные общественные цели. Конечно, приобретение робота-судьи является дорогостоящим событием, однако в будущем оно окупится и принесет пользу не только судебной системе и обществу, обеспечивая справедливость судопроизводства, но и государственному аппарату в финансовом аспекте.

Тем не менее есть и некоторые недостатки внедрения искусственного интеллекта в суды. Так, существует большое количество случаев, когда программы цифровых механизмов были взломаны злоумышленниками. В контексте судебной системы недопустимо, чтобы кто-либо мог оказывать влияние на решение робота-судьи, ведь тогда может быть наказан невиновный человек, что категорически противоречит целям судопроизводства. Также сложно сказать, кто будет нести ответственность за неправильный судебный приговор, вынесенный машиной, что может негативно повлиять на мнение населения о правосудии. Не менее важным является то, устройство не способно в полной степени понять и оценить человеческие чувства, а это может иметь значение в процессе принятия окончательного решения. Судьи опираются порой не только на законодательство и судебную практику, но и на собственный жизненный опыт. А роботизированный судья лишен этой способности, а следовательно, предрасположен к назначению иногда слишком суровых наказаний, строго следуя заложенному в него алгоритму. И наконец, искусственный интеллект принимает решения на основе имеющейся судебной практики, но в случае появления особого случая, ранее не встречаемого дела или новых общественных отношений неизвестно, каков будет результат работы системы. Изучение вынесения машиной судебного заключения показало, что робот-судья принимает менее правильное решение, рассматривая дело, ранее отсутствующее в прошлом, так как в алгоритме не могут быть заложены будущие события [16].

Таким образом, использование искусственного интеллекта в качества судьи имеет как плюсы, так и минусы. Однако человечество лишь недавно начало исследовать данную область, поэтому однозначного мнения на введение роботов-судьей нет. Тем не менее на сегодняшний день уже существуют действующие системы и механизмы с искусственным интеллектом, выполняющие судебные функции, и такие инновационные достижения показывают довольно положительные результаты. Сегодня многие развитые страны начали разрабатывать подобные цифровые технологии, осознавая пользу и преимущества их использования. Важно подчеркнуть, что существующие примеры судебных систем с искусственным интеллектом внедряются для строго определенных дел и задач, так как не все судебные процедуры могут быть автоматизированы. В Китае – дела о воровстве, мошенничестве с кредитными картами и опасным вождением; в России – подготовка судебных приказов о налоговых взысканиях; проект Великобритании затрагивает гражданские и семейные процессы, а также дела, рассматриваемые в трибуналах; планы Эстонии – автоматизировать процедуру оплаты и развивать информационно-коммуникативных технологий. Заметно, что ни одна из перечисленных стран

не намеревается полностью заместить живых судей на искусственный интеллект, а также не рассматривает возможность использования роботов-судей для серьезных и сложных судебных дел.

Заключение. В данной статье были рассмотрены примеры внедренных и разрабатываемых в разных странах технологий с искусственным интеллектом для использования в качестве судей. Их изучение позволяет сделать вывод, что применение роботов-судей действительно возможно, однако стоит подчеркнуть, что подобные достижения цифровизации не могут использоваться для всех судебных процедур и задач. Были упомянуты проекты Китая, России, Великобритании и Эстонии, каждый из которых отличается кругом рассматриваемых дел и выполняемых функций. Тем не менее общим является то, что ни одна страна не «доверила» искусственному интеллекту трудные дела, решение которых может серьезно повлиять на судьбу человека и изменить его жизнь.

В работе были отмечены достоинства и недостатки использования роботов-судей, что позволяет более полно оценить перспективы данного процесса. Так как человечество только начинает знакомиться со способностями искусственного интеллекта в судебной системе, еще нет достаточного количества отзывов о результатах этого направления цифровизации. Однако, изучив плюсы и минусы, можно утверждать, что технологии, рассматривающие типичные судебные дела и выполняющие рутинные судебные задачи, значительно снижают рабочую нагрузку живых судей, а также обрабатывают информацию быстрее и порой успешнее, что улучшает процесс судопроизводства. Вышеперечисленное ведет к тому, что инновационные разработки дают возможность уполномоченным людям более подробно и качественно рассматривать сложные и запутанные дела. Тем не менее нельзя забывать, что любой механизм может допустить ошибку, дать сбой и вынести слишком суровое заключение, оценив только объективные факты и положения законодательства, поэтому наличие человека, способного всесторонне изучить обстоятельства и все тонкости случая, проверить решение цифровой системы и при необходимости принять иное, является необходимым.

Пример дела Эрика Лумиса показывает недостатки использования инновационных технологий, работающих по заложенному алгоритму [11]. В 2016 году мужчина был приговорен Верховным судом штата Висконсин к шести годам тюремного заключения за вождение автомобиля, который он арендовал, но который ранее был использован для совершения правонарушения со стрельбой. Приговор был вынесен по рекомендациям программного обеспечения COMPAS, принимающего решение на основе опроса из 137 вопросов. Лумис пытался оспорить решение суда, так как ни он, ни его адвокат не могли высказать свою позицию и опровергнуть доводы программы, что являлось нарушением конституционного права на надлежащую судебную процедуру было нарушено. Однако в 2017 г. Верховный суд США отклонил его ходатайство. Данное дело показывает, что судебная система предполагает совмещение справедливости и человечности, а искусственный интеллект не всегда способен в полной мере их обеспечить, поэтому живые судьи остаются неотъемлемым элементом судов. Конечно, роботы значительно упрощают процесс осуществления правосудия, однако их нельзя использовать для всех судебных целей.

Ассоциированный профессор ПАО «МТС» по эмпирико-правовым исследованиям Дмитрий Скугаревский и ассоциированный профессор по социологии права им. С. А. Муромцева Европейского университета в Санкт-Петербурге Кирилл Титаев в статье «Спасут ли роботы-судьи российскую судебную систему» подчеркивают, что цифровые технологии должны улучшать жизнь общества и выступать помощниками для людей в осуществлении их рабочих задач [6]. То есть роботов-судьей следует использовать преимущественно для облегчения нагрузки живых судей путем перекалывания на устройства и машины выполнения примитивных, элементарных и рутинных задач.

Некоторые специалисты считают, что искусственный интеллект нельзя использовать в качестве судьи в уголовных делах. Так, доктор юридических наук Роберт Абдулин заметил, что только человеку, имеющему необходимые знания и жизненный опыт, следует выносить окончательный приговор [5]. Машина же может указать на найденные ошибки в протоколе и документах или предложить судье предварительное решение, но последнее слово должно быть за человеком. Поэтому российский профессор утверждает, что никогда искусственный интеллект не сможет заменить живых судей, но подходящим для него местом может быть роль судебного секретаря. Однако иностранный эксперт Теренс Маури предположил, что к 2070 году роботизированные механизмы будут выполнять функции не только судебных секретарей, но и солиситоров, помощников юристов, судей в мировые и окружные суды, а также в рассмотрении некоторых семейных споров. Но искусственный интеллект не заменит высших судей и барристеров, так как их участие в судебном заседании обязательно: судьи устанавливают прецеденты, принимают некоторые законы и рассматривают апелляции, а барристеры выступают в суде в защиту интересов своих клиентов [14].

Таким образом, цифровые технологии предоставляют уникальную возможность разгрузить работу судей, тем самым позволяя уполномоченным людям сконцентрировать внимание и силы на выполнении более важных, сложных и трудоемких задач. Некоторые страны начали разрабатывать системы с искусственным интеллектом для простых судебных дел, а в некоторые уже добились определенных успехов: например, Китай запустил помощника-консультанта для судей в делах об опасном вождении, воровстве и мошенничестве с кредитными картами, а Россия успешно протестировала систему, подготавливающую судебные приказы по взысканию имущественных, транспортных и земельных налоговых задолженностей. Искусственный интеллект в судах имеет плюсы и минусы, поэтому специалисты считают, что цифровизацию следует направлять в сторону внедрения его для выполнения несложных судебных процедур и задач, однако нельзя допускать замещения человека в рассмотрении более важных, запутанных или новых судебных дел. Очевидно, в будущем искусственный интеллект будет встречаться в качестве судьи в типовых, элементарных делах, где участие человека как арбитра может быть минимизировано. Не все люди готовы к тому, чтобы разрешение их споров и конфликтов зависело от решения устройства, особенно если это может повлиять на судьбу сторон. Поэтому можно предположить, что в перспективе роботы-судьи будут внедряться постепенно и для тех судебных дел, которые стали довольно обычными и постоянными и решение которых можно в той или иной степени предвидеть в силу их частой встречаемости.

Судья занимает важное место в судебной системе, так как он должен независимо и непредвзято оценивать обстоятельства дела, принимать во внимание не только факты и законы, но и эмоциональное состояние людей, принимать правильное решение и обеспечивать справедливость в обществе. Данная работа очень сложна и требует как знаний и навыков, так и наличие многих других, важных составляющих, что не допускает полной замены человека на роботов. Алан Карлсон, юридический консультант и вышедший на пенсию судебный исполнитель Высшего окружного суда в Калифорнии, подчеркнул, что человечество должно понимать, где необходимо соблюдать границу между технологиями и человеком [21].

Список литературы

1. «Сделает суды честнее»: 18 % россиян выступили за появление судей-роботов // Ruposters. 2021. December. URL: <https://ruposters.ru/news/10-12-2021/vistupili-royavlenie-sudeirobotov> (дата обращения: 21.08.2022).
2. В Китае искусственный интеллект начал помогать судьям выносить приговор // Российский интернет-портал и аналитическое агентство «TAdviser». 2022. URL: <https://www.tadviser.ru/a/678914> (дата обращения: 19.08.2022).
3. Анастасия Синченкова. Робот-судья: реальность или фантастика – решали на ПМЮФ-22 // Право.ru. 2022. Июль. URL: <https://pravo.ru/lf/story/241675/amp/> (дата обращения: 21.08.2022).
4. В России искусственный интеллект привлекли к вынесению судебных решений // РИА Новости. 2021. Май. URL: <https://ria.ru/20210525/intellekt-1733789200.html> (дата обращения: 21.08.2022).
5. Пичурина В. Сможет ли робот заменить судью // Российская газета. 2019. Ноябрь. URL: <https://rg.ru/amp/2019/11/12/reg-urfo/smozhet-li-robot-zamenit-sudiu.html> (дата обращения: 25.08.2022).
6. Скугаревский Д., Титаев К. Спасут ли роботы-судьи российскую судебную систему // Ведомости. 2019. Декабрь. URL: <https://www.vedomosti.ru/opinion/articles/2019/12/19/819082-spasut-roboti-sudi> (дата обращения: 25.08.2022).
7. Российские IT-решения внедрили в мировых судах Ижевска по цифровому нацпроекту // Группа компаний ЦРТ. 2021. Январь. URL: <https://www.speechpro.ru/media/news/21-01-2021> (дата обращения: 21.08.2022).
8. Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // Официальный интернет-портал правовой информации. 2019. Октябрь. URL: <http://publication.pravo.gov.ru/Document/View/0001201910110003?index=0&rangeSize=1> (дата обращения: 21.08.2022).
9. Aditya Tarar China made the world's first artificial intelligence-equipped judge, gives 97 percent of the decisions right // Hindustan News Hub. 2021. December. URL: <https://hindustannewshub.com/world-news/china-made-the-worlds-first-artificial-intelligence-equipped-judge-gives-97-percent-of-the-decisions-right/?amp=1> (дата обращения: 19.08.2022).
10. Anett Numa Artificial intelligence as the new reality of e-justice // e-Estonia. 2020. April. URL: <https://e-estonia.com/artificial-intelligence-as-the-new-reality-of-e-justice/> (дата обращения: 20.08.2022).

11. Atanu Biswas A robot in a judge's chair // The Statesman. 2021. December. URL: <https://www.thestatesman.com/opinion/robot-judges-chair-1503031697.html/amp> (дата обращения: 20.08.2022).
12. e-File // RIK / Centre of Registers and Information Systems. URL: <https://www.rik.ee/en/international/e-file> (дата обращения: 20.08.2022).
13. Guodong Du (杜国栋), Meng Yu (余萌) Chinese Courts on Smart Phones // China Justice Observer (中司观察). 2021. June. URL: <https://www.chinajusticeobserver.com/a/chinese-courts-on-smart-phones> (дата обращения: 19.08.2022).
14. Jonathan Chadwick Robots that analyse body language to determine guilt 'with 99 % accuracy' will replace human judges in 50 years, expert claims // Daily Mail Online. 2020. October. URL: <https://www.dailymail.co.uk/sciencetech/article-8858753/amp/Robot-judges-replace-humans-courtroom-50-years.html> (дата обращения: 25.08.2022).
15. Maria-Elisa Tuulik Estonia does not develop AI Judge // Republic of Estonia. Ministry of Justice. 2022. February. URL: <https://www.just.ee/en/news/estonia-does-not-develop-ai-judge> (дата обращения: 20.08.2022).
16. Masha Medvedeva Using machine learning to predict decisions of the European Court of Human Rights // SpringerLink. 2020. January. URL: <https://link.springer.com/article/10.1007/s10506-019-09255-y> (дата обращения: 22.08.2022).
17. Michael Legg The Future of Dispute Resolution: Online ADR and Online Courts // Australasian Dispute Resolution Journal. 2016. С. 3. URL: Legg, Michael, URL: <https://ssrn.com/abstract=2848097> (дата обращения: 20.08.2022).
18. News Desk China: Robot judges, an AI that hits 97 % of verdicts in virtual courts // Paris Beacon News. 2022. March. URL: <https://www.parisbeacon.com/63267/amp/> (дата обращения: 19.08.2022).
19. Online Dispute Resolution Advisory Group Online Dispute Resolution for Low Value Civil Claims // Civil Justice Council. 2015. February. С. 11–16. URL: <https://www.judiciary.uk/wp-content/uploads/2015/02/Online-Dispute-Resolution-Final-Web-Version1.pdf> (дата обращения: 20.08.2022).
20. Sir Brian Neill The Society of Computers and Law // Courts and Tribunals Judiciary. 2022. March. С. 1–2. URL: <https://www.judiciary.uk/wp-content/uploads/2022/03/MR-to-SCL-Sir-Brain-Neill-Lecture-2022-The-Future-for-Dispute-Resolution-Horizon-Scannings-.pdf> (дата обращения: 20.08.2022).
21. Stephanie Condon AI in the court: Are robot judges next? // ZDNET. 2020. January. URL: <https://www.zdnet.com/home-and-office/kitchen-household/best-robot-mop/> (дата обращения: 22.08.2022).
22. Tanmay Kadam China's AI-Enabled 'Smart Courts' To Recommend Laws & Draft Legal Docs; Judges To Take Consult AI Before Verdict // The EurAsian Times. 2022. July. URL: <https://eurasianimes.com/chinas-ai-enabled-smart-court-to-recommend-laws-judges/> (дата обращения: 19.08.2022).
23. Xin Wen Robot gives guidance in Beijing court // Chinadaily.com.cn. 2017. October. URL: https://www.chinadaily.com.cn/china/2017-10/13/content_33188642.htm (дата обращения: 19.08.2022).
24. Zoë Corbyn Hungry judges dispense rough justice // Nature. 2011. April. URL: <https://www.nature.com/articles/news.2011.227> (дата обращения: 22.08.2022).

Е. И. Дружинина,

студент,

Новосибирский государственный университет экономики и управления

Д. А. Шабалина,

студент,

Новосибирский государственный университет экономики и управления

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ЖИЗНИ СОВРЕМЕННОГО ОБЩЕСТВА

Аннотация. В статье рассматривается проблема внедрения и использования искусственного интеллекта, а также юридические аспекты данного вопроса на примере иностранных государств и Российской Федерации. Особое внимание уделяется нарушению прав и свобод человека искусственным интеллектом. Устанавливается необходимость дополнительного регулирования не только самих информационных алгоритмов, но и специально уполномоченных лиц.

Ключевые слова: искусственный интеллект, цифровое право, информация, персональные данные, права и свободы, частная жизнь, ответственность

ARTIFICIAL INTELLIGENCE IN THE LIFE OF MODERN SOCIETY

Abstract. The article discusses the problem of the introduction and widespread use of artificial intelligence, as well as the legal aspects of this issue, using the example of foreign states and the Russian Federation. Special attention is paid to the violation of human rights and freedoms by artificial intelligence. In this connection, the need for additional regulation is established not only of the information algorithms themselves, but also of specially authorized persons.

Keywords: Artificial intelligence, Digital law, Information, Personal data, Rights and freedoms, Privacy, Responsibility

Тема совместимости искусственного интеллекта (далее – ИИ) с правами человека далеко не нова. Искусственный интеллект – это не далекое будущее, он уже плотно обосновался в нашей жизни, хотя многие до сих пор не понимают, что это и есть он. Например, часто заходя на различные сайты, мы видим предупреждение, что используются файлы cookie, которые собирают данные, чтобы сделать сайт более удобным в использовании. Так же появляется и целевая реклама, которая ориентируется на интересы одного покупателя. Все эти данные собираются и анализируются искусственным интеллектом через заданный алгоритм. Огромное значение ИИ для нас имеет его высокая производительность и эффективность.

Но насколько законен это сбор данных? Что если ИИ собирает те данные, которые человек не хотел бы сохранять и хранить в базе данных, и будет ли это означать вмешательство в частную жизнь?

Право на неприкосновенность частной жизни – основополагающее право каждого человека, однако мы сами предоставляем немало персональных данных при использовании приложений и социальных сетей, а они, синхронизируясь между

собой, передают эту информацию друг другу. Мы сообщаем информацию разного рода, начиная от здоровья и семейного положения, заканчивая политическими и религиозными убеждениями, не представляя, зачем, кем и каким образом будут использоваться эти данные.

На самом деле, когда дело касается дачи соглашения или разрешения в интернет-пространстве, зачастую большинство людей не читают предоставляемый договор. Например, в 2010 г. был случай, когда магазин видеоигр GameSteishtel на своем сайте выпустил лицензионное соглашение, которое ничем не отличалась от старого, кроме одной строчки, в которой говорилось о передаче «бессмертной души в безвозмездное пользование магазина», однако в этом же пункте так же было оговорено, что пользователь может отказаться от этого, перейдя по ссылке. В итоге шуточного соглашения 88 % пользователей «продали душу» магазину, и это в очередной раз доказало, что большинство люди не читают соглашения перед согласием. Тогда на что же мы еще соглашаемся, сами того не зная, и могут ли это использовать против нас? Это была всего лишь шутка магазина, но она показала всю безалаберность людей в данном вопросе.

Возможностью воспользоваться невнимательностью сможет и искусственный интеллект, тем самым нарушая границы частной жизни человека, или же и вовсе не спрашивая разрешения.

Манипулирование данными происходит на постоянной основе, ведь мы создаем одну учетную запись, а после синхронизируем все устройства с ней, начиная с обычного компьютерного программного обеспечения и заканчивая программой умного дома. Тем самым все больше и больше данных поступает в распоряжение ИИ. Умные часы запрашивают информацию о состоянии здоровья, различные сайты рабочий и семейный статус, практически везде требуется ФИО дата рождения, пол, почта и номер телефона, иногда это даже адрес проживания и паспортные данные и т. п. И удаляя учетную запись на сайте, в приложении, нет полной уверенности в том, что все эти данные и правда уничтожаются. Таким образом, со временем появляется целое досье на пользователя информационного пространства.

Иногда даже не нужно предоставлять определенную информацию, ИИ сам способен вычислить, например, этническую идентичность или политические взгляды, опираясь на данные местоположения и различные предпочтения.

Таким образом, опираясь на всю полученную информацию, искусственной интеллект начинает решать за нас, что нам подходит, а что нет, это уже можно считать вторжением в частную жизнь, которое медленно может перерасти в социальное угнетение. Иначе говоря, мы слепо руководствуемся тем, что нам подбирает ИИ, это сказывается на правах человека.

Почему речь зашла о социальном угнетении, ведь искусственный интеллект создан для того, чтобы наоборот облегчить жизнь людей? Все верно, благодаря алгоритму, ИИ в самом деле подбирает нам самые «выгодные» предложения, однако это лишает нас права попробовать что-то другое. Проще говоря, в системе ИИ отсутствует разнообразие.

Один из положительных моментов ИИ называют его объективность, но не стоит забывать, что алгоритмы для ИИ программируют люди, соответственно,

в систему случайно, или же осознано, могут быть включены человеческие предубеждения, которые можно считать дискриминативными. Вопреки мнению, что ИИ может самостоятельно думать, решения ИИ представляют собой лишь результат сложения и вычитания изначально заданных паттернов.

Так, например, было замечено, что в зависимости от пола, алгоритм подбирает возможные вакантные рабочие места, т. е. на лицо происходит нарушение прав равенства.

Известны случаи использования ИИ в судебных процессах, но из-за того, что его мыслительные процессы состоят лишь из статистических выводов корреляции, то выданный результат может быть расово, религиозно или социально дискриминативным. Самая известная корреляция – тождество низкого уровня дохода и склонность к преступной деятельности. Естественно, что в ИИ будет прописан этот паттерн, т. е. схема-образец выявления закономерностей. Так же, например, схема борода – мусульманство – угроза, как известно, именно бородатых мужчин чаще всего просят пройти на личный досмотр в аэропортах.

Распознавание лиц давно уже является болезненной темой в обществе. ИИ все больше и больше используется для наблюдения, поиска и отслеживания. Немало людей придерживаются мнения, что подобная практика неприемлема, ведь это фактически слежка за человеком. Помимо всего прочего, вся эта информация становится частью больших данных, что, конечно же, не многим понравится.

Лицо, как и голос, это уже не просто персональные данные, а биометрия, это уже совсем иной уровень идентификации личности и иной уровень опасности, номер телефона, паспортные данные, место проживания и имя – все это можно сменить, а вот биометрические данные – нет.

Предоставление такой информации ИИ может поставить под угрозу анонимность человека. Лишь однажды разблокировав лицом телефон или включив камеру на ноутбуке, эти данные отправляются в базу данных, откуда обычный пользователь ее достать уже не может.

ИИ не просто собирает и хранит информацию, но и классифицирует, дает свои оценки и ранжирует, на это не требуется отдельного согласия и оспорить это никак нельзя. Например, в Китае действует балльная система социального рейтинга граждан, где система распознавания лиц превратилась в самого настоящего Большого Брата, бросил мусор мимо урны – минус баллы. В зависимости от количества баллов, накладываются ограничения или же предоставляются привилегии, зачатки ли утопии или антиутопии нам лишь предстоит узнать.

В 2017 г. в Стэнфорде нейросеть научили распознавать сексуальную ориентацию человека, и нейросеть показала результаты с точностью до 80 %. Ей достаточно было считать эмоции и особенности мимики. Что это, как не прямое вмешательство в частную жизнь?

Но нельзя отрицать и положительное влияние искусственного интеллекта на общество, поэтому для устранения подобных проблем и их предотвращения нужно следовать принципу должной осмотрительности. Иначе говоря, все участники создания подобных систем должны проявить должную осмотрительность для обеспечения уважения прав и свобод человека [6. С. 41–62.].

В современном мире для человека уже естественно соблюдать права других, будь то под влиянием внутренних убеждений или внешних ограничений. Однако, это нельзя отнести к искусственному интеллекту, потому что как бы не бились над этим специалисты, наделить ИИ человечностью не получается и вряд ли получится, поскольку все эмоции и ощущения даны человеку от рождения и создать их искусственно не представляется возможным. Именно поэтому все действия и решения ИИ, так или иначе, будут индифферентны по отношению к человеку и обществу в целом.

Общество на данном этапе своего развития плотно загнано в рамки прав, которые, без всяких сомнений, обеспечивают порядок и комфорт, поэтому появление такой непредсказуемой в своей деятельности переменной, как искусственный интеллект, может создать определенный хаос в кропотливо выстраиваемой системе.

Так каким же образом ограничить искусственный интеллект, тем самым обезопасив человека? Специалисты ИИ говорят о наложении определенных запретов в ядро ИИ, однако, если верить их же словам, то он способен учиться, а значит придет время, когда он сможет обойти все эти запреты [1. С. 130–146].

Невозможно так же применить к искусственному интеллекту словосочетание «юридическая ответственность», поскольку он не осознает вину за содеянное. Таким образом, из цепочки выпадает важнейший элемент состава правонарушения – вина.

Другой вариант – понести ответственность за неправомерную деятельность искусственного интеллекта должен производитель или же оператор, такой точки зрения придерживается Парламентская Ассамблея Совета Европы.

В целом группа европейских экспертов еще в 2019 г. опубликовало отчет об ответственности за искусственный интеллект и другие появляющиеся технологии. Суть отчета в том, что стоит острая необходимость разработать режимы юридической ответственности за действия искусственного интеллекта. В отчете уже присутствует базовая терминология и первичные принципы ответственности [7].

Для того чтобы избежать самой вероятности правонарушений со стороны ИИ, самым разумным и логичным вариантом, исходя из всего, является обязательное внедрение механизма человеческого контроля. Иначе говоря, человек должен иметь право, а главное, возможность отключать алгоритмы, переписывать функционал, т. е. иметь необходимые компетенции для контроля. Однако даже с такими предосторожностями невозможно избежать прецедентов правонарушения ИИ, поэтому вопрос юридической ответственности остается на повестке дня.

Отставание законодательства от технологий совершенно понятно, поскольку загнать в рамки закона то, что без остановки прогрессирует, довольно непросто. Именно поэтому существует особый правовой режим, называемый «регуляторной песочницей», в котором можно тестировать инновации, вопреки законодательным ограничениям. В 2020 г. Михаил Мишустин утвердил перечень таких технологий для «песочницы» (Постановление Правительства Российской Федерации от 28 октября 2020 г. № 1750), в этот список также вошел и искусственный интеллект. Такой правовой режим обычно устанавливается на срок до трех лет в определенных регионах, где разработчики тестируют свои разработки, чтобы доказать эффективность своих инноваций, не будучи загнанными в рамки. Внедрение подобной практики поможет совершенствовать законодательство с учетом темпа роста технологий.

Тема правового регулирования искусственного интеллекта невероятно обширна, требуется уделить внимание таким аспектам, как:

- конфиденциальность данных, получаемых ИИ при взаимодействии с пользователем;

- работа с большими данными, несмотря на то, что у нас уже принят Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О защите персональных данных». Но, как уже говорилось ранее, технологии прогрессируют с такой скоростью, что разница даже в год создает большую пропасть, не говоря о почти двадцати годах, поэтому этот закон также требует корректировки;

- безопасность прав человека и ответственность за правонарушения со стороны ИИ;

- этническая сторона вопроса использования искусственного интеллекта.

В процессе развития общества происходит модернизация и развитие передовых технологий, что в свою очередь непосредственно влияет и на применение искусственного интеллекта во всех отраслях общественной жизни, в том числе и в праве. Применение искусственного интеллекта в праве и в процессах, сопутствующих ему, не является чем-то новым и передовым, однако, как показывает практика, не многие страны стремятся ввести их в повсеместное применение.

Рассматривая международные случаи применения искусственного интеллекта в праве, следует обратиться к опыту Китая, который уже довольно долгое время так или иначе стремится облегчить деятельность правоохранительных органов посредством введения ИИ.

Так, с 2015 г. китайские суды были привлечены к проекту под названием «Умный суд». В его основе лежит идея объединить информационные системы судов в одну базу, и предоставить судам открытый доступ к базам данным полиции, прокуратуры и иных правоохранительных органов [8. С. 60–62]. Цель данного проекта заключается в унификации имеющихся материалов проверок, судебных разбирательств и иных процессуальных проверок. Свободный доступ судов к базам сократил время необходимое для запроса материалов из полиции и прокуратуры.

Также китайские судьи с 2022 г. обязаны консультироваться с ИИ, однако следует отметить, что не ставится вопрос о самостоятельности ИИ в вопросе вынесения судебного решения. В данном случае искусственный интеллект наделен следующими полномочиями: проверка документов на наличие и правильное оформление юридических ссылок, а также формулирует список нормативно-правовых актов, в том числе законов и постановлений, необходимых в использовании для процессуальных действий. Подобные введения в китайскую систему правосудия не умаляет основные принципы права такие как объективность принятия решений и независимости, однако возлагает на судью обязанность проведения контроля ИИ на наличие ошибок в проведенных расчетах.

В то же время нейросети активно используются и в США, однако уже в несколько иной сфере, а именно для сбора статистических данных, которые в последующем используются для составления «криминальной истории» и социально-демографической характеристики.

Составление криминальных историй необходимо в рамках информации о конкретном субъекте, т. е. информация о его судимостях, привлечении в качестве

обвиняемого, подозреваемого, свидетеля и др. В свою очередь социальная-демографическая характеристика, такие данные как возраст, пол, занятость в совокупности с криминальной историей используются правоохранительными органами посредством ИИ с целью прогнозирования возможности повторного совершения преступления. В данном алгоритме прописаны возможные наказания, которые коррелируются не только в зависимости от тяжести совершенного преступления, но и от характеристики личности обвиняемого и наличия или отсутствия в его жизни ранее совершенных преступлений.

Однако в отличие от опыта Китая в США использование системы ИИ не является обязательным, а остается на усмотрение судьи.

Следует отметить, что встает вопрос об объективности использования данного алгоритма. С одной стороны, использование ИИ дает возможность учитывать все смягчающие и отягчающие обстоятельства при вынесении приговора, исключает предвзятость судьи по отношению к обвиняемому, однако с другой стороны ИИ является той системой, которая не застрахована от ошибок, а вносимые в нее данные не являются абсолютными

Е. А. Войниканис выделяет явный минус системы ИИ, суть которой заключается в выявленной дискриминации, иными словами программа с учетом вводных данных о национальности выносит более строгие наказания афроамериканцам, а с учетом вероисповедания – мусульманам [2. С. 586–589].

Искусственный интеллект также применяется в европейских странах в частности в Германии, чей опыт несколько схож с китайским в рамках использования ИИ для формирования обвинительного заключения в рамках использования нормативно-правовых актов. В частности, германская система судопроизводства пока нацелена лишь на обучение ИИ, а не повсеместное применение.

Главная идея судов Германии, выделяемая учеными разрабатывавшими ИИ, состоит в том, чтобы алгоритм на основании имеющихся данных выдавал средний размер наказания для каждого дела в отдельности, в первую очередь такую систему хотят использовать для назначения штрафов [5. С. 74–79].

Однако на практике встречаются некоторые проблемы в реализации данной системы: если у американцев данные уже преподносятся в почти готовом виде, то немцам приходится создавать трудоемкую систему экстракции данных из судебных приговоров.

Обращая внимание на отечественный опыт следует отметить, что по объему вложений в развитие ИИ Россия входит в первую пятерку.

В соответствии с Указом Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» под искусственным интеллектом в России понимается как комплекс технологических решений, позволяющих имитировать когнитивные функции человека, и который наделен возможностью самообучения [3].

С нашей точки зрения, внедрения немецкого подхода в российскую систему возможно с внесением нескольких изменений, в частности внести возможность пресечения неправомерных мер. Первоначально необходимо спроектировать такую систему, которая могла бы лишь показывать судебную практику на основании

вменяемого преступления или проступка, а лишь потом создать алгоритм, который бы уже выработывал средние значения наказания.

Если же обращать внимание на американскую систему, то необходимо составить среднестатистический профиль преступника, а лишь потом провести анализ и выявить какие признаки правонарушителя проявляются в той или иной ситуации, в зависимости от места, времени и иных сопутствующих обстоятельств.

Дальнейшее сопоставление правонарушителя и среднестатистического портрета должны сопоставляться, и чем больше лицо соответствует статистическим данным, тем строже ему назначается наказание.

Так сфера применения ИИ в правовом поле России достаточно обширна: дорожное движение, система распознавания лиц, составление процессуальных документов. Следует отметить, что все вышеперечисленные случаи использования ИИ не является повсеместным на территории РФ, а лишь только в отдельных регионах в рамках правовых экспериментах.

Однако следует отметить, что ряд ученых указывают на возможность сокращения количества рабочих мест в правоохранительных органах. Однако, в противовес данному утверждению, уже другие правоведы отмечают, что без наличия понятия «человека» в праве невозможно будет добиться соблюдения основных принципов, гарантирующих основные права и свободы человека [1. С. 130–146].

Прогноз исчезновения ряда профессий в правовой сфере невозможно предсказать ввиду того, что развитие информационных технологий продолжается и с каждым годом происходит расширение баз данных и создаются новые алгоритмы.

Использование ИИ в правовой сфере не всегда представляется возможным ввиду того факта, что машина не является человека, она может анализировать, делать выводы, однако она никогда не начнет чувствовать и сопереживать потерпевшим, обвиняемым и другим лицам. Ввиду этого искусственный интеллект лишен возможности определять психологическое состояние лица, его мотивы и цели. У компьютера нет потребностей и эмоций, нет социальной ориентации, он никогда не станет разумным.

Однако, учитывая то, что некоторые страны уже имеют опыт передачи ИИ полномочий по вынесению приговоров, встает вопрос о законности таких решений и деликтоспособности. Перенимая практику иностранных государств, РФ должна в первую очередь законодательно урегулировать возможности и запреты использования искусственного интеллекта, в том числе должно установить ответственность человека за злоупотребление такими системами.

Так, можно установить следующие ограничения, которые помогут избежать потери контроля и необоснованности принятых решений искусственным интеллектом:

1) необходимо запретить использование вторичных алгоритмов, т. е. тех систем, которые были созданы самим ИИ, т. е. человек первоначально не имеет возможность влиять на действие вторичного алгоритма;

2) ввести ответственность лиц за неправомерное вмешательство в алгоритмы искусственного интеллекта;

3) итоговое решение всегда должно оставаться на усмотрение правоохранительного органа;

4) запретить самообучения робота, так как возможно попадание в систему недостоверных данных. Любое обучение должно осуществляться под руководством специально обученного человека;

5) любое принятое решение искусственным интеллектом должно сопровождаться официальным юридическим актом.

Все предложенные выше меры ИИ должны послужить неким гарантом того, что алгоритм не выйдет из-под контроля человека, который в свою очередь отвечает всем необходимым юридическим и технологическим знаниям.

Однако в предложенной концепции имеется несколько существенных минусов: не каждый юрист имеет IT-образование; введение системы контроля возложит на юристов дополнительные обязанности и увеличит объем бюрократизма, что в свою очередь нельзя допустить, ведь первостепенная цель внедрения ИИ в правоприменительный процесс заключается в оптимизации [2. С. 586–589].

Следует отметить, что не все сферы права пригодны для того, чтобы внедрить использование ИИ, так как возможные ошибки в системе будут наносить существенный неблагоприятный ущерб лицу, в отношении которого выносится решение.

В свою очередь ряд авторов выдвигают некоторые сферы права, в которых использование технических алгоритмов будет связано, например, не с назначением наказания в виде лишения свободы, а с назначением штрафа [6. С. 41–62].

Однако имеется диаметрально противоположное мнения касательно нужности и эффективности использования ИИ, все противоречия, которые встречаются на пути к ведению повсеместного использования ИИ заключается в вопросе обеспечения безопасности и ответственности за неправомерное стороннее вмешательство в алгоритм.

Таким образом, выделяется необходимость правоприменителей уделить внимание конфиденциальности данных, которые будут собираться как на основании эмпирических данных, официальных, предоставленных самими субъектами. Не стоит забывать и о безопасности, которая в век информационных технологий не всегда осуществима, а кибератакам подвергаются и правительственные сайты; это так же соблюдение прав и свобод человека и гражданина; обеспечить процесс оспаривания решения вынесенного ИИ.

Федеральный закон от 27 июля 2006 г. № 152 «О персональных данных» обращает внимание на необходимость обезличивания персональных данных, которые используются ИИ для обработки информации, однако такой процесс возможен только в исследовательских целях, что в свою очередь исключает использование этих данных уже для непосредственного принятия решения [4].

Границы тех или иных прав были установлены давно, однако, прогрессивный рост цифровых технологий заставляет немедленно разрабатывать и принимать новые законы, способные идти в ногу с технологиями и обеспечить безопасность прав человека.

В недалеком будущем будет достаточно лишь показать человека ИИ, чтобы составиться полное досье, начиная от ФИО, телефона, адреса проживания и заканчивая эмоциональным и психическим состоянием, сексуальной ориентацией и социальным положением. ИИ приносит немалую пользу, однако существует опасность того, что собранные им данные могут быть использованы против вас. Перед обществом стоит вопрос, готовы ли мы пожертвовать частью своих прав на,

возможно, более комфортную и эффективную жизнь. Без всяких сомнений, искусственный интеллект расширяет наши возможности, но и он может их и ограничить.

Список литературы

1. Войниканис Е. А., Семенова Е. В., Тюляев Г. С. Искусственный интеллект и право: вызовы и возможности самообучающихся алгоритмов // Вестник ВГУ. Серия: Право. 2018. № 4 (35).
2. Крысанова Н. В. Правовые вопросы искусственного интеллекта // Россия: тенденции и перспективы развития. 2021. № 16–1. С. 586–589.
3. О развитии искусственного интеллекта в Российской Федерации: Указ Президента Российской Федерации от 10.10.2019 № 490. URL: <http://www.kremlin.ru/acts/bank/44731/page/1> (дата обращения: 05.09.2022).
4. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ // СПС «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 05.09.2022).
5. Hildebrandt M. The Artificial Intelligence of European Union Law // German Law Journal. 2020. Vol. 21, № 1. Pp. 74–79. URL: <https://doi.org/10.1017/glj.2019.99> (дата обращения: 09.09.2022).
6. Raso F., Hilli-Goss H., Krishnamurthy V., Bavitz C., Kim L. Artificial Intelligence & Human Rights: Opportunities & Risks // Berkman Klein Center for Internet & Society research publication. 2018. С. 41–62. URL: https://dash.harvard.edu/bitstream/handle/1/38021439/2018-09_AIHumanRights.pdf (дата обращения: 10.09.2022).
7. Report of High-Level Expert Group on Artificial Intelligence // An official website of the European Union. 2019. URL: <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence> (дата обращения: 11.09.2022).
8. Roberts H., Cows J., Morley J., Taddeo M., Wang V., Floridi L. The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation // AI & SOCIETY. 2021. С. 60–62. URL: https://www.researchgate.net/publication/342246048_The_Chinese_approach_to_artificial_intelligence_an_analysis_of_policy_ethics_and_regulation (дата обращения: 09.09.2022).

Д. А. Дудкин,
адъюнкт,

Академия управления Министерства внутренних дел
Российской Федерации

ПУБЛИЧНО-ПРАВОВЫЕ И ЧАСТНОПРАВОВЫЕ СВОЙСТВА ЦИФРОВЫХ ТЕХНОЛОГИЙ, ПРИМЕНЯЮЩИХСЯ В РАМКАХ ОКАЗАНИЯ ДЕТЕКТИВНЫХ УСЛУГ

Аннотация. Статья посвящена выявлению проблем, которые раскрывают публично-правовые и частноправовые свойства цифровых технологий, применяющихся в рамках оказания детективных услуг, на основе правовых свойств детективной деятельности как публично-правового, так и частноправового характера.

В реалиях сегодняшнего времени, в том числе в условиях появления кибервойны как особого вида информационной войны, вопрос безопасности государства, а также граждан и их имущества в информационном поле и киберпространстве становится особенно острым.

Ключевые слова: информационная война, цифровизация, частный сыск (поиск), детективная деятельность

PROBLEMS OF THE COMPETITIVE ENVIRONMENT IN THE PROVISION OF DETECTIVE SERVICES IN THE RUSSIAN FEDERATION

Abstract. The article is devoted to the identification of problems that reveal the public-legal and private-law properties of digital technologies used in the provision of detective services, based on the legal properties of detective work, both public-legal and private-law. In the realities of today's time, including in the conditions of information warfare, as well as with the emergence of cyber warfare as a special type of information warfare, the issue of the security of the state, as well as citizens and their property in the information field and cyberspace becomes especially acute.

Keywords: Information warfare, Digitalization, Private investigation (search), Detective work

В реалиях сегодняшнего времени, в том числе в условиях информационной войны, а также с появлением кибервойны как особого вида информационной войны вопрос безопасности государства, а также граждан и их имущества в информационном поле и киберпространстве становится особенно острым. С началом специальной военной операции Россия столкнулась с беспрецедентным по масштабам информационным вторжением, для которого были активизированы значительные ресурсы Запада. В том числе к противостоянию подключились крупные интернет-компании, чья аудитория насчитывает сотни миллионов людей по всему миру.

Информационная война – это война без правил, война без видимых разрушений и порой даже без четко определенного противника. Разнообразие применяемых в ней методов бесконечно, а ключевая опасность состоит в том, что воздействие на отдельного человека может долгое время оставаться незамеченным. Более того, одна из главных особенностей информационной войны заключается в возможности многократного «захвата» одной и той же аудитории, без четкого осознания факта «захвата» самой аудиторией.

Признаки информационной войны можно обнаружить еще в Античности, и по мере развития коммуникаций росло ее влияние на человеческую цивилизацию. Сейчас мы лишь проходим очередную острую фазу противостояния, которое тянется уже несколько десятилетий и периодически достигает условной точки кипения. Отличие в том, что сейчас удар оказался настолько массивным, что его в той или иной мере ощутили практически все трансляторы и потребители информации, и некоторые оказались к нему попросту не готовы. В условиях цифровизации информации частные детективы вынуждены выстраивать свою деятельность в новом режиме.

Среди проблем следует отметить конкурентные преимущества государственных органов (МВД и др.) и пользователей, разработчиков частных поисковых программ перед частным детективом, которые проявляются в правах и обязанностях, т. е. в содержании правоотношений. В структуре этого основания отчетливо видится два преимущества. Первое из них связано с запретом частным детективам оказывать услуги, не включенные в перечень ст. 3 Закона РФ от 11.03.1992 № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации» (далее – Закон о частном сыске) [4]. Второе преимущество заключается в правомочиях вышеуказанных субъектов по проведению поиска информации, людей, имущества с применением баз данных, в то время как частный детектив на законных основаниях не имеет такой возможности, что в свою очередь не позволяет надлежащим образом оказать сыскные услуги. Причем интересен тот факт, что если частный детектив в процессе оказания сыскных услуг будет вынужден использовать специальные программы для поиска, то фактически становится пользователем частных поисковых программ.

На сегодняшний день отсутствуют полноценные исследования, которые раскрывают публично-правовые и частноправовые свойства цифровых технологий, применяющихся в рамках оказания детективных услуг. Стоит, однако, отметить, что Минтрудом был утвержден новый профессиональный стандарт, в соответствии с которым теперь в России будут готовить специалистов по поиску и анализу данных цифрового следа [5]. Цифровой след, как можно догадаться, – это те данные, которые человек оставляет за собой во Всемирной сети, его разнообразные аккаунты, посты и прочие элементы паззла, из которого можно составить целостную картину личности, а не только выяснить то, что сам гражданин о себе говорит.

Разумеется, подобные возможности в первую очередь очень интересуют спецслужбы, однако потенциальное применение анализа цифрового следа неизмеримо шире. Например, HR сможет таким образом узнать гораздо больше о потенциальном сотруднике (особенно если это ответственная должность в госорганах), учебные заведения – о студентах, сыщик – о гражданине и его имуществе и т. д.

По сути, такие анализы уже давно проводятся, в основном по материалам социальных сетей и открытых источников. Однако теперь этим профессионально будут заниматься специально обученные люди, которые будут опираться на понятные алгоритмы, а не только на собственный опыт.

Однако проблема законодательного закрепления расширения полномочий частных детективов остается, а в условиях цифровизации информации, даже обостряется. По сути, потребность в поиске обозначена, должность разработана, а полномочия и субъект поиска не обозначен в законодательстве.

Стоит отметить, что до сих пор не существует всестороннего исследования термина сыскной (поисковой) деятельности как процесса оказания детективных услуг, выражающегося в определенном виде услуг, допустим в части поиска пропавших граждан, имущества или информации [2. С. 80–85].

Основное содержание частноправового аспекта заключается в вовлечении людей в исследуемую сферу путем заключения договоров и применения саморегу-

лирования. Например, ученые отмечают, что благодаря договорным отношениям реализуется и опосредуется предпринимательская инициатива сторон [1. С. 8–12].

Аспект социального характера проявляется в достаточно высокой степени воздействия детективной деятельности на решения государственных задач социальной направленности, а также в содействии публично-правовой правоохранительной функции государства. Такое содействие может быть реализовано частными детективами исключительно в рамках гражданских правоотношений, т. е. в процессе осуществления детективом своих гражданских прав в соответствии с Законом о частном сыске.

Реальная сторона данного положения заключается в его методологической основе, позволяющей выявить двойственную правовую природу этого термина, проявляющуюся в аккумуляции публично- или частноправовых свойств. Интерес такой методики заключается в том, что в состав элементов поиска могут быть включены публично-правовые или частноправовые элементы.

Примером проявления публично-правовых элементов могут служить приложения для отслеживания – поиска контактов с заболевшими COVID-19 при поддержке государства, которые были разработаны во многих странах [8], но еще в недостаточной степени получили развитие в процессе оказания детективных услуг. Исследователи из Оксфордского университета пришли к выводу, что такие приложения способны оказать существенную помощь в борьбе с инфекцией [9].

Иными словами, меры, предпринимаемые государством к защите персональных данных и минимизации рисков, не были решающим фактором для принятия решения об использовании приложения. В данном контексте заслуживает внимания специальное руководство, принятое в 2020 г. Европейским советом по защите данных, в который входят представители всех национальных органов по защите персональных данных [10]. Гораздо более значимыми оказались социальные, психологические и культурные факторы. Можно сказать, что граждане не чувствовали социальную ответственность и как результат пришлось жертвовать приватностью для пользы обществу.

Также примером публично-правовых свойств могут являться действия специальных органов власти, таких как МВД, ФСБ, СК, и регламентируются как правоохранительная функция государства, т. е. деятельность государства, осуществляемая с целью охраны права уполномоченными органами с применением мер воздействия при безусловном соблюдении установленного ими порядка [3. С. 13].

В свою очередь примером частноправовых свойств может служить наличие договорных отношений с частным детективом или приобретение программы для приватного поиска, что является одним из критериев частного сыска [7. С. 135]. Благодаря договорным отношениям реализуется и опосредуется предпринимательская инициатива сторон [1. С. 8–12], которая направлена на получение материальной выгоды.

Таким образом, профессиональная сыскная деятельность (профессиональный сыск) представляет собой отдельный, самостоятельный вид социально значимой человеческой деятельности, осуществляемый государственными органами,

юридическими и физическими лицами для достижения определенных целей и решения задач в порядке, установленном законодательством, важное специфическое средство поставки информации потребителю.

Список литературы

1. Андреев В. К. Сделка и ее недействительность // Юрист. 2014. № 1. С. 8–12.
2. Дудкин Д. А. «Поиск без вести пропавших граждан» и «Поиск утраченного гражданами или предприятиями, учреждениями, организациями имущества» как виды сыскных услуг, востребованных на современном этапе гражданского оборота // Сборник научных трудов 4-й Международной научной конференции: Государство и право: проблемы и перспективы совершенствования. Курск, 2021. С. 80–85.
3. Лукичев Ю. А. Проблемы дисциплины «Правоохранительные органы» // Право и образование. 2017. № 4. С. 13.
4. О частной детективной и охранной деятельности в Российской Федерации: Закона РФ от 11.03.1992 № 2487-1 // Российская газета. № 100. 30.04.1992.
5. Об утверждении профессионального стандарта «Специалист по моделированию, сбору и анализу данных цифрового следа»: приказ Минтруда России от 09.07.2021 № 462н (Зарегистрировано в Минюсте России 30.07.2021 № 64502) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 19.09.2022).
6. Шаронов С. А. Понятие, правовая природа и классификация оказания охранных услуг как объекта гражданских прав в контексте осуществления предпринимательской охранной деятельности // Вестник Санкт-Петербургского университета МВД России. 2018. № 2. С. 126–130.
7. Шумилов А. Ю. Феномен научных школ профессионального сыска: монография. Москва: ИД Шумиловой И. И., 2007. 159 с.
8. Contact tracing apps: A new world for data privacy. Norton Rose Fulbright. 2021, February. URL: <https://www.nortonrosefulbright.com/ru-ru/knowledge/publications/d7a9a296/Africa#South> (дата обращения: 15.09.2022).
9. Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown. University of Oxford. 2020. April. URL: <https://www.research.ox.ac.uk/article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown> (дата обращения: 15.09.2022).
10. Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. The European Data Protection Board, adopted. 2020. April. URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en (дата обращения: 15.09.2022).

В. Э. Дюмина,

магистрант,

Санкт-Петербургский государственный университет,
помощник генерального директора АО «ЛенОблАИЖК»
по правовым вопросам

ПАРАДИГМА ЧАСТНОГО ПРАВА В ИННОВАЦИОННУЮ ЭПОХУ: ЦИФРОВОЙ ОБРАЗ ПРОИЗВЕДЕНИЯ КАК НОВЫЙ ОБЪЕКТ ГРАЖДАНСКИХ ПРАВ

Аннотация. В рамках данной работы рассмотрена необходимость расширения перечня объектов гражданских прав путем добавления новой сущности – цифрового образа произведения. Основная сложность заключается в отсутствии единого теоретического подхода к базовым вопросам, связанным с цифровой средой, и недостаточной научной проработки данной области. Целью работы является не только обоснование идеи о необходимости включения в часть первую Гражданского кодекса РФ (далее – ГК) дополнительного объекта гражданских прав, но и введение общих теоретических понятий, выработка единого понимания природы цифровых объектов. Особенно актуальна данная тема для института интеллектуальной собственности, выступающего ключевым ресурсом новой (цифровой) экономики, а также для новых цифровых активов.

Ключевые слова: право, цифровой образ, цифровая экономика, новый объект гражданских прав, инновационные технологии, NFT, искусство, цифровые активы

PARADIGM OF PRIVATE LAW IN THE INNOVATIVE AGE: DIGITAL IMAGE OF A WORKS AS A NEW OBJECT OF CIVIL RIGHTS

Abstract. As part of this work, the need to expand the list of objects of civil rights by adding a new entity – the “digital image of the work” will be considered. The main difficulty of the study is related to the lack of a unified theoretical approach to basic issues related to the digital environment, and insufficient scientific study of this area. In this connection, the purpose of this work is not only to defend the idea of the need to include an additional object of civil rights in part one of the Civil Code (hereinafter referred to as the Civil Code), but also to introduce general theoretical concepts, develop a common understanding of the nature of digital objects. This topic is especially relevant for the institution of intellectual property, which is a key resource of the “new” (digital) economy, as well as for new digital assets.

Keywords: Law, Digital image, Digital economy, New object of civil rights, Innovative technologies, NFT, Art, Digital assets

Развитие инновационных технологий обуславливает появление новых институтов, требующих законодательного регулирования. Многие открытия и достижения влияют не только на социальную среду общества, но и охватывают все сферы человеческой деятельности, становятся востребованными в гражданско-правовом обороте. Следовательно, активный прогресс требует вмешательства законодателя и адаптации правовой среды к веяниям времени.

Однако проблема заключается в отсутствии необходимой для гражданского оборота в условиях цифровой экономики правовой базы и неэффективности законодательного регулирования цифрового рынка с учетом современных тенденций цифровизации интеллектуальной собственности, что порождает разрозненность судебной практики и, как следствие, незащищенность прав авторов оригиналов произведений и авторов цифровых «копий» (цифрового образа произведения).

Цифровизация права и экономики обуславливает появление новых объектов гражданского оборота [6. С. 21–28], отличающихся от классических не только формой существования, но и конститутивными признаками. Появление целого ряда цифровых технологий, которые получили широкое распространение, существенным образом влияет на гражданско-правовой оборот и требует доктринальной проработки. При этом, анализ правовых источников по данной теме показал, что поставленная проблема мало исследована в доктрине, отсутствуют адекватные предложения о внесении законодательных изменений, вопреки очевидным разногласиям в сфере цифрового взаимодействия, что также свидетельствует об актуальности и новизне данной работы.

Так, Non Fungible Token (NFT) или невзаимозаменяемые токены, о которых пойдет речь в настоящем исследовании, являются уникальными, «индивидуальными кодами» [12, 13]. Именно разработка технологии NFT дала возможность конвертировать произведения искусства в цифровую среду и говорить о новом объекте гражданских прав – цифровом образе произведения.

Вместе с тем, NFT является частью более общего понятия – цифровые активы. Под цифровыми активами, в свою очередь, в контексте настоящей работы будут пониматься криптоактивы, большие данные (Big Date), доменные имена, аккаунты, виртуальное имущество [6. С. 21–28], а также активы, включающие цифровой образ произведения. При этом, вопреки высказанным в литературе мнениям [10], не следует определять цифровые активы как «все, что может храниться и передаваться в электронном виде» [2. С. 201], поскольку смысл выделения отдельной категории активов связан не с тем, что классические объекты гражданских правоотношений обретают новую форму, а с тем, чтобы предоставить правовую охрану уникальным цифровым объектам, не имеющим материальных аналогов. Именно поэтому важна концептуальная проработка цифрового образа произведения, с учетом его сложной дихотомичной природы, где творческое начало заменяется уникальной цифровой формой, которая, по существу, становится неотъемлемой частью содержания произведения, индивидуализируя его в цифровой среде. В то же время некорректно ставить вопрос о целесообразности закрепления на уровне закона понятия цифровых активов, которое охватывало бы все разнообразие новых цифровых объектов, поскольку это приведет к усугублению тех проблем, которые есть сейчас с закрытым перечнем объектов гражданских прав и с размытым определением цифровых прав.

На сегодняшний день оборот невзаимозаменяемых токенов практически никак законодательно не урегулирован и упорядочивается только конкретной платформой, на которой выпустили NFT, что порождает риски для авторов, правообладателей и иных участников оборота, желающих приобрести права на цифровые активы. При этом, невзаимозаменяемые токены подтверждают права только на цифровой образ произведения, а не на сам объект искусства. Так, пользователю, купившему

NFT, не принадлежат исключительные права на произведение, т. е. между покупателем цифрового образа и создателем оригинального арт-объекта нет никакого соглашения, исключительные права остаются за автором.

Это уточнение имеет принципиальное значение, поскольку цифровой образ произведения, будучи цифровой «копией» материального объекта интеллектуальных прав, не сводим к материальной форме и не может быть преобразован в нее. Цифровой образ возникает как объект и существует непосредственно в информационной среде, обладает принципиальными отличиями технологического характера и является отдельным объектом, права на который обеспечиваются невзаимозаменяемыми токенами.

Таким образом, в отличие от произведения, созданного изначально в цифровой форме (цифрового произведения) и оцифрованного (или машиночитаемого) произведения, которое, напротив, создается в материальной форме, но в дальнейшем конвертируется в цифровую среду, цифровой образ произведения представляет собой нечто иное. На произведение, созданное изначально в цифровой форме, должны распространяться все положения части IV ГК РФ, точно так же, как и на оцифрованное произведение, так как никаких существенных особенностей, требующих отступления от традиционного института защиты авторских прав не возникает. Иная ситуация складывается при создании объекта с помощью технологий блокчейн. Цифровой образ произведения не может считаться цифровой копией произведения, поскольку такая модификация не предполагает сохранение формы и основных характеристик. Цифровой образ становится как бы вторым оригиналом, существующим в цифровой среде и индивидуализируемым с помощью NFT.

Сказанное выше иллюстрирует важные технологические и юридические особенности, отражающие правовую природу цифрового образа произведения. Данные отличительные характеристики подтверждают уникальность нового актива, но не развеивают сомнений касательно его правовой сущности, места и роли среди других правовых явлений, в частности, вопрос: можно ли отнести цифровой образ произведений к объектам гражданских прав, остается открытым.

В рамках системы блокчейн, позволяющей обеспечить владение, пользование и распоряжение максимально индивидуализированными токенами (NFT), объектом правоотношений будет являться поведение участников сети по обороту цифровыми образами произведений. Характеристика объекта таких правоотношений сама по себе не позволяет проанализировать природу цифрового образа произведения как самостоятельного объекта гражданских прав, однако, поскольку цифровой образ произведения обладает стоимостными характеристиками (экономической ценностью) и полезными свойствами, такие правоотношения имеют предмет, по поводу которого складываются, и должны порождать права и обязанности сторон, в них вступающих. Но для того, чтобы обосновать данное положение необходимо перейти к рассмотрению цифрового образа произведения в рамках системы объектов гражданских прав.

Прежде всего следует обратиться к доктринальному определению самого понятия объекта права. Так, Г. Ф. Шершеневич считал, что объект права – это «все то, что может служить средством осуществления интереса» [9. С. 121], а Д. И. Мейер

понимал под объектом права то, что подлежит господству лица как субъекта права, при этом такие «вещи» должны состоять в гражданском обороте и представлять собой какую-либо ценность [3. С. 367]. В связи с этим не любой объект, полученный в результате использования цифровых технологий, может быть отнесен к объектам гражданских прав, а лишь тот, который обладает экономической ценностью, реальной или потенциальной [14].

Перечень объектов гражданских прав закреплен в ст. 128 ГК РФ и формально является закрытым, однако в теории гражданского права не прекращаются споры по этому поводу. Суть дискуссий сводится к тому, что, во-первых, отсутствует единое определение объекта гражданских прав, во-вторых, нет единого мнения по поводу исчерпывающего характера перечня [5. С. 31]. Разногласия возникают из-за отсутствия конкретных формулировок и широких пределов усмотрения при толковании нормы (см. Определение Конституционного Суда РФ 2014 г. № 1350-О «Об отказе в принятии к рассмотрению жалобы гражданина Гинеевского В. А. на нарушение его конституционных прав статьей 128 ГК РФ»). Следует отметить, что в зарубежных правовых системах как определение, так и перечень объектов отсутствуют (ФРГ, Французская Республика и др.), что представляется в большей степени отвечающим современным тенденциям, поскольку более рационально определить основополагающие свойства и принципы объектов гражданских прав, а не вводить каждый раз новые сущности, стараясь сохранить перечень исчерпывающим.

С другой стороны, до момента признания нового объекта гражданских прав *ex lege* (прямым указанием закона), присутствуют сомнения касательно правовой природы указанного объекта. Законодатель осознает важность развития цивилистической мысли и модифицирует формулировки ст. 128 ГК, что по большей части обусловлено политико-правовыми целями. Так, в 2006 г. из числа объектов была исключена информация (см. ст. 17 Федерального закона от 18.12.2006 № 231-ФЗ «О введении в действие части четвертой Гражданского кодекса Российской Федерации»), а в 2019 г. вновь были внесены изменения: безналичные денежные средства и бездокументарные ценные бумаги были включены в категорию имущественных прав, а также появился новый объект – цифровые права (см. ст. 1 Федерального закона от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации»).

Основными критериями легитимации объектов гражданских прав в правовой системе РФ служат два положения, выделяемые в доктрине. Во-первых, способность объекта удовлетворять экономические блага, что чревато междисциплинарной сложностью применения данного критерия, в связи с необходимостью определения экономических признаков. Во-вторых, необходимость правовой охраны. Последний критерий включает в себя в том числе: ограниченность объекта в обороте, возможность реального господства над объектом и вероятность нарушений права обладания (владения, пользования, распоряжения) объектом. Цифровой образ произведения соответствует данным критериям, поскольку он может быть идентифицирован с помощью технологий блокчейн, которые помимо этого обеспечивают владение (господство) над цифровым образом произведения и оборот таких активов.

Одновременно эти же признаки цифрового образа произведения как самостоятельного объекта права потенциально создают почву для столкновения интересов различных лиц и возникновения споров о нарушении их прав. Об этом свидетельствует, например, спор Государственного Эрмитажа с вокалистом и автором песен немецкой группы Rammstein Тиллем Линдемманном, который выпустил серию «эрмитажных токенов» без согласования с музеем.

Таким образом, анализ направлений цивилистической мысли был необходим для правильного понимания системы объектов гражданских прав и возможности логически обоснованного добавления в нее нового элемента (цифрового образа произведения). Правовое регулирование объектов гражданских прав во многом строится с учетом их экономической сущности и интересов участников оборота, в связи с чем классификация объектов приобретает не только теоретическое, но и практическое значение. С учетом названных обстоятельств цифровой образ произведения отвечает всем формальным признакам объекта гражданских прав. Но нерешенным остается вопрос о том, какое место цифровой образ произведения занимает среди существующих объектов гражданских прав? В данном случае мыслимы два пути.

Первый – это причисление цифрового образа произведения к закрепленным в ст. 128 ГК РФ объектам, среди которых наиболее близко по правовой природе располагаются права интеллектуальной собственности и имущество, в частности, цифровые права. Однако стоит отметить, что путем простого расширения терминологии одних объектов на другие, искомый результат не будет достигнут.

Второй путь – это закрепление цифрового образа произведения как отдельного объекта гражданских прав, не сводимого ни к одному из существующих и законодательно закрепленных объектов, и создание специального регулирования, отвечающего особенностям цифровых образов произведений. Именно данный подход будет проанализирован в дальнейшем в настоящей работе.

Начнем с вопроса о соотношении криптоискусства и объектов права интеллектуальной собственности. Объектами интеллектуальной собственности традиционно считаются результаты интеллектуальной (творческой) деятельности и приравненные к ним средства индивидуализации. Стоит заметить, что несмотря на формально закрытый перечень ст. 1225 ГК РФ (что уникально для мировой практики), он может быть расширен, например, за счет открытого перечня объектов авторских прав (п. 1 ст. 1259 ГК РФ) (см. абз. 1 п. 80 Постановления Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского Кодекса Российской Федерации»), а также за счет отнесения новых результатов интеллектуальной деятельности к одному из охраняемых видов объектов.

Одновременно дополнение данного перечня таким объектом как цифровой образ произведения представляется невозможным в связи со следующими фундаментальными отличиями цифрового образа произведения от категории объектов интеллектуальной собственности.

Так, объекты, включенные в ст. 1225 ГК РФ, являются результатом интеллектуального, умственного труда авторов, отличаются творческим характером и оригинальностью, в то время как цифровой образ произведения представляет собой цифровой код, созданный с помощью технических средств. Иными словами, «автор» (технический создатель) цифрового образа произведения не вложил в него никакого дополнительного

творческого элемента. Следовательно, NFT-токены, защищающие данное произведение в цифровой среде, сами по себе не являются объектами творческого труда. Например, авторство картины остается за ее художником, создавшим произведение искусства и защищается по правилам ч.и IV ГК РФ, а авторство на цифровой образ, которое автоматически возникает и принадлежит лицу (пользователю), выгрузившему работу на платформу, может переходить к пользователю, купившему права на NFT-токены, защищающие данный объект. То есть NFT выступают в роли подписи оригинала работы художника, подтверждая подлинность цифрового оригинала (в связи с чем невозможно согласиться с Законопроектом № 126586-8 «О внесении изменений в статью 1225 части четвертой ГК РФ (в части расширения перечня охраняемых результатов интеллектуальной деятельности в виде невзаимозаменяемых токенов)»).

Кроме того, стоит отметить, что результат творческой деятельности является благом нематериальным, поскольку существует только в сознании автора и не может признаваться объектом гражданских прав до тех пор, пока не будет обличен в объективную форму.

Цифровой образ произведения также обладает нематериальной природой (является бестелесным, неовещественным объектом), однако «нематериальность» цифрового образа в отличии от объектов интеллектуальной собственности связана, главным образом, с его формой существования в виртуальном пространстве, которая позволяет объективно воспринимать сам объект при невозможности его материализации. Такое свойство не только подчеркивает уникальность цифрового образа, но и позволяет цифровым объектам приобретать дополнительные потребительские свойства и дополнительную коммерческую ценность, что особенно важно в условиях цифровой экономики.

Также важным отличием цифрового образа произведения от объектов права интеллектуальной собственности является тот факт, что последние не могут отчуждаться или иным образом переходить от одного лица к другому, оборотоспособны только права на объекты права интеллектуальной собственности. В то же время в случае с цифровым образом произведения приобретаться и отчуждаться может как право на цифровой образ произведения с сохранением оригинала у изначального правообладателя, так и сам образ, который переходит внутри платформы к разным лицам путем пересылки.

Наконец, для цифровых образов произведений не характерна территориальная и временная ограниченность действия права, поскольку глобальный характер технологий блокчейн нацелен на отсутствие каких-либо границ.

Таким образом, криптоискусство (цифровой образ произведения) и объекты права интеллектуальной собственности существенно отличаются. Приведенные характеристики не позволяют включить цифровой образ произведения в систему объектов интеллектуальной собственности, но в то же время отражают взаимосвязь данных явлений. Без создания произведения как объекта интеллектуальных права, невозможно говорить и о создании цифрового образа произведения, что неминуемо влечет определенную схожесть и соприкосновение объемов данных понятий.

При этом, вопрос о соотношении указанных категорий, не исчерпывает проблематику влияния цифрового образа произведения на сферу права интеллектуальной собственности. Учитывая специфику настоящей работы, в предмет обсуждения стоит

включить саму возможность токенизации произведения искусства. Представляется, что цифровизация объектов интеллектуальной собственности может ущемлять права авторов произведений. Так, перевод произведения в цифровую среду без прямого согласия автора может привести к искаженному восприятию произведения, нарушению целостности понимания и, как следствие, нарушению личных немущественных прав автора. Более того, даже после того, как произведение перешло в общественное достояние вопрос о цифровизации остается открытым.

При этом, музеи искусств в последнее время активно токенизируют произведения из своих коллекций. Так, в июле 2021 года Государственный Эрмитаж начал сотрудничество с блокчейн-экосистемой Vinance с целью создания и выпуска токенизированных произведений из собрания музея. В ноябре 2021 года стартовал проект «Незримый эфир. Выставка цифрового искусства», который стал началом построения «Небесного Эрмитажа» – цифрового двойника музея. NFT Эрмитажа являются самостоятельными арт-объектами, а исключительные права на новые произведения, цифровые образы картин, закреплены за музеем.

В то же время представляется, что автор, давший согласие на цифровизацию, не вправе в дальнейшем заявлять о нарушениях своих прав из-за создания цифрового образа произведения, что следует из принципа эстоппель, а также создает категорию «исчерпания прав» для объектов авторского права. То есть, разрешение автора нужно получить для того, чтобы перевести объект интеллектуальной собственности в NFT, но дальнейшее его использование правом интеллектуальной собственности не регулируется.

Одновременно введение в оборот такого объекта как цифровой образ произведения может предоставить авторам дополнительные возможности. Так, важной технологической особенностью системы блокчейн является возможность проведения транзакций анонимно, что дает гарантию авторам, не желающим раскрывать свое имя, обеспечить защиту их прав при сохранении персональных данных закрытыми.

Данные положения подчеркивают важность создания специального регулирования, способного защитить законные права и интересы как правообладателей криптоискусства, так и авторов физических оригиналов произведений, переведенных в NFT-токинг. Не менее важной задачей является и создание правового режима для безопасного оборота цифровых активов и предоставление доступа к криптоискусству.

Из сказанного следует, что цифровой образ произведения – это не просто особая форма результатов интеллектуальной деятельности, это абсолютно самостоятельный единый объект, в котором не происходит разделения на произведение и его форму в цифровом виде. При этом, анализ, произведенный в данном параграфе, продемонстрировал схожесть правовых моделей, в связи с чем определенные механизмы регулирования исключительных прав могут быть применимы к новому цифровому объекту, но лишь в той части, в которой они не противоречат технологическим особенностям и природе цифрового образа.

Второй вопрос, который стоит рассмотреть в рамках поставленной проблемы – соотношение цифрового образа произведения и цифровых прав.

В научной литературе существует мнение о том, что «феномен «цифровых прав» не порождает для юристов новой сущности» [8]. В действительности, основная масса споров по поводу цифровых прав (ст. 141.1 ГК РФ) связана с максимально

абстрактными формулировками, содержащимися в ГК РФ, которые, по сути, сводятся к тому, что цифровыми правами является все то, на что прямо указал законодатель, исходя из чего, перечень цифровых прав может постоянно расширяться.

Однако проблема отнесения цифрового образа произведения к такому объекту гражданских прав как цифровые права заключается в разном правовом содержании данных категорий и, как следствие, в отличающемся регулировании указанных объектов. Так, исходя из системного толкования законодательства, под цифровыми правами в ст. 141.1 ГК РФ понимаются, в первую очередь, цифровые финансовые активы (денежные требования, токены, криптовалюта, некоторые корпоративные права и прочее) (см. Законопроект № 424632-7 «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации»; ст. 1 Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты РФ», ФЗ от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и ст. 1124 части третьей ГК РФ»; ФЗ от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты РФ»; ФЗ от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в РФ»). Подобное законодательное регулирование свидетельствует о попытке создания специальной нормативно-правовой базы в области цифровой валюты, которая, по существу, и составляет категорию цифровых прав, но не о введении в оборот нового объекта прав. Аналогичное мнение встречается и в доктрине: понятие «цифровые права» тождественно понятию цифровые деньги [4. С. 40; 6. С. 21–28].

Распространенной также является точка зрения о том, что цифровые права – это способ удостоверения имущественных прав [1. С. 3–14; 4. С. 43]. По сути, сторонники данного подхода отрицают наличие у цифровых прав особой экономической и правовой сущности. Наиболее категорично это утверждает С. В. Сарбаш: «Цифровые права суть химера» [4. С. 6–9]. Автор считает, что «цифровизация как таковая и цифровизация экономики – лишь метод оформления, но не содержание имущественного отношения» [4. С. 6–9]. В таком случае, рассматривая криптоактивы (цифровые права) лишь в качестве способа фиксации прав, необходимо признать, что новый способ фиксации не порождает новые права. Но существует и другое мнение, например, Л. А. Новоселова утверждает, что у владельцев криптоактивов возникают новые экономические возможности [4. С. 39].

Однако даже те авторы, которые признают цифровые права в качестве объекта гражданских прав, считают, что ст. 128 ГК РФ уже содержит понятие «имущественные права», в связи с чем происходит умножение сущностей [4. С. 17–18].

В то же время в отличие от владельца цифрового права правообладатель цифрового образа произведения обладает экономическим интересом, но не имущественным (связанным с правом собственности, иными вещными правами и обязательствами), что подтверждается следующими аргументами. Во-первых, невозможностью конвертации цифрового образа в материальный носитель, во-вторых, особой правовой природой цифрового образа, регулирование которого отчасти совпадает с регулированием института интеллектуальной собственности, что позволяет констатировать

неимущественный характер цифровых образов произведений аналогичный в этом смысле природе объектов права интеллектуальной собственности. Наконец, обязанным субъектом в правоотношениях, складывающихся по поводу цифровых образов произведений, является не конкретное лицо как это происходит в случае с цифровыми правами, а всякий и каждый [12], т. е. неопределенное число обязанных лиц. Исходя из этого, по правовой конструкции право на цифровой образ произведения является абсолютным правом. Одновременно в доктрине имущественные права как объекты гражданских прав рассматриваются только совместно с их юридической принадлежностью тем или иным субъектам в правоотношениях с конкретными должниками, т. е. являются относительными. И в этом смысле законодательно закрепленные имущественные права по своей природе не совпадают с абсолютным правом на цифровой образ произведения.

Таким образом, цифровой образ произведения не сводим к объему закрепленной правовой категории цифровых прав, поскольку данные понятия отличаются как сущностно, так и содержательно. Если цифровые права являются относительными имущественными правами, включающими в первую очередь цифровые финансовые активы, то право на цифровой образ произведения – абсолютное и не обеспечивает какие-либо объекты материального мира.

Однако все-таки необходимо отметить, что цифровой образ произведения обладает некоторыми чертами имущественных прав, так как мыслим оборот прав на цифровой образ произведения отдельно от самого объекта, что, в свою очередь, отличает его от более общей категории «имущества» как объекта гражданских прав. То есть цифровой образ произведения обладает двойственной природой, при которой может функционировать в гражданском обороте и как право, и как «вещь», что уже отмечалось ранее.

Кроме того, понятие «имущество» в гражданском праве многозначно [7. С. 362], что предполагает риск смешения цифрового образа произведения с материальным носителем. В то же время из-за широкого понимания данного термина, вплоть до признания имуществом любого, имеющего экономическую ценность объекта гражданских прав [5. С. 29], сложно провести четкую грань между цифровым образом произведения и имуществом. Однако представляется неверным расширять категорию имущества до абсурда, включая в нее все остальные объекты гражданских прав [5. С. 21].

Таким образом, цифровой образ представляет собой виртуальный, оборотоспособный объект гражданских прав, не сводимый к существующим объектам и не имеющий аналогов, в том числе среди имущества и имущественных прав, поскольку последние, с учетом существующей дискуссии в доктрине, имеют лишь некоторые схожие черты с цифровым образом произведения, но не отражают всех его сущностных правовых особенностей.

Итак, действующее российское законодательство закрепляет закрытый перечень объектов гражданских прав, однако в ходе данной работы, автором было предложено легитимировать новый объект, необходимость регулирования которого позволит обеспечить соблюдение интересов общества, государства и гарантировать правопорядок в условиях цифровой среды.

Цифровой образ произведения при наличии определенных сходств с другими объектами гражданских прав обладает настолько существенной спецификой,

выражающейся в тесном сплетении технико-правовых феноменов и неразрывной связи произведения и его цифровой сущности, что его включение в какую-либо категорию существующих объектов гражданских прав представляется невозможным. В настоящей работе было обосновано, что цифровой образ является обособленным, самостоятельным объектом гражданских прав.

Введение нового объекта и урегулирование оборота цифровых образов, включая фиксацию и переход права собственности на них, отвечает вызовам цифровой эпохи и требует детальной законодательной проработки. Так, на сегодняшний день открытым остается вопрос о юридических гарантиях участников цифровых рынков, поскольку наличие одних лишь технических способов защиты не в полной мере отвечает потребности участников оборота цифровых активов. Отсутствие специального правового режима не только ставит под сомнение права авторов цифровых и материальных произведений, но и не позволяет надлежащим образом ограничить оборот цифровых объектов с целью защиты прав авторов результатов интеллектуальной деятельности, что свидетельствует о необходимости определения места цифрового образа произведения в ряду объектов гражданских прав.

Помимо прочего, применение технологий блокчейна и токенизации позволяют ускорить транзакции и обеспечить дополнительную безопасность для участников рынка, что безусловно способствует развитию гражданского права и экономическому росту [11]. Однако до сих пор новые цифровые явления находятся вне правового поля, что не позволяет продолжать игнорировать их с точки зрения законодательного регулирования.

Также правовая регламентация цифрового образа произведения повлечет максимальное стимулирование интеллектуального творчества и коммерциализацию объектов интеллектуальных прав. Результаты творческого труда будут более доступны, что станет вехой развития новой правовой и социальной реальности в условиях современной цифровой среды.

Список литературы

1. Василевская Л. В. Цифровые права как новый объект гражданских прав: проблемы юридической квалификации. 2019. № 5. С. 3–14.
2. Лаптев В. А. Цифровые активы как объекты гражданских прав // Юридическая наука и практика. 2018. № 2 (42). С. 199–204.
3. Мейер Д. И. Русское гражданское право: чтения Д. И. Мейера, изданные по запискам слушателей под редакцией А. Вицына. Санкт-Петербург: Издательство Н. Тиблена, 1864. 789 с.
4. Новоселова Л. А. Цифровые права как новый объект гражданского права / Л. А. Новоселова, А. В. Габов, С. В. Сарбаш, А. В. Асосков [и др.] // Закон. 2019. № 5. 47 с.
5. Рожкова М. А. Право цифровой экономики: Ежегодник-антология / под ред. М. А. Рожковой. Москва: Статут. 2020. № 16. С. 29.
6. Санникова Л. В. Цифровые активы: правовой анализ: монография / Л. В. Санникова, Ю. С. Харитоновна. Москва: 4 Принт, 2020. 304 с.
7. Сергеев А. П. Гражданское право: учебник: в 3 т. Т. 1 / под ред. А. П. Сергеева. 2-е изд., перераб. и доп. Москва: Проспект, 2020. 1040 с.

8. Сулейменов М. К. Цифровизация и совершенствование гражданского законодательства. URL: <https://www.zakon.kz/5009131-tsifrovizatsiya-i-sovershenstvovanie.html>
9. Шершеневич Г. Ф. Учебник русского гражданского права. 3-е изд. Казань, 1901. 556 с.
10. Hoffman M. R., Choudhry T. Blockchains and Digital Assets. URL: https://www.eublockchainforum.eu/sites/default/files/research-paper/blockchains_and_digital_assets_june_version.pdf (дата обращения: 10.09.2022).
11. Kuner C. The Internet and the global reach of EU law // LSE Law, Society and Economy Working Papers. 2017. № 4. URL: http://eprints.lse.ac.uk/73421/1/WPS_2017-04_Kuner.pdf (дата обращения: 10.09.2022).
12. Malviya H. Blockchain for commercial real estate. URL: <https://ssrn.com/abstract=2922695> или <http://dx.doi.org/10.2139/ssrn.2922695> (дата обращения: 26.10.2021).
13. Pelnik E. Why are non-fungible tokens valuable? // Medium. 2018. URL: <https://medium.com/coinmonks/non-fungible-tokens-ac1c1a7aebed> (дата обращения: 26.10.2021).
14. Windsor R. Defining Digital Assets. URL: <https://digitalassetnews.org/assets/defining-digital-assets/> (дата обращения: 10.09.2022).

М. С. Евстефеева,

студент,

Самарский национальный исследовательский университет
имени академика С. П. Королева

ВИРТУАЛЬНАЯ СОБСТВЕННОСТЬ В МЕТАВСЕЛЕННОЙ

Аннотация. Статья посвящена вопросу существования виртуальной собственности и виртуальных объектов в метавселенной, а также концепции метавселенной и стремлению компаний занять свое место в ней. Описывается алгоритм получения виртуальной собственности в метавселенной, особенности владения виртуальными объектами, а также риски, связанные с отсутствием правового регулирования и наличием лицензионных соглашений компаний.

Ключевые слова: право, цифровые технологии, цифровое право, метавселенная, виртуальные объекты, виртуальная собственность, блокчейн, криптовалюта, NFT

VIRTUAL PROPERTY IN THE METAVERSE

Abstract. The article focuses on the existence of virtual property and virtual objects in the metaverse. The author discusses the increased attention to the concept of the metaverse and the desire of companies to take their place in it. The article describes the algorithm for obtaining virtual property in the metaverse, the peculiarities of owning virtual objects, as well as the risks associated with the lack of legal regulation and the existence of licensing agreements of companies.

Keywords: Law, Digital technologies, Digital law, Metaverse, Virtual objects, Virtual property, Blockchain, Cryptocurrency, NFT

Мы все чаще стали слышать слово «метавселенная». Да и вообще, приставка «мета» как никогда оказалась на повестке. Бренды, коллаборации, NFT – буквально все пространство кричит о придвижении новой волны. Волны под названием виртуальная реальность.

Что же такое метавселенная? Само слово «метавселенная» состоит из префикса «мета», что означает «за пределами» и «вселенная». Оно обычно используется для описания пространства виртуальной реальности, позволяющего пользователям взаимодействовать с компьютерной средой, а также с другими пользователями посредством нахождения в виртуальном мире.

Но на самом деле, будем честны, мало кто до конца осознает, что же на самом деле представляет из себя метавселенная. Что с точки зрения права представляет из себя метавселенная? Кто обладает правами на аппаратный комплекс и программную часть?

Несмотря на растущую популярность в настоящее время, концепция метавселенной не такая уж новая. Термин впервые был введен в 1992 г. в книге писателя Нила Стивенсона «Лавина», антиутопическом научно-фантастическом произведении, относящемся к миру виртуальной реальности, где люди, представленные цифровыми аватарами, взаимодействуют друг с другом и программными агентами.

О популярности метавселенной говорит и смена стратегии компании Facebook, которая переименовала себя в Meta (организация, признанная экстремистской. Запрещена в РФ) – ключевой элемент грандиозных амбиций основателя Марка Цукерберга по переосмыслению платформы социальных сетей как «компании метавселенной, строящей будущее социальных связей» [6]. Кроме этого, растет интерес к иным платформам метавселенной, таким как Sandbox, Decentraland

Другие корпорации также стремятся занять свое место в метавселенной, от Nike, регистрирующей новые торговые марки для продажи виртуальных Air Jordans, и Walmart, готовящейся предлагать виртуальные товары в интернет-магазинах, используя собственную криптовалюту и взаимозаменяемые токены (NFT).

В мае 2021 г. модный дом Gucci объявил о сотрудничестве с Roblox в рамках создания собственной цифровой метавселенной. Пользователи Roblox могли посетить несколько локаций под общим названием «Сад Gucci». С помощью виртуального пространства и интерактивных предметов пользователи игровой платформы смогут познакомиться с историей бренда [2].

Продолжающееся сотрудничество между люксовыми брендами и игровым миром на этой неделе сделало еще один значительный шаг вперед – Balenciaga стала первым люксовым брендом, сотрудничающим с Fortnite от Epic Games. На ежегодной конференции Business of Fashion Voices генеральный директор Balenciaga Седрик Шарбит заявил, что Balenciaga создает специализированный бизнес для изучения маркетинга и коммерции в Метавселенной, продолжая свои инновации и присутствие в виртуальном мире. В принципе, мы все сможем носить Balenciaga couture на наших цифровых свиданиях [1].

Метавселенная в глазах закона может выглядеть не более особенной, чем Интернет, которым мы пользуемся каждый день. Вспомним киберутопистов 1990-х гг., которые объявили интернет-пространством, свободным от юрисдикции офлайн-за-

конов. Они были убеждены, что интернет-общение помогает добиться более децентрализованного и демократического общества.

«Метавселенная создаст новую экономику, которая превысит по размеру глобальный ВВП», – так отзывается о возможном будущем генеральный директор Nvidia Дженсен Хуанг [5].

В виртуальной реальности существуют свои время, пространство и законы. Тем не менее отправной точкой в любом случае является порождающая ее действительность. Виртуальная реальность – это образная реальность, ее образы не имеют предметно-сущностного содержания, но она является ареной проявления действия свободной воли реального человека [3. С. 3–9].

По мнению А. А. Лукьяненко, свобода, которую приобретает человек в мире виртуальных предметов, может толкнуть его к стремлению властвовать над реальностью, тем самым ее разрушая, а может направить его по пути раскрытия тайн собственного бытия и созидания истинного логоса жизни [4. С. 124–130].

Право является официальной мерой свободы, устанавливаемой государством. Возможен ли и необходим ли правовой контроль в пространстве метавселенной?

Как же обстоят дела с виртуальной собственностью в метавселенной? Когда вы покупаете товар в метавселенной, ваша покупка записывается в транзакцию на блокчейне, который представляет собой цифровой реестр, который никто не контролирует и в котором записи транзакций не могут быть удалены или изменены, т. е. он надежен и постоянен. Ваша покупка предоставляет вам право собственности на NFT, который в свою очередь представляет собой уникальную строку битов. Вы храните NFT в крипто-кошельке, который можете открыть только вы, и который вы «носите» с собой, куда бы вы ни отправились в метавселенной. Каждый NFT связан с определенным виртуальным предметом.

Существование виртуальных товаров порождает вопросы о том, что произойдет, если виртуальная собственность будет уничтожена, украдена (например, путем взлома).

Легко подумать, что, поскольку ваш NFT находится в вашем крипто-кошельке, никто не сможет отобрать у вас виртуальную квартиру, снаряжение, поддерживаемые NFT, без доступа к закрытому ключу вашего кошелька.

Когда вы присоединяетесь к платформе метавселенной, вы должны сначала согласиться с условиями обслуживания платформы, условиями использования или лицензионным соглашением. Однако лицензионное соглашение имеет правовую природу договора присоединения. Лицензионное соглашение находится в ведении частной организации – что крайне проблематично, которая самостоятельно определяет условия пользования, а также правила поведения в метавселенной. В отличие от самого блокчейна условия обслуживания для каждой платформы метавселенной централизованы и находятся под полным контролем одной компании.

Частные организации-владельцы платформ, исходя из условий лицензионного соглашения могут законно удалять или отдавать ваши товары, удаляя цифровые активы из их оригинальных идентификационных кодов NFT. В итоге, даже если вы владеете NFT, который пришел в результате вашей цифровой покупкой, вы

юридически не владеете или не владеете самими цифровыми активами. Вместо этого платформы просто предоставляют вам доступ к цифровым активам и только на тот период времени, который они хотят. В случае блокировки, пользователь может лишиться виртуальной собственности, при этом вы равно будете владеть NFT на блокчейне с его оригинальным идентификационным кодом, но теперь такой виртуальный объект (собственность) станет функционально и финансово бесполезным.

Таким образом, интерес к концепции метавселенной растет с каждым годом все больше. Виртуальная реальность – это образная реальность, тем не менее отправной точкой в любом случае будет являться порождающая ее действительность. Отсутствие правового регулирования вопросов виртуальной собственности позволяет компаниям-разработчикам создавать собственные правила игры путем принятия лицензионных соглашений. Мы оказываемся в ситуации, при которой крупные компании обладают безграничными возможностями по установлению собственных правил в виртуальной реальности, забывая самое главное: «Право – это искусство добра и справедливости».

Список литературы

1. Balenciaga has major plans for the metaverse // Highsnobiety. URL: <https://www.highsnobiety.com/p/balenciaga-metaverse/> (дата обращения: 17.09.2022).
2. Inside Gucci and Roblox's new virtual world // Vogue Business. URL: <https://www.voguebusiness.com/technology/inside-gucci-and-robloxs-new-virtual-world> (дата обращения: 17.09.2022).
3. Галкин А. И. Философские проблемы виртуальной реальности // Известия высших учебных заведений. Северо-Кавказский регион. Общественные науки. 2004. № 4 (128). С. 3–9. EDN: JSIDBZ
4. Лукьяненко А. А. Феноменология свободы в виртуальной реальности // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2017. № 4 (78). С. 124–130. EDN: YKKNIT
5. Следующая версия интернета: как изменится жизнь в метавселенной // Forbes. URL: <https://www.forbes.ru/tekhnologii/439893-sleduusaa-versia-interneta-kak-izmenitsa-zizn-v-metavselennoj> (дата обращения: 17.09.2022).
6. Товарищи по Meta: Цукерберг объявил о новых ценностях бывшей Facebook // Forbes. URL: <https://www.forbes.ru/milliardery/455773-tovarisip-meta-cukerberg-ob-avil-o-novyh-cennostah-byvsej-facebook> (дата обращения: 17.09.2022).

К. П. Ермоченко,

магистрант,

Смоленский государственный университет

СМАРТ-КОНТРАКТ СЕГОДНЯ: «УМНЫЙ ДОГОВОР» В СИСТЕМЕ ПРАВОВЫХ ОТНОШЕНИЙ ИЛИ МАЛОЭФФЕКТИВНЫЙ «ЦИФРОВОЙ ЗАРОДЫШ» НЕСАМОСТОЯТЕЛЬНОЙ ДОГОВОРНОЙ КОНСТРУКЦИИ

Аннотация. Цель данного исследования заключается в анализе современного состояния, развития и внедрения в область права и правовых отношений смарт-контрактов как возможного информационного агента, способного сегодня конкурировать с «живым умом» человека. Делается вывод о несостоятельности данного агента в силу наличия у него большого количества противоречивых недостатков.

Ключевые слова: информационное общество, смарт-контракт, договор, правовые отношения, цифровая платформа, блокчейн

SMART CONTRACT TODAY: A “SMART CONTRACT” IN THE SYSTEM OF LEGAL RELATIONS OR AN INEFFECTIVE “DIGITAL GERM” OF AN INDEPENDENT CONTRACTUAL STRUCTURE

Abstract. The purpose of this study was to thoroughly analyze the current state, development and implementation of smart contracts in the field of law and legal relations as a possible information agent capable of competing with the “living mind” of a person today. The author comes to the conclusion about the insolvency of this agent due to the presence of a large number of contradictory shortcomings.

Keywords: Information society, Smart contract, Contract, Legal relations, Digital platform, Blockchain

Введение. Современный «мир цифры и информации» предъявляет совершенно новые требования к возможному эффективному взаимодействию между субъектами правовых отношений, вырабатывает актуальные информационные реалии, на основе которых возможно достичь наибольшего успеха в решении большинства проблем из области права.

Сначала нового тысячелетия возникло огромное количество цифровых платформ, механизмов, технических агентов информационного общества, первоначальная цель которых сводится к упрощению процедуры решения возникшего вопроса или проблемы из любой сферы человеческой жизни.

К числу таких «информационных проводников» между агентами-посредниками власти, закона, юридического лица и гражданина, например, является всем известная и набирающая популярность Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)» – справочно-информационный интернет-портал.

Эффективность работы портала, ее необходимость была прокомментирована в 2015 г. руководителем рабочей группы Агентства стратегических инициатив по

продвижению новых проектов Павлом Романовым: «Чем были раньше недовольны люди? Они были недовольны очередями, которые выстраивались для получения самых популярных государственных услуг, и все мы это хорошо помним. А сегодня ведомства оказывают все наиболее востребованные свои услуги в электронном виде, т. е. сегодня ты не только не должен стоять в очереди, а даже и ходить никуда не должен» [2].

И с этим нельзя не согласиться, несмотря на то, что сказано это было в 2015 г. Эта платформа доказала свою эффективность сегодня, в 2022 г., в условиях сложной обстановки в стране, связанной с продолжающимся распространением пандемии COVID-19 и специальной военной операции на территории Украины.

Представленная онлайн-платформа является многозадачным, стремительно развивающимся механизмом решения возникающих проблем граждан из социальной, экономической сферы. Но в меньшей степени она затрагивает область правовых отношений и защиту прав индивидов и организаций, являющихся субъектами данной правовой связи.

Сегодня многофункциональные определения термина «правовые отношения» в общем универсальном понимании современной правовой науки означают определенную установленную форму современного социального бытия права при условии полного раскрытия в нем процесса воплощения правовой нормы в реальной жизни современного гражданина.

Правовые отношения, как отмечает Н. Н. Вопленко, «отличаются от всех других общественных отношений своей юридической гарантированностью» [3. С. 77].

Смарт-контракт в системе правовых отношений: современное состояние. «Юридическая гарантированность» всегда представлена, подкреплена и оформлена, как правило, в виде договора, контракта или иного другого письменного соглашения сторон.

В связи с этим, на наш взгляд, в условиях информационного общества, цифровизации, которая проникает во все сферы жизни человека, в том числе и в правовую, и возникает необходимость постепенно отойти или полностью перейти от «бумажной гарантированности» к «электронной» в системе правовых отношений.

На наш взгляд, сегодня наиболее прогрессивным информационным инструментом решения правовых вопросов является смарт-контракт (Smart Contract), который представляет собой своего рода компьютерный протокол, необходимый для тщательной проверки основных компонентов контракта именно в цифровом виде и исполнения его основных условий, которые могли бы быть представлены в привычном бумажном виде.

Словосочетание Smart Contract впервые предложил в 1994 г. ученый в области информатики и умных контрактов и криптовалюты Ник Сабо, разработавший, помимо всего прочего, алгоритм одной из первых криптовалют – bit gold, предопределившей биткоин, но не реализованной, чего нельзя сказать о концепции смарт-контрактов. Сегодня они широко применяются, например, в сети Ethereum. Она также функционирует на базе блокчейна и направлена на создание онлайн-сервисов.

Блокчейн представляет собой базу данных, которая содержит информацию обо всех транзакциях, проведенных участниками системы, при возможности хранения информации в виде цепочки блоков. Это фундамент смарт контрактов.

Смарт-контракты являются полностью автономными, но при этом обеспечивают выполнение всех обязательств, которые прописаны в них. Это своеобразный торговый автомат.

Вы отправляете в него какую-нибудь цифровую монету, например, TON Crystal, а он отправляет вам то, что вы должны были получить. В системе правовых отношений смарт-контракты – это адвокаты или нотариусы, но не реальные, а «живые цифровые копии».

Несмотря на сравнительную новизну этого информационного явления, проблемам Smart Contract посвящено достаточное количество научных работ, авторы которых по-своему трактуют и оценивают их эффективность, приводя ряд объективных доказательств и мер совершенствования.

Так, в научной статье С. С. Кузнецовой «Актуальные вопросы реализации и защиты прав человека в практике применения технологии смарт-контракта» [4. С. 136] были сформулированы основные характерные особенности последнего, указаны его преимущества и недостатки и проанализирована практика правового регулирования смарт-контрактов в отдельных странах.

Автор подводит нас к мысли о необходимости «расширения» законодательного определения смарт-контрактов, которое «позволило бы подстраивать объективное право под меняющиеся условия, под изменения цифрового пространства».

«Правовое регулирование смарт-контрактов является необходимым в том объеме, которое позволит обеспечить реализацию прав человека и их защиту, например путем установления сфер, в которые применение смарт-контрактов должно быть запрещено с целью соблюдения принципов гуманизма, верховенства права (например, при проведении медицинских вмешательств, в военных целях и т. д.)» [4. С. 140].

Мы полностью согласны с мнением С. С. Кузнецовой и считаем, что никто сегодня не может возложить на себя обязанности прямого гаранта и законного посредника между таким «информационно-специфическим» контрактом и реальными людьми, стоящими за ним.

Несмотря на такие очевидные преимущества смарт-контракта, как безопасность, представленная максимально безопасной средой для хранения документов; отсутствие пауз в работе, потому что смарт-контракты полностью автономны; быстрое осуществление транзакции, отсутствие комиссий, ошибок, на наш взгляд, он является малоэффективным «цифровым зародышем» несамостоятельной договорной конструкции, который сегодня не в силах заменить человека. «Смарт-контракты являются не только объектом, но и орудием преступлений» [4].

Следует особо отметить, что было предпринято несколько попыток сформулировать и закрепить понятие смарт-контракта на законодательном и правоприменительном уровнях.

Но в Федеральном законе от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные

акты Российской Федерации» изменений в пользу юридического закрепления смарт-контрактов нет.

В настоящее время правовое регулирование вопросов о смарт-контрактах ограничивается общими положениями (Федеральный закон от 18.03.2019 № 34-ФЗ), к числу которых, в частности, относится ч. 2 ст. 434 ГК РФ: «Договор в письменной форме может быть заключен путем составления одного документа (в том числе электронного), подписанного сторонами, или обмена письмами, телеграммами, электронными документами либо иными данными...» [4. С. 135].

Но, несмотря на отсутствие юридического закрепления, сегодня смарт-контракты развиваются, находят новые сферы применения, многие ведущие компании их стремительно разрабатывают, к их числу относятся следующие организации: Coin Fabric, Cyber Infrastructure Inc, Eleks, HashCash Consultants [1. С. 78] и многие др. Результаты не заставили себя долго ждать.

Так, блокчейн-эксперты отметили, что количество скриптов на основе языка Plutus увеличилось на 489 единиц в период с 28 по 30 марта 2022 г. Статистика указала: их число выросло с 1671 до 2160. Это свидетельствует о том, что суммарное количество смарт-контрактов на базе сети Cardano превысило 2 тыс. [5. С. 130].

Заключение. Таким образом, сегодня объективно точно ответить на вопрос, касающийся эффективности смарт-контрактов в современных цифровых реалиях, невозможно.

Это связано с тем, что они имеют заметные и даже очень важные достоинства, которые обеспечили им право конкурировать сегодня с человеком в полном смысле этого слова с возможностью подменить последнего или полностью заменить его автономной работой в системе правовых отношений.

Но при всех возможностях, достоинствах, отличиях этого «цифрового зародыша» информационной эпохи от традиционных бумажно-договорных конструкций мы солидарны с авторами научной работы «Смарт-контракт: от определения к определенности», которые считают, что «SC не заменят обычных контрактов – это лишь альтернатива в конкретных областях, которая обеспечивает значительные преимущества» [2].

У человека нет возможности предвидеть дальнейший путь эволюционного или иного развития общества, он не может проложить траекторию от сегодняшнего информационного общества, потому что есть исходная точка развития, но в то же время есть и тысячи направлений этого развития. Сможет ли «цифра» заменить человека? Сегодня ответа нет.

Список литературы

1. Barbry E. Smart contracts... Aspects juridiques! // *Réalités Industrielles*. 2017, Août. P. 77–80.
2. Szwed M. Constitutional protection of freedom of contract in the European Union, Poland and the United States and its potential impact on the European contract law. Central European University, 2014. 87 p. URL: http://www.etd.ceu.hu/2014/szwed_marcin.pdf (дата обращения: 17.08.2022).

3. Вопленко Н. Н. Правовые отношения: понятие и классификация // Вестник Волгоградского государственного университета. Серия 5: Юриспруденция. 2003. № 6. С. 76–89.

4. Кузнецова С. С. Актуальные вопросы реализации и защиты прав человека в практике применения технологии смарт-контракта // Правоприменение. 2022. Т. 6, № 1. С. 134–149.

5. Трунцевский Ю. В. Смарт-контракт: от определения к определенности / Ю. В. Трунцевский, В. В. Севальнев // Право. Журнал Высшей школы экономики. 2020. № 1. С. 118–148.

А. Л. Журавлева,
студент,

Донецкий национальный университет

ЛИЦЕНЗИРОВАНИЕ ОНЛАЙН-ОБРАЗОВАНИЯ КАК ЭЛЕМЕНТА ЦИФРОВЫХ ТЕХНОЛОГИЙ

Аннотация. Актуальность данной темы обусловлена стремительным ростом популярности онлайн-образования и недостаточностью правового регулирования данного элемента цифровизации. Целью работы является установление истинной причины необходимости лицензирования онлайн-образования с помощью онлайн-курсов, предоставляемых индивидуальными предпринимателями и организациями, для которых предоставление образовательных услуг не является основным видом деятельности. Также обозначены критерии, при которых лицензирование является необходимым, и обоснована необходимость развития регулирования лицензирования онлайн-образования.

Ключевые слова: онлайн-образование, дистанционное образование, онлайн-курсы, лицензия, лицензирование, образовательная деятельность, дистанционные образовательные технологии

LICENSING ONLINE EDUCATION AS AN ELEMENT OF DIGITAL TECHNOLOGY

Abstract. The relevance of this topic is due to the rapid growth in the popularity of online education and the lack of legal regulation of this element of digitalization. The purpose of the work is to establish the true reason for the need to license online education using online courses provided by individual entrepreneurs and organizations for which the provision of educational services is not the main activity. Criteria are also indicated in which licensing is necessary and the need to develop regulation of online education licensing is justified.

Keywords: Online education, Distance education, Online courses, License, Licensing, Educational activities, Remote educational technologies

Благодаря развитию цифровых технологий и использованию их для образования на данный момент существует множество обучающих курсов, тренингов и других форм получения знаний онлайн. Такой формат позволяет получать знания в любое время и в любой точке мира. Особенно актуально онлайн-образование для полу-

чения тех навыков и узкоспециализированных знаний, которые не всегда можно освоить при классическом образовании.

Как и во многих других сферах, в сфере образования цифровизация имеет не только положительные, но и отрицательные аспекты. К ним можно отнести некомпетентных лиц, продающих обучающую информацию, низкое качество и отсутствие научной обоснованности такой информации и т. д. Из-за быстрого распространения образования в онлайн-среде и высокой маржинальности такого бизнеса, которая привлекает недобросовестных предпринимателей, у потребителя исчезла уверенность, что можно доверять предоставляемой информации. Самым ярким примером недобросовестного онлайн-обучения являются обучающие курсы, на которых предлагают обучение быстрым и легким способам получения высокого дохода. Частично данную проблему помогает решить лицензирование онлайн-образования.

Точное определение лицензии и лицензирования дано в Федеральном законе от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности». Так, согласно данному закону, лицензия – специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается записью в реестре лицензий. Лицензирование – деятельность лицензирующих органов по предоставлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, оценке соблюдения соискателем лицензии, лицензиатом лицензионных требований, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса, а также по предоставлению в установленном порядке информации по вопросам лицензирования [11].

Слово «лицензия», произошедшее от лат. *Licentia* – «право», в современном своем смысле представляет собой способ контроля за качеством отдельных видов деятельности [2. С. 200]. Такой контроль осуществляет государство, которое и определяет нормы, которым необходимо соответствовать для получения лицензии. Основной целью лицензирования является обеспечение качества услуг.

Рассматривая сферу онлайн-образования, стоит отметить, что в данном случае речь идет об образовательной лицензии. Наиболее интересным со стороны вопросов правового регулирования представляется осуществление образовательной деятельности индивидуальными предпринимателями и организациями, для которых предоставление образовательных услуг не является основным видом деятельности, так как в работах ученых онлайн-образование рассматривается преимущественно в аспекте создания онлайн-курсов университетами или крупными образовательными платформами. Такой подход можно встретить в работах М. В. Макаровой, М. А. Бичеева [3. С. 260; 6. С. 63].

Основными нормативно-правовыми актами, регулирующими на данный момент сферу онлайн-образования, являются законы «О лицензировании отдельных видов деятельности» [11] и «Об образовании в Российской Федерации» [12]. Данные НПА не предусматривают понятие «онлайн-образование», лишь упоминают «электронное

обучение» и «дистанционные образовательные технологии». На данную проблему также обращает внимание в своей работе А. А. Стриженко, акцентируя внимание на том, что в научной среде нет единства даже в отношении терминологии рассматриваемой темы [10. С. 75].

Понятие онлайн-курсов упоминается лишь в Порядке применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ [1. С. 69]. Исходя из содержания представленного Порядка, можно сформировать понятие, которое предусматривает, что онлайн-школа – это организация, которая предоставляет образовательные услуги при помощи электронного образования или дистанционных образовательных технологий, имеет свою программу обучения, реализуемую в виде онлайн-курсов.

Исходя из анализа НПА, регулирующих образовательную деятельность, становится понятно, что отсутствие должного регулирования препятствует развитию онлайн-образования, несмотря на высокий спрос среди потребителей на такой способ получения знаний.

Как уже было указано, все процессы в онлайн-школе происходят дистанционно, через Интернет, однако на практике, после получения лицензии, закон выдвигает к лицензиату ряд требований, среди которых наличие на праве собственности или ином законном основании зданий, строений, сооружений, помещений, необходимых для осуществления образовательной деятельности; наличие материально-технического обеспечения образовательной деятельности, оборудование помещений, необходимых для осуществления образовательной деятельности и т. д. [5. С. 107; 8]. Такие требования противоречат самой сущности цифровизации.

Образовательная лицензия необходима только в том случае, если обучение реализуется по образовательным программам, имеет длительный, а не разовый характер [4. С. 83]. Именно согласно данному критерию определяется необходимость получения лицензии. В случае отсутствия лицензии на осуществление онлайн-образования при ее необходимости предприниматель привлекается к административной или уголовной ответственности [7. С. 199].

Стоит отметить, что лицензирование онлайн-образования должно преследовать не только цель контроля за предоставляемой информацией, а и за компетентностью спикеров на определенном курсе. К примеру, в социальных сетях распространены обучающие марафоны и курсы по правильному питанию, спорту, похудению, однако не всегда информация в них безопасна для здоровья, потому что составлена некомпетентными лицами. Также известна ситуация с так называемой продажей воздуха через «Марафоны желаний». В рекламных кампаниях освещаются обещания о быстрых результатах благодаря уникальным методикам, которые на самом деле не запатентованы в качестве таковых. Такая информация может нанести вред ментальному состоянию человека и нравственности и в целом имеет мошеннический характер. Так как может быть неоригинальной или ложной. В то же время не всегда в деяниях создателей таких курсов имеются все необходимые для привлечения к ответственности за мошеннические действия признаки. Введение дополнительных мер контроля и расширение норм, регули-

рующих именно онлайн-образование, осуществляемое индивидуальными предпринимателями или организациями, для которых образовательная деятельность не является основной, позволит потребителям иметь возможность эффективнее защищать свои права.

Также остро стоит вопрос о соблюдении законодательства об авторских правах, так как если незарегистрированная программа обучения будет скопирована, такая ситуация может быть решена только путем судебного разбирательства [9. С. 304].

Таким образом, поскольку изменения и технологии продолжают влиять на образование с помощью методологии обучения и доступности ресурсов, вопрос о качественном образовании следует продолжать анализировать, вносить изменения или создавать новые нормативно-правовые акты, регулирующие онлайн-образование. Такие нововведения необходимы, так как переход образования в онлайн-среду является неотъемлемой частью цифровизации, становления информационного общества, путем развития доступности знаний. Реформирование регулирования онлайн-образования позволит привлекать специалистов, расширять взаимодействие между преподавателями, ведущими свою деятельность онлайн, увеличит процент доверия к такому способу получения знаний и позволит получать такие документы, подтверждающие прохождение курса или иного формата, которые будут признаваться на государственном уровне. Также развитие регулирования позволит уменьшить количество правонарушений в сфере онлайн-образования.

Список литературы

1. Белова И. А. Анализ факторов, влияющих на развитие онлайн-обучения в России // Вестник Челябинского государственного университета. 2022. № 4 (462). С. 161–172.
2. Бибик А. М. Развитие института лицензирования в отношении получения лицензий на онлайн-образование // Вестник науки. 2022. Т. 1, № 6 (51). С. 195–203.
3. Бичеев М. А., Доронина И. В. Скилл-обучение в режиме онлайн: новый вызов профессиональному образованию в России // Философия образования. 2012. № 6 (45). С. 258–262.
4. Буторина Г. В. Актуальные вопросы лицензирования онлайн-образования // Альманах научных работ молодых ученых Университета ИТМО. Санкт-Петербург: Национальный исследовательский университет ИТМО, 2021. С. 81–84.
5. Лубышева Л. И. Онлайн-образование: состояние и перспективы // ТиПФК. 2022. № 4. С. 107–108.
6. Макарова М. В. Перспективы онлайн-образования в России // Современное образование. 2020. № 2. С. 59–70.
7. О лицензировании образовательной деятельности: Постановление Правительства РФ от 18.09.2020 № 1490 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_363079/ (дата обращения: 17.09.2022).
8. О лицензировании отдельных видов деятельности: Федеральный закон от 04.05.2011 № 99-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_113658/ (дата обращения: 17.09.2022).

9. Об образовании в Российской Федерации: Федеральный закон от 29.12.2012 № 273-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_140174/ (дата обращения: 17.09.2022).

10. Осанова М. В., Одинцова О. В. Развитие онлайн-образования в России // Образование и право. 2022. № 5. С. 196–201.

11. Соловьев А. С. К вопросу о лицензировании отдельных видов предпринимательской деятельности / А. С. Соловьев, М. Л. Макаревич // Перспективы развития институтов права и государства. Курск: Юго-Западный государственный университет, 2019. С. 303–305.

12. Стриженко А. А. Онлайн-образование: теория и практика // Экономика Профессия Бизнес. 2016. № 1. С. 74–78.

И. В. Захаров,
магистрант,

Российский университет дружбы народов

ОРГАНЫ И УЧРЕЖДЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: РЕГИОНАЛЬНЫЙ АСПЕКТ

Аннотация. В статье анализируется система регионального управления информационными технологиями. Сделан акцент на классификации органов и учреждений, осуществляющих управление на уровне субъектов Российской Федерации. Большинство субъектов Российской Федерации осуществляют управление в информационной отрасли, проанализирована связь между уровнем информатизации региона и органом управления соответствующей отрасли, а также выдвинуты предположения возможных изменений организационной формы органов.

Ключевые слова: информационные технологии, органы исполнительной власти, субъекты Российской Федерации, государственное управление, министерства, государственные учреждения, информатизация

BODIES AND INSTITUTIONS IN THE FIELD OF INFORMATION TECHNOLOGY: REGIONAL ASPECT

Abstract. The article analyzes the system of regional management of information technologies. Emphasis is placed on the classification of bodies and institutions that manage at the level of the subjects of the Russian Federation. The majority of the subjects of the Russian Federation carry out management in the information industry, the relationship between the level of digitalization of the region and the governing body of the relevant industry is analyzed, and assumptions are made about possible changes in the organizational form of the bodies.

Keywords: Information technologies, Executive authorities, Subjects of the Russian Federation, Public administration, Ministries, State institutions, Digitalization

Предмет правового регулирования в сфере информационных технологий менялся по мере развития технологий и их внедрения в жизнь общества. В настоящее время информационные технологии в самом широком смысле понимаются как

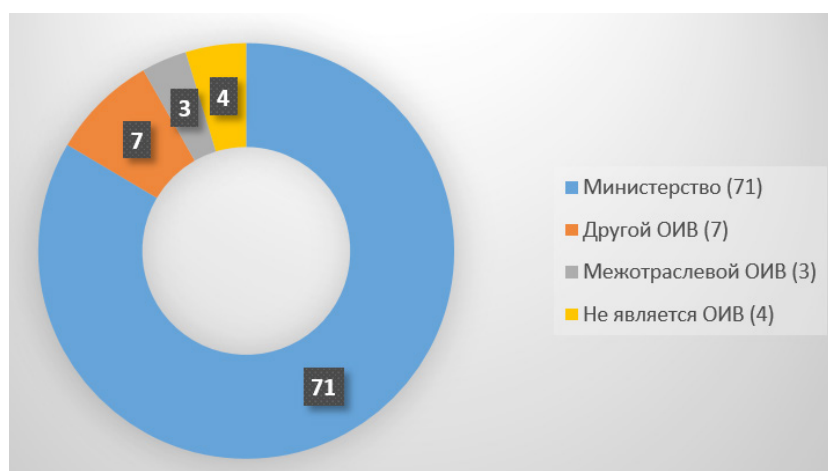
область человеческой деятельности, связанной с созданием систем и устройств для обработки и передачи информации [1]. В зависимости от области применения термина информационные технологии могут трактоваться как комплекс дисциплин или область практической деятельности; как процесс или знание; как метод или средства.

Наряду с федеральными транспортом и путями сообщения информация, информационные технологии и связь, в соответствии с п. «и» ст. 71 Конституции Российской Федерации, отнесены к ведению федеральной власти. Следуя буквальному грамматическому толкованию, можно было бы заключить, что в компетенции Федерации находятся лишь федеральные информационные технологии. Однако такое понятие нашему законодательству неизвестно.

Проясняет конституционное положение Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» [2]. В ст. 4 и 12 Федерального закона вся сфера регулирования информационных технологий закрепляется за Российской Федерацией. Органам государственной власти субъектов РФ и органам местного самоуправления предоставлены полномочия по участию в разработке целевых программ, а также в организации доступа к информационным ресурсам на русском языке и языке республики, принятым наравне с государственным.

В случаях, когда сфера управления отнесена к исключительному ведению Федерации, министерства обычно создают свои территориальные органы, в том числе и в субъектах Российской Федерации. Функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий осуществляет Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) [3], однако территориальные органы Минцифры России, в том числе и по субъектам РФ, не созданы.

В субъектах Российской Федерации региональные органы исполнительной власти в сфере информационных технологий создаются, но единый подход при этом отсутствует, что иллюстрирует рисунок.



В 71 субъекте Российской Федерации управление информационными технологиями осуществляет специализированный орган, имеющий статус министерства, у большинства которых в полномочия входит осуществление государственной

политики в конкретной сфере деятельности, а также нормативное правовое регулирование. Руководитель соответствующего органа является членом высшего органа исполнительной власти субъекта Российской Федерации. Примером такого подхода являются Департамент информационных технологий города Москвы [4], Министерство цифрового развития Удмуртской Республики [5], Департамент цифрового развития, информационных технологий и связи Администрации Тамбовской области [6].

В семи субъектах Российской Федерации управленческие полномочия в сфере информационных технологий осуществляют органы исполнительной власти субъекта, не являющиеся министерствами и подведомственные высшему должностному лицу, правительству или министерству субъекта РФ. Такую модель реализовали Республика Бурятия [7] и Республика Северная Осетия – Алания [8] (Комитет цифрового развития), Республика Марий Эл [9] и Краснодарский край [10] (Департамент информатизации и связи), Самарская область [11] (Департамент информационных технологий и связи), Псковская область [12] (Управление цифрового развития и связи Правительства Псковской области).

В Республике Хакасия действует Государственный комитет цифрового развития и связи, статус которого отличается определенной спецификой. В соответствии с законодательством Республики Хакасия в систему органов исполнительной власти республики входят как министерства, так и государственные комитеты. К компетенции государственных комитетов Хакасии относится проведение государственной политики в установленной сфере деятельности и осуществление функций по нормативно-правовому регулированию, а руководители этих органов являются членами Правительства Хакасии [13]. Хотя государственные комитеты логичнее было бы отнести к министерствам, в законе об органах исполнительной власти Хакасии поясняется, что министерства осуществляют государственную политику «в наиболее важных отраслях и установленных сферах деятельности». На основании этого можно сделать вывод, что для этой республики управление информационными технологиями является не приоритетным, как и для других субъектов, перечисленных во второй категории.

К третьей категории отнесены субъекты Российской Федерации, в которых вопросы управления информационными технологиями переданы в ведение органов межотраслевого управления. Так, в Министерстве внутренней политики, информации и связи Республики Крым [14], Министерстве жилищно-коммунального хозяйства, энергетики, цифровизации и связи Забайкальского края [15] и Министерстве энергетики, промышленности и связи Ставропольского края [16] информационные технологии являются не приоритетной или единственной, а одной из ряда сфер регулирования и управления, которыми занимаются указанные министерства.

В Республике Крым Министерство внутренней политики, информации и связи осуществляет регулирование в том числе в сфере культурного просвещения, книгопечатания, отвечает за формирование положительного образа республики, проведение фестивалей и мероприятий. В Забайкальском крае и Ставрополье регулирование информационных технологий совместили с регулированием энергетического сектора. В Забайкалье соответствующее министерство занимается также

жилищно-коммунальным хозяйством, в то время как в Ставрополье – промышленным производством.

В четвертую категорию объединены Республика Карелия, Чукотский автономный округ, Чеченская Республика и Ульяновская область, в которых вопросы, связанные с управлением информационными технологиями, переданы не органам исполнительной власти, а государственным учреждениям. На территории этих субъектов Российской Федерации функционируют: Государственное бюджетное учреждение Республики Карелия «Карельский ресурсный центр цифровых технологий», Государственное казенное учреждение «Центр цифрового развития и информационной безопасности чукотского автономного округа», Областное государственное казенное учреждение «Корпорация развития Интернет-технологий – многофункциональный центр предоставления государственных и муниципальных услуг в Ульяновской области». При этом функции учредителя осуществляют органы исполнительной власти субъектов – Администрация главы Республики Карелия [17], Департамент промышленной политики Чукотского автономного округа [18], Правительство Ульяновской области [19], Министерство транспорта и связи Чеченской Республики [20].

Все органы и учреждения, решающие вопросы информационных технологий, наделяются функцией организации и обеспечения использования информационных технологий в деятельности и взаимодействии органов исполнительной власти. Связано это, прежде всего, с внедрением системы электронных государственных услуг и развитием соответствующих интернет-сервисов.

В рамках Федеральной целевой программы «Электронная Россия (2002–2010 годы)» [21] в 2008 г. заработал первый региональный интернет-портал государственных услуг в рамках города федерального значения Санкт-Петербурга [22]. На смену «Электронной России (2002–2010 годы)» пришла Государственная программа «Информационное общество (2011–2020 годы)» [23], в рамках которой планировалось существенно увеличить долю населения, которая пользуется государственными услугами через Интернет. По состоянию на 2010 г. электронными государственными услугами пользовалось только 11 % населения России [24], а к 2020-му – уже абсолютное большинство населения России, 81,1 % [25].

Для обеспечения работы сервисов по оказанию государственных услуг как минимум необходима структура, способная обеспечивать нормальную работу электронного сервиса и взаимодействие органов, связанных с оказанием государственных услуг.

С 2004 г. эти функции выполняло подведомственное Министерству информационных технологий и связи Российской Федерации (Мининформсвязи России) Федеральное агентство по информационным технологиям (Росинформтехнологии) [26] – орган, ответственный за управление государственным имуществом и оказание государственных услуг в сфере информационных технологий, в том числе в части использования информационных технологий для формирования государственных информационных ресурсов и обеспечения доступа к ним.

Однако в 2010 г. Росинформтехнологии были ликвидированы, а соответствующие полномочия по управлению госимуществом и оказанию государственных услуг

переданы Министерству связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) [27], правопреемнику Мининформсвязи России [3].

Оптимизация управления в сфере информационных технологий привела к расширению компетенции федерального министерства, которое, вопреки положениям Указа Президента РФ № 314 от 9 марта 2004 г. «О системе и структуре федеральных органов исполнительной власти» [28], стало оказывать государственные услуги. На уровне субъектов Российской Федерации соответствующие органы с самого начала, т. е. с первой половины 2010-х гг., наделялись функцией оказания государственных услуг в сфере информационных технологий, в том числе в части использования информационных технологий для формирования государственных информационных ресурсов и обеспечения доступа к ним.

В связи с этим можно предположить, что передача функций управления информационными технологиями государственным учреждениям обусловлена, во-первых, невысоким уровнем цифровизации в соответствующем субъекте Российской Федерации, а во-вторых, недостаточно развитой системой оказания государственных услуг в электронной форме.

И действительно, согласно расчетам [29], Чукотский автономный округ и Чеченская Республика входят в последнюю десятку субъектов Российской Федерации по уровню цифровизации, занимая 77-е и 84-е место, соответственно. Хотя Республика Карелия занимает шестое место по уровню цифровизации, она значительно уступает другим регионам по количеству электронных государственных услуг [30]. Неслучайно поэтому республика первой среди субъектов Российской Федерации присоединилась к федеральному проекту «Цифровая Россия» [31].

В Ульяновской области до 2013 г. действовало Министерство по развитию информационных технологий и электронной демократии [32], функции которого позже передали Правительству Ульяновской области [33]. С 2016 г. было создано Областное государственное казенное учреждение «Корпорация развития интернет-технологий – многофункциональный центр предоставления государственных и муниципальных услуг в Ульяновской области» [34]. Область планирует к 2030 г. увеличить долю массовых социально значимых услуг, доступных в электронном виде, до 95 %, а рост доли домохозяйств, которым обеспечена возможность широкополосного доступа к Интернету, – до 97 % [35].

В регионах с высоким уровнем цифровизации, вовлеченности населения и государственных органов в использование информационных технологий (Москва, Санкт-Петербург, Республика Татарстан, Нижегородская область) [29] создаются специализированные министерства, что объясняется большим объемом управленческой работы. И, наоборот, регионы, отстающие по цифровизации [29], например, Республика Дагестан, Тверская область или Республика Тыва, вынуждены уделять развитию информационных технологий повышенное внимание и также создавать специализированные министерства. В таком случае министерства не столько обеспечивают существующие информационные технологии, сколько занимаются процессом их внедрения в повседневную жизнь общества и деятельность государственных органов субъекта Российской Федерации.

Таким образом, создание региональных специализированных органов с увеличением роли информационных технологий на соответствующей территории,

с одной стороны, и с необходимостью активного участия государственных органов во внедрении информационных технологий, в том числе в деятельность региональных органов – с другой. Так, в Тамбовской области Управление информационных технологий, связи и документооборота Администрации Тамбовской области было реорганизовано в Департамент Администрации Тамбовской области [6] в том числе в связи с увеличением значимости этой сферы жизни общества в регионе.

В Ульяновской области соответствующее министерство было ликвидировано, но через три года пришлось создать казенное учреждение для осуществления Правительством области полномочий в сфере информационных технологий. Можно предположить, что в случае увеличения доли массовых социально значимых услуг, доступных в электронном виде, до планируемых 95 % появление министерства по информационным технологиям или по информационному развитию станет необходимым.

Если возвращаться к исходному тезису о том, что информационные технологии признаны исключительной прерогативой федерального центра как Конституцией Российской Федерации, так и специализированным Федеральным законом. В данном случае можно сказать, что в соответствующих нормативных правовых актах определен строгий перечень полномочий и вопросов, по которому Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации может принимать решения и осуществлять политику в рамках всего государства, а не отдельной территории [3]. И эти вопросы не пересекаются с перечнем вопросов, которые регулируют органы исполнительной власти субъектов Российской Федерации.

Подводя итог, можно констатировать следующее, система органов исполнительной власти и учреждений субъектов Российской Федерации в сфере государственного управления информационными технологиями представляет из себя децентрализованную систему, которой не свойственно организационное единство и единый подход к управлению в рамках разных территорий. В связи с тем, что полномочия органа исполнительной власти федерального уровня с каждым разом только увеличивались в связи с объективными причинами увеличения роли информационных технологий в обществе. Подобное увеличение полномочий в такой короткой по историческим меркам срок существует вполне обозримый риск излишней концентрации полномочий в рамках одного органа. В связи с этим существующая система на уровне субъектов Российской Федерации отчасти компенсирует риск излишней концентрации полномочий в рамках одного ведомства, так как приводить в централизованный вид органы субъектов Российской Федерации в отрасли информационных технологий приведет к слишком большим издержкам при не самых очевидных выгодах. На этом основании опасения преобразования системы управления информационных технологий в России в аналог системы управления силовых ведомств маловероятны.

Список литературы

1. Минькович Т. В. Информационные технологии: понятийно-терминологический аспект // Образовательные технологии и общество. 2012. № 2. С. 371–389.

2. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» 27.07.2006 № 149 // Российская газета. 2006. № 165.

3. Постановление Правительства РФ «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации» от 02.06.2008 № 418 // Собрание законодательства Российской Федерации. 2008. № 23. Ст. 2708.

4. Постановление Правительства Москвы «Об утверждении Положения о Департаменте информационных технологий города Москвы» от 05.04.2011 № 105-ПП // Вестник Мэра и Правительства Москвы. 2011. № 22.

5. Постановление Правительства Удмуртской Республики «О Министерстве цифрового развития Удмуртской Республики» от 21.12.2017 № 546 // Официальный сайт Главы Удмуртской Республики и Правительства Удмуртской Республики с изм. и доп. в ред. от 20 июля 2022 г. URL: <http://www.udmurt.ru>

6. Постановления главы администрации Тамбовской области «Об утверждении Положения о департаменте цифрового развития, информационных технологий и связи Администрации Тамбовской области» от 17.08.2022 № 113 // Сайт сетевого издания «Тамбовская жизнь». URL: www.tamlife.ru

7. Указ Главы Республики Бурятия «Об утверждении Положения о Комитете цифрового развития Администрации Главы Республики Бурятия и Правительства Республики Бурятия» от 15.11.2007 № 674 // Бурятия.

8. Постановление Правительства Республики Северная Осетия – Алания «Вопросы Комитета цифрового развития Республики Северная Осетия – Алания» от 01.04.2022 № 122 // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>

9. Постановления Правительства Республики Марий Эл «О внесении изменения в постановление Правительства Республики Марий Эл от 11 ноября 2010 г. № 303» от 18.09.2018 № 380 // Официальный интернет-портал Республики Марий Эл. URL: марийэл.рф

10. Постановление Главы Администрации (Губернатора) Краснодарского края «О создании департамента информатизации и связи Краснодарского края и о внесении изменений в некоторые правовые акты главы администрации (губернатора) Краснодарского края» от 13.01.2011 № 5 // Кубанские новости. 2011.

11. Постановление Правительства Самарской области «Об утверждении Положения о департаменте информационных технологий и связи Самарской области» от 22.12.2010 № 677 // Волжская коммуна. 2010. № 475.

12. Приказ Аппарата Правительства Псковской области «Об утверждении Положения об Управлении цифрового развития и связи Правительства Псковской области» от 01.06.2022 № 13-од. Документ опубликован не был.

13. Закон Республики Хакасия «О системе исполнительных органов государственной власти Республики Хакасия» от 22.12.2010 № 1-ЗРХ // Вестник Хакасии. 2007. № 10.

14. Постановление Совета министров Республики Крым «Об утверждении Положения о Министерстве внутренней политики, информации и связи Республики Крым» от 27.06.2014 № 154 // Документ опубликован не был.

15. Постановление Правительства Забайкальского края «Об утверждении Положения о Министерстве жилищно-коммунального хозяйства, энергетики, цифровизации и связи Забайкальского края» от 20.05.2019 № 198. Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>. 2019.

16. Постановление Губернатора Ставропольского края «Об утверждении Положения о министерстве энергетики, промышленности и связи Ставропольского края» от 16.08.2012 № 559 // Ставропольская правда.

17. Устав «Государственное бюджетное учреждение «Карельский ресурсный центр цифровых технологий» / Государственное бюджетное учреждение «Карельский ресурсный центр цифровых технологий». URL: <https://digital.gov.karelia.ru/upload/iblock/3ee/Ustav.pdf> (дата обращения: 06.08.2022).

18. Подведомственные учреждения и предприятия, находящиеся в ведомственном подчинении // Чукотский автономный округ. URL: <https://чукотка.рф/vlast/organy-vlasti/depprom/podvedomstvennye-uchrezhdeniya.php>

19. Устав 131-пр // Электронный Ульяновск – Правительство для граждан. URL: <https://e-ul.ru/wp-content/uploads/2021/04/Ustav-131-pr.pdf> (дата обращения: 17.08.2022).

20. Государственное унитарное предприятие «Центр информационных технологий» // Министерство транспорта и связи Чеченской Республики. URL: http://mtischr.ru/index.php?option=com_content&view=article&id=75&Itemid=76 (дата обращения: 20.08.2022).

21. ФЦП «Электронная Россия (2002–2010 годы)» / Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: <https://digital.gov.ru/ru/activity/programs/6/#section-results> (дата обращения: 13.03.2022).

22. Государственные услуги в Санкт-Петербурге. URL: <https://gu.spb.ru/> (дата обращения: 10.03.2022).

23. Распоряжение Правительства РФ «О государственной программе Российской Федерации «Информационное общество (2011–2020 годы)» от 20.10.2010 № 1815-р // Собрание законодательства Российской Федерации.

24. Кравчук Н. Ю., Юрков Д. В. Государственные информационные ресурсы Российской Федерации на современном этапе: проблемы и перспективы развития // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. 2017. № 2. С. 116–129.

25. Доля граждан, использующих механизм получения государственных и муниципальных услуг в электронной форме // ЕМИСС. Государственная статистика. URL: <https://fedstat.ru/indicator/43568> (дата обращения: 07.09.2022).

26. Постановление Правительства РФ «Об утверждении Положения о Федеральном агентстве по информационным технологиям» от 30.06.2004 № 319 // Собрание законодательства Российской Федерации. 2004. № 27. Ст. 2782.

27. Указ Президента РФ «О совершенствовании государственного управления в сфере информационных технологий» от 25.08.2010 № 1060 // Собрание законодательства Российской Федерации. 2010. № 35. Ст. 4528.

28. Указ Президента РФ «О системе и структуре федеральных органов исполнительной власти» от 09.03.2004 № 314 // Собрание законодательства Российской Федерации. 2004. № 11. Ст. 945.

29. Садырtdинов Р. Р. Уровень цифровизации регионов России // Вестник Челябинского государственного университета. 2020. № 10. С. 230–235.

30. Карелия оказалась в числе регионов, отстающих в цифровизации госуслуг // Аргументы и факты в Карелии. URL: https://karel.aif.ru/society/details/karelii_okazalas_v_chisle_regionov_otstayushchih_v_cifrovizacii_gosuslug (дата обращения: 03.09.2022).

31. Карелия первой в стране присоединилась к федеральному проекту «Цифровая Россия» // Республика – все новости Карелии и Петрозаводска. URL: <http://rk.karelia.ru/social/kareliya-pervaya-v-strane-prisoedinilas-k-federalnomu-proektu-tsifrovaya-rossiya/> (дата обращения: 03.09.2022).

32. Министерство информационных технологий Ульяновской области // Ульяновская область: Губернатор и Правительство. URL: <https://ulgov.ru/page/index/permlink/id/3043/> (дата обращения: 03.09.2022).

33. Постановление Губернатора Ульяновской области «О мерах по совершенствованию деятельности исполнительных органов государственной власти Ульяновской области» от 28.06.2013 № 123 // Ульяновская правда. 2013. № 75.

34. О Портале // МФЦ Ульяновской области. URL: <https://mfc.ulgov.ru/about/> (дата обращения: 03.09.2022).

35. Алексей Русских утвердил Программу цифровой трансформации области // Медиа 73. URL: <https://media73.ru/2022/aleksey-russkikh-utverdil-programmu-tsifrovoy-transformatsii-oblasti> (дата обращения: 03.09.2022).

В. В. Зубкова,

магистрант,

Национальный исследовательский Нижегородский
государственный университет имени Н. И. Лобачевского

ОСНОВНЫЕ ТЕНДЕНЦИИ ПРАВОВОГО РЕГУЛИРОВАНИЯ РЫНКА БАНКОВСКИХ УСЛУГ В ЕАЭС В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. В настоящей статье рассматривается современное состояние формирования общего рынка банковских услуг в странах ЕАЭС. Сформулированы основные направления гармонизации правового регулирования банковского сектора стран-участниц с учетом развития и необходимости внедрения цифровых технологий, а также с учетом применения к ЕАЭС санкционных ограничений.

Ключевые слова: ЕАЭС, право, цифровые технологии, банковское право, общий рынок

THE MAIN TRENDS IN THE LEGAL REGULATION OF THE BANKING SERVICES MARKET IN THE EURASIAN ECONOMIC UNION (EAEU) IN THE CONTEXT OF DIGITALIZATION

Abstract. The article analyzes the current situation of the formation of a common banking services market in the EAEU. The main trends of the legal regulation'

harmonization of the banking sector of the EAEU countries are formulated, taking into account the development and need for the introduction of digital technologies, as well as taking into account the application of sanctions restrictions to the EAEU.

Keywords: EAEU, Law, Digital technologies, Banking law, Common market

В условиях санкционного давления и перестройки экономической системы Евразийский экономический союз (ЕАЭС) становится альтернативной площадкой для развития торговой интеграции. ЕАЭС – объединение, созданное относительно недавно, но уже показывает определенные позитивные результаты. Большинство экспертов отмечают, что развитие в различных отраслях проходит неравномерно, национальные системы отличаются друг от друга, что порождает необходимость гармонизации национальных систем, национального регулирования и одновременного совершенствования.

Одним из важных направлений развития ЕАЭС является создание общего рынка финансовых услуг, которой завершит собой торговую и экономическую интеграцию. Рынок финансовых услуг формируется из трех основных секторов – банковского, рынка страхования и фондового рынка. Каждый сектор имеет свои тенденции в развитии и особенности на территории государств – участников ЕАЭС. Необходимость создания общего рынка финансовых услуг позволит привлечь больше инвестиций, будет способствовать развитию цифровых технологий и их применения в различных секторах интеграции.

Так, идея создания общего финансового рынка была заложена еще в Договоре о Евразийском экономическом союзе. Статья 103 Договора предусматривает гармонизацию национальных законодательств в сфере финансового рынка, в ней обозначено, что к 2025 г. должен быть сформирован наднациональный орган по регулированию финансового рынка. В Приложении № 17 к Договору – «Протокол по финансовым услугам» – перечислены виды услуг и форма деятельности на данном рынке.

Итак, участники ЕАЭС приняли тенденцию на гармонизацию своих систем и правовых норм для выработки наиболее взаимовыгодного развития. С 2018 г. началась активная работа по выработке единого сектора банковских услуг, в частности в кредитно-денежной и валютно-финансовой политике, и отдельно можно говорить, что одним из направлений было также и повышения уровня доверия ко всей банковской системе. В том же году было подписано соглашений о гармонизации законодательств в финансовой сфере главами национальных банков – участников ЕАЭС.

В следующем, 2019 г. была сформирована Концепция формирования общего финансового рынка, в которой уже были обозначены конкретные методы, задачи и цели формирования, привлечения инвестиций и усиления доверия к новой политике.

Решение Высшего Евразийского экономического совета 2020 г. № 12 «О Стратегических направлениях развития евразийской экономической интеграции до 2025 года» обозначило многие основные требования для регулирования финансового рынка и предстоящие мероприятия в этом секторе. Основными среди них было указаны такие, как: взаимное признание лицензий; осуществление финансовых услуг на всей территории ЕАЭС; административное сотрудничество между уполномоченными органами, в том числе путем обмена информацией. На сегодня

нышний день находится еще на стадии обсуждения программа по формированию единой платежной системы и соглашение об обмене информации по кредитным историям. «Государства-члены самостоятельно разрабатывают, формируют и реализуют национальную политику в сферах цифровизации экономики, связи и информатизации, обеспечения устойчивого функционирования и безопасности единого информационного пространства и инфраструктуры связи, в том числе реализуют национальные мероприятия по развитию цифровой повестки. В целях реализации настоящих Основных направлений государства-члены обеспечивают согласованную политику в соответствии с правом Союза» [12. С. 3].

В банковском секторе на сегодняшний день особо важной является необходимость введения наднационального регулятора, а с учетом политики дедолларизации крайне остро возник вопрос об осуществлении платежей в национальных валютах, с учетом курсовой разницы.

Цифровизация, как новая тенденция в сфере банковских услуг, предполагает развитие и изменение привычных традиционных форм услуг, форм их применения и обмена информации. Это качественно новый этап, предполагающий как и ресурсные затраты, так и формирование обновленной правовой концепции регулирования таких услуг. В цифровой повестке до 2025 г. [11. С. 5] обозначено создание программ цифровизации и применения новых технологий в каждом секторе финансового рынка, создание цифровых платформ и маркетплейсов. Несомненно, в этом секторе будет и трудность в создании общего банковского пространства, связанная с изначальным уровнем экономического развития государств, разноплановыми темпами гармонизации законодательств.

Особую роль в развитии общего банковского пространства играет и Евразийский банк развития (ЕАБР). На сегодняшний день банк участвует в национальных биржевых торгах. С другой стороны, к примеру, попытки разработки единой валюты на территории государств – участников ЕАЭС имели место, но окончательного формирования единой валюты так и не произошло, в связи с чем государства до сих пор для расчетов используют национальные валюты.

Отдельно поднимаются вопросы применения блокчейн-технологий, вопросы кибербезопасности, но политики в этом направлении еще не разработаны, и на сегодняшний день проводятся только первые попытки рассмотреть вопросы, связанные с такими технологиями в реальном их применении.

Одной из успешных политик можно считать соглашение по определению валютных операций, на которые не распространяется введение ограничений, при этом на такие операции направляется обеспечение в части административной и уголовной ответственности. Такой операцией может служить открытие без ограничений счетов в иностранных и национальных валютах. Рассматриваются вопросы взаимного кредитования и финансирования в национальных валютах. При этом применение цифровых технологий не только повышает имидж ЕАЭС в целом, но позволяет говорить о небольшой конкуренции, приводит к снижению затрат на финансовом рынке, упрощает информационную систему.

Борьба с пандемией с 2020 г. внесла коррективы в развитие интеграции объединения в связи с ростом экономических барьеров. Так, на преодоление пандемии государства ЕАЭС привлекли дополнительные финансовые средства, что сказалось

на снижении макроэкономических показателей. За последние два года пандемии реальный совокупный ВВП государств ЕАЭС снизился на 2,9 %, при среднемировом снижении в 3 % [4.С. 98] этот показатель является допустимым. Этот период характеризовался как очередной барьер, выход из которого мог стать направлением на деградацию Союза либо на дальнейшие шаги по его укреплению. Государства ЕАЭС приняли решение остаться в рамках намеченного курса, и такие совместные усилия способствовали быстрому восстановлению национальных экономик. В Евразийской экономической комиссии была создана специальная рабочая группа для проработки общих мер с целью поддержания макроэкономической стабильности во всех сферах деятельности ЕАЭС.

В феврале 2022 г. была создана рабочая группа высокого уровня для дальнейшего укрепления устойчивости экономик стран ЕАЭС, предлагаемые меры которой сейчас направлены на неотложные регулирования в связи с санкционными ограничениями: товарозамещение, налоговое, таможенное и административное регулирование, макроэкономическая политика. На эти направления в первую очередь направлены усилия по интеграции. Финансовый рынок на сегодняшний момент не представляет крайне срочного формирования, в связи с необходимостью решения более конкретных проблем, связанных с введенными ограничениями. При этом планомерное формирование рынка финансовых услуг продолжается в заданном темпе, государства ЕАЭС не планируют вносить изменения в дальнейшую интеграцию и следуют намеченному плану. Соответственно, выбранная тактика формирования общего рынка изначально отвечает интересам всех участников и не требует корректировки даже при усилении санкционного давления.

Среди знаковых проблем, с которыми столкнулся рынок финансовых услуг в последнее время, можно назвать, к примеру, в банковском секторе стран ЕАЭС отсутствие собственных корреспондентских счетов, в связи с чем затруднены либо полностью заморожены переводы финансовых средств. Для фондового рынка важным событием стало лишение Московской биржи (Моех) статуса признанной со стороны Великобритании. Такое действие привело в большей степени к потере репутации биржи, а также к потере налоговых льгот для инвесторов и, соответственно, оттоку инвесторов из Великобритании.

В ходе пленарного заседания Евразийского экономического форума, проходившего в конце мая 2022 г. в Бишкеке, представители стран ЕАЭС высказались за более тесную координацию и дальнейшее взаимодействие. Развитие цифровых технологий также было указано как основное для углубления интеграции в экономике между членами Союза. Отмечались на форуме успехи по достижению гармонизации национальных правовых систем, особое внимание уделяется на сегодняшний день разработке международного договора о взаимном признании ценных бумаг, выпущенных в одном из государств-участников другими участниками в рамках Союза. Потенциал ЕАЭС значителен, и в рамках беспрецедентных ограничений, которым подвергнуты некоторые государства – участники Союза, в частности Россия и Белоруссия, заставляет государства активнее формировать общий рынок, в том числе и в финансовой сфере. Преимущества такой интеграции на сегодняшний день очевидны и позволят в будущем не только противостоять санкционному давлению, но и улучшить экономические показатели стран ЕАЭС. Налаживание связей и заключение новых соглашений ЕАЭС

с другими участниками мирового рынка также становятся необходимостью. На форуме было заявлено, что активно прорабатываются вопросы заключения соглашения о свободной торговле с Ираном (на данный момент заключено только Временное соглашение), Индонезией и рассматривается вопрос о заключении торгового соглашения с Объединенными Арабскими Эмиратами.

Создание общего банковского рынка не возможно без внедрения новых финансовых технологий, необходимых для нормального функционирования информационных систем внутри и для создания более привлекательной модели для привлечения третьих стран, создания инвестиционных зон.

Для правового регулирования общий банковский рынок ЕАЭС требует огромной работы. Каждый этап как внутри функционирования системы, корректного применения новых технологий, взаимоотношений с другими государствами должен быть детально изучен в правовом отношении.

Список литературы

1. Андрияшин С. А., Кузнецова В. В. Финансовые рынки, технологические инновации и финансовая стабильность: риски и проблемы регулирования // Актуальные проблемы экономики и права. 2019. Т. 13, № 3. С. 1315–1329.
2. Мещерякова О. М. Правовое регулирование финансовой сферы в Европейском союзе и формирование единого рынка финансовых услуг // Международное право. 2019. № 3. С. 8–13.
3. Лифшиц И. М. Теоретические основы взаимодействия международного финансового права и права Европейского союза: дис. ... д-ра юрид. наук. Москва, 2020. 578 с.
4. Доклад Евразийской экономической комиссии «О реализации основных направлений интеграции в рамках Евразийского экономического союза». Москва, 2018.
5. Отчет о научно-исследовательской работе по теме «Разработка Стратегии развития финансовых рынков государств – членов ТС и ЕЭП на период до 2025 года». 3-й этап. Москва, 2015. URL: http://www.mirkin.ru/_docs/report3-08082014.pdf
6. Касьянов Р. А. Регулирование рынка финансовых услуг по праву ЕС и ЕАЭС: монография / под ред. д-ра юрид. наук, профессора Г. П. Толстопятенко. Москва: МГИМО – Университет, 2021. 749 с.
7. The Economic Dimension of Eurasian Integration / ed. N. A. Piskulova. Palgrave Macmillan, 2021. 236 p.
8. Договор о Евразийском экономическом союзе (Астана, 29.05.2014). URL: <http://www.consultant.ru> (дата обращения: 19.05.2022).
9. Распоряжение Евразийского межправительственного совета от 07.03.2017 № 2 «О сферах экономики, обладающих интеграционным потенциалом в Евразийском экономическом союзе, и мерах, направленных на его использование». URL: <https://www.alt.ru/tamdoc/17mr0002/> (дата обращения: 11.05.2022).
10. Распоряжение Совета Евразийской экономической комиссии от 23.11.2020 № 27 «О плане мероприятий по гармонизации законодательства государств – членов ЕЭС в сфере финансового рынка» // Альта-софт. URL: <https://www.alt.ru/tamdoc/20s00027/> (дата обращения: 05.05.2022).

11. Распоряжение Совета ЕЭК от 17.03.2022 № 12 «О реализации мер по повышению устойчивости экономик государств – членов Евразийского экономического союза, включая обеспечение макроэкономической стабильности». URL: https://docs.eaeunion.org/docs/ru-ru/01431501/err_18032022_12 (дата обращения: 18.05.2022).

12. Решение № 12 Высшего Евразийского экономического совета «О Стратегических направлениях развития евразийской экономической интеграции до 2025 года». URL: https://docs.eaeunion.org/docs/ru-ru/01428320/err_12012021_12 (дата обращения: 10.05.2022).

13. Решение от 01.10.2019 № 20 Высшего Евразийского экономического совета «Концепция формирования общего финансового рынка Евразийского экономического союза». URL: <https://eec.eaeunion.org/upload/medialibrary/881/29.-Obshchiy-finansovyy-rynok.pdf> (дата обращения: 10.05.2022).

14. Концепция общего финансового рынка Евразийского экономического союза. 27 июня 2019 г., Москва. URL: https://cbr.ru/Content/Document/File/72918/q_1.pdf (дата обращения: 18.05.2022).

15. Борщ Л. М., Герасимова С. В. Развитие финансовых рынков стран ЕАЭС с применением IT-технологий // Научный вестник: Финансы, банки, инвестиции. 2021. № 4. С. 43–55.

16. Голодова Ж. Г., Гречкин Н. В. Развитие финансовой интеграции в условиях внедрения финансовых технологий в странах Евразийского экономического союза // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 1. С. 166–179.

17. Гурский В. Л. Перспективы развития международной экономической интеграции государств-членов ЕАЭС в условиях глобальных изменений в мировой экономике // Экономическая наука сегодня: сб. науч. ст. / БНТУ. Минск, 2020. Вып. 12. С. 91–99.

18. Лидеры стран ЕАЭС обсудили перспективы развития Союза на пленарном заседании Евразийского экономического форума в Бишкеке. URL: <https://eec.eaeunion.org/be/news/lidery-stran-eaes-obsudili-perspektivy-razvitiya-soyuza-na-plenarnom-zasedanii-evraziyskogo-ekonomich/> (дата обращения: 18.05.2022).

19. Оценка интеграционных процессов ЕАЭС в сфере торговли: 2022: междунар. докл. к XXIII Ясинской (Апрельской) междунар. науч. конф. по проблемам развития экономики и общества. Москва, 2022 / М. К. Глазатова (рук. авт. кол.), С. С. Агаджанян, А. С. Амирбекова и др.; Нац. исслед. ун-т «Высшая школа экономики». Москва: Изд. дом Высшей школы экономики, 2022. 64 с.

20. План мероприятий гармонизации национальных законодательств в финансовой сфере Евразийского экономического союза на 2015–2030 гг. («дорожная карта») / под ред. д-ра экон. наук И. Н. Рыковой. Москва: Научно-исследовательский финансовый институт, 2015. 42 с.

21. Яник А. А. Цифровое пространство ЕАЭС: актуальное состояние и перспективы // Международное право и международные организации / International Law and International Organizations. 2021. № 3.

22. Andrei Yeliseyeu The Eurasian Economic Union: Expectations, Challenges, and Achievements. 2019 German Marshal Fund. URL: <https://www.gmfus.org/news/eurasian-economic-union-expectations-challenges-and-achievements> (дата обращения: 18.05.2022).

Л. И. Ивардава,

аспирант,

Институт законодательства и сравнительного правоведения
при Правительстве Российской Федерации

СУБЪЕКТ ПРАВА В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ В РОССИИ

Аннотация. Право и цифровизация оказывают взаимное влияние друг на друга в самых разнообразных сферах на макро и микро уровнях. При этом субъект права испытывает сильное воздействие со стороны цифровых технологий, цифровой экономики, что неизбежно сказывается на трансформации его статуса, характере и деятельности. С возникновением и активным распространением Интернета и современных технологий субъект права получает новые возможности, в том числе по созданию цифрового двойника, виртуальной личности, что для права является новыми феноменами. В статье рассматривают отдельные юридические вопросы, связанные с трансформацией субъекта права в условиях развития интернет-технологий.

Ключевые слова: цифровая экономика, субъект права, виртуальная личность, цифровой образ, персональные данные, идентификация субъекта

THE SUBJECT OF LAW IN THE CONTEXT OF THE DEVELOPMENT OF THE DIGITAL ECONOMY IN RUSSIA

Abstract: Law and digitalization have a mutual influence on each other in a wide variety of areas at the macro and micro levels. At the same time, the subject of law is strongly influenced by digital technologies, the digital economy, which inevitably affects the transformation of its status, nature and activities. With the emergence and active spread of the Internet and modern technologies, the subject of law receives new opportunities, including the creation of a digital double, a virtual personality, which are new phenomena for law. The article considers certain legal issues related to the transformation of the subject of law in the context of the development of Internet technologies.

Keywords: Digital economy, Legal entity, Virtual personality, Digital image, Digitalization of the economy, Personal data, Identification of the subject.

Безусловно, одна из главных проблем цифровой эпохи – изменение основных компонентов права и государства [5]. Если использовать определение права как комплекса норм, которые регулируют отношения, существующие между субъектами относительно определенного объекта [9. С. 6], то становится очевидным, что в новую эпоху, связанную с появлением цифровых технологий, необходимо уточнить каждый их представленных элементов. Важно отметить, что меняется сам концепт субъекта права.

В классической теории права субъектами права выступают государство, физические и юридические лица, однако в обществе постмодерна классические концепции и модели меняются, что наглядно показано в современной научной литературе [2. С. 22-37; 3. С. 104-120; 4]. С возникновением и активным распро-

странением Интернета субъект права получает новые возможности, например, физическое лицо может скрываться под цифровым образом или виртуальной личностью. В Интернете реальное имя субъекта отношений может быть заменено псевдонимом. Однако в сети Интернет размещаются персональные данные того же субъекта, которые представляют собой согласно российскому законодательству [10; 11] информацию, относящуюся к определенному или же определяемому физическому лицу (подобным образом персональные данные понимаются в том числе при распространении данных через Интернет).

Интернет предоставил большее количество возможностей определения лица, скрывающегося за цифровым образом, при помощи косвенных средств, в том числе через сопоставление ряда данных. Благодаря этому потенциальный злоумышленник может идентифицировать личность без формального нарушения правил автоматической обработки данных. Таким образом, в данной ситуации цифровые технологии повышают вероятность действий, идущих вразрез с правами физического лица и при этом формально не наказуемых.

Кроме того, персональные данные тесно взаимосвязаны со служебным имиджем. Иллюстрация данной связи проявляется в случаях особого контроля государственных служащих, когда слова и действия этих лиц записываются на аудио, видео и т. д.

Согласно российскому законодательству [12] государственные гражданские служащие не имеют права распространять информацию от своего имени. Таким образом, государственные гражданские служащие и граждане, претендующие на замещение должностей государственной гражданской службы, должны предоставить своему нанимателю необходимые сведения, касающиеся адресов сайтов и / или страниц сайтов в Интернете, где данный гражданин размещал общедоступную информацию, а кроме того, те данные, которые могут служить источником его идентификации. Следовательно, посредством данного закона затрагиваются использование гражданами социальных сетей типа Facebook (социальная сеть, которая в России признана экстремистской и запрещена), а также всевозможные публичные комментарии.

Исходя из этого, можно сделать вывод, что идентификация лица в Интернете представляет собой разностороннюю проблему, которая может послужить причиной нарушения прав разнообразных субъектов [9. С 7].

Решение этой проблемы может быть различными способами.

Первый – смириться с тем, что идентификация субъекта права в Интернете может быть вообще невозможной, поскольку, несмотря на то что при помощи технических способов идентификации возможно создать юридическую фикцию, остается невозможной окончательная идентификация субъекта права. По словам Р. Ф. Азизова, результатом этого становится «принципиально новая для теоретического осмысления ситуация, в которой цикл жизни правового отношения может происходить без юридически значимой идентификации его субъектов, которая, более того, может в принципе быть практически невозможной (например, в случае с децентрализованными сетями, построенными по принципу анонимности с использованием алгоритмов шифрования)» [1, С. 18].

Второй – признать за персональными данными качество объекта гражданского права, который может быть коммерциализирован, а, следовательно, является отчуждаемым [8]. Отметим также, что в утратившей силу программе «Цифровая экономика Российской Федерации» [6], по сути, содержалось предположение касательно применения к персональным данным виртуальной личности режима права собственности.

Помимо упомянутого комплекса вопросов, касающихся персональных данных, существуют и другие проблемы, связанные с правами физического лица в Интернете. Например, это право на забвение или право на цифровую смерть.

В цифровую эпоху человек практически потерял возможность уйти без цифрового следа, остающегося после смерти. Однако в данной сфере необходимо предоставить человеку как субъекту право выбора. Исходя из этой концепции родилось так называемое право на забвение (right to be forgotten), которое закреплено, в том числе в российском законодательстве.

В этом же ряду стоит право на цифровую смерть, которое предполагает, что лицо имеет право на соблюдение его воли после его смерти касательно персональной информации, опубликованной в Интернете после его смерти поставщиками интернет-услуг или же доверенными лицами. С точки зрения теории права это означает, что права субъекта при помощи Интернета в определенном смысле продлеваются после его кончины.

Также у физического лица появляются в Интернете другие права, значительная часть которых распространяется и на юридические лица. Такие права называются цифровыми, и их источником являются разнообразные правовые документы: Конституция Российской Федерации и Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [10], а также судебная практика, в том числе практика Европейского суда по правам человека. Такими правами являются, например, право на изображение, право на доступ в Интернет и т.п.

Основываясь на анализе данных процессов, можно сделать вывод, что информационное общество привело к трансформации такой правовой ценности, как свобода, и в частности, свобода слова. Трансформации подверглось также право на информацию и доступ к информации, и они в совокупности со свободой слова стали универсальным товаром, структура которого представляет собой данные о человеке и его сообщениях в Интернете [7].

На основании вышеизложенного можно сделать два вывода. Во-первых, одним из результатов цифровизации общества стала трансформация ценностей права. Во-вторых, вследствие цифровизации на первый план в цифровом мире выходит вопрос обеспечения прав человека.

Список литературы

1. Азизов Р. Ф. Правовое регулирование в сети Интернет: сравнительно и историко-правовое исследование: автореф. дис. ... д-ра юрид. наук. СПб., 2017.
2. Залоило М. В. Законность и целесообразность в обществе постмодерна: пересмотр сложившейся классической модели // Журнал российского права. 2020. № 6. С. 22–37.

3. Залоило М. В. Субъект права и динамика его правового статуса в условиях цифровизации // Вестник Московского городского педагогического университета. Серия «Юридические науки». 2021. № 3 (43). С. 104–120.

4. Залоило М. В., Пашенцев Д. А. Национальный правопорядок России в условиях цифровизации // Вестник Санкт-Петербургского университета. Право. 2019. № 2.

5. Концепция цифрового государства и цифровой правовой среды: монография / под общ. ред. Н. Н. Черногора, Д. А. Пашенцева. Москва: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: Норма: ИНФРА-М, 2021.

6. Программа «Цифровая экономика Российской Федерации»: Утв. распоряжением Правительства Российской Федерации от 28.07.2017 № 1632-р (утратила силу).

7. Родимцева М. Ю. Регулировать нельзя манипулировать (о рисках информационного общества) // Государство и право. 2016. № 7.

8. Савельев А. И. Правовая природа «облачных» сервисов: свобода договора, авторское право и высокие технологии // Вестник гражданского права. 2015. № 5.

9. Талапина Э. В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2.

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

11. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ, 31.07.2006, № 31, ст. 3451.

12. Федеральный закон от 30.06.2016 № 224-ФЗ «О внесении изменений в Федеральный закон «О государственной гражданской службе Российской Федерации» и Федеральный закон «О муниципальной службе в Российской Федерации» // Собрание законодательства РФ, 04.07.2016, № 27, ст. 4157.

П. А. Иллюк,

аспирант,

Институт законодательства и сравнительного правоведения
при Правительстве Российской Федерации

ПРАВОВОЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: ОПЫТ ИНДИИ

Аннотация. Индия – страна ярко выраженных контрастов. С одной стороны, она сохранила богатые традиции прошлого и до сих пор в ряде вопросов ориентируется на легендарные Законы Ману, с другой стороны, она старается идти в ногу со временем, особенно в сфере развития информационных технологий. Как известно, Индия является глобальным IT-гигантом, что стало возможным в том числе благодаря умному регулированию сферы информационных техноло-

гий, заложенному 17 октября 2000 года, когда в стране был принят Акт об информационных технологиях (IT Act). История становления и совершенствования правового регулирования в сфере информационных технологий являются предметом настоящего исследования.

Ключевые слова: Акт об информационных технологиях, цифровое право, индийское право, IT-право, кибертерроризм, Индия

LEGAL REGULATION IN THE FIELD OF INFORMATION TECHNOLOGY: THE EXPERIENCE OF INDIA

Abstract. India is a country of pronounced contrasts. On the one hand, she has preserved the rich traditions of the past and still focuses on the legendary Laws of Manu in a number of issues, on the other hand, she tries to keep up with the times, especially in the field of information technology development. As you know, India is a global IT giant, which became possible, among other things, thanks to the smart regulation of the information technology sector, laid down in 2000, when the country adopted the Information Technology Act. The history of legal regulation and its improvement are the subject of this study.

Keywords: Information Technology Act, Digital Law, Indian Law, IT Law, Cyberterrorism, India

Введение. Масштабное развитие цифровых технологий охватило все передовые страны мира. Современные ученые отмечают, что вступление современных государств в эпоху шестого технологического уклада приводят к существенным изменениям самого устройства государства и права [7; 8]. Одним из таких государств является Индия — страна ярко выраженных контрастов. С одной стороны, она сохранила богатые правовые традиции прошлого и до сих пор в ряде вопросов ориентируется на легендарные Законы Ману, а с другой стороны, она старается идти в ногу со временем, особенно в сфере развития информационных технологий. Как известно, Индия является глобальным IT-гигантом, что стало возможным в том числе благодаря умному регулированию сферы информационных технологий, заложенному в 2000 году, когда в стране принимается Акт об информационных технологиях (IT Act) [1].

Главная идея принятия закона заключалась в том, чтобы юридически признать и развить интернет-торговлю одновременно обезопасить участников этих отношений от киберпреступлений. С развитием современных технологий количество преступлений, совершенных в сети Интернет, резко увеличилось, и довольно быстро возникла необходимость повысить кибербезопасность путем совершенствования правового регулирования. В итоге в целях усиления правовой защиты от киберпреступлений в 2008 году в Акт об информационных технологиях были внесены ряд важных изменений. Эффективные правовые решения возникающих отношений в сфере информационных технологий позволили Индии стать ведущей страной в области IT-индустрии.

Основная часть. Акт об информационных технологиях Индии (IT Act) был принят 17 октября 2000 года. В первую очередь IT Act был разработан для развития

электронной торговли и электронного государства в Республике Индия, для создания правового обеспечения информационных технологий [4. Р. 333]. Первоначально Акт содержал 94 раздела, разделенных на 13 глав и 4 приложения. Действие Акта распространялось на всю территорию Республики Индия, его юридическая ценность заключалась в признании электронной коммерции, уравнивании электронных операций с бумажными, юридическом признании цифровых подписи. Были даны определения таким понятиям как «компьютер», «данные», «доступ», «информация» и т.д. Также был создан апелляционный трибунал по киберправу для рассмотрения апелляций на судебные органы. Однако положения данного акта не распространяется на оборотные инструменты, доверенности, траст, завещание и любой договор купли-продажи или передачи недвижимого имущества.

Кроме того, Уголовный кодекс Индии 1860 г. был признан недостаточным для противодействия новым преступлениям, возникающих в условиях распространения Интернета, так как некоторые из преступлений, возникших задолго до изобретения Интернета (например, сговор, вымогательство, ценные бумаги, мошенничество, шпионаж) стали совершаться в новом для себя пространстве — Интернете. Закон об информационных технологиях 2000 г. восполнил этот пробел в части совершенствования правового регулирования предотвращения киберпреступлений и борьбы с ними [5; 6]. Так, глава XI рассматриваемого акта была дополнена такими составами правонарушений, как фальсификация исходных компьютерных документов, взлом компьютерной системы, публикация информации непристойного содержания в электронном виде, а в 2009 году был введено новый состав преступления, получивший название кибертерроризм.

Кибертерроризмом признавались любые действия, совершенные с намерением угрожать единству, целостности, безопасности или суверенитету Индии или вызывающие террор путем проведения DoS-атак, внедрения компьютерных вирусов, несанкционированного доступа к компьютерным ресурсам, кражи конфиденциальной информации, любой информации, которая может вызвать ущерб интересам суверенитета или целостности Республики Индии, безопасности, дружественным отношениям с другими государствами, общественному порядку, порядочности, морали, неуважение к суду, распространение порочащих сведений, или подстрекательство, либо в пользу любого иностранного государства, либо в пользу группы лиц или иным образом [5. Рр. 1743–1744; 6. Р. 201–204].

Представляет интерес раздел 69А Акта об информационных технологиях, которые наделяет правительство полномочиями издавать по блокировке доступа к веб-сайтам, которые считались несоответствующими индийским стандартам порядочности, морали и общественного порядка [3. Р. 312]. Однако в 2015 г. Акт о внесении поправок 2009 г. был признан неконституционным на том основании, что его терминология не была конкретизирована. Толчком к такому решению стало дело Шрея Сингхал против Союза Индии. Шрейя Сингхал, студентка 2-го курса юридического колледжа, подала исковое заявление от 29 ноября 2012 г. в Верховный суд, в котором требовала оспорить конституционность раздела 69А. Ходатайство о судебном приказе было принято и объединено с другими ходатайствами со схожими требованиями. Суд признал неконституционным положения раздела 69А, однако, отмены раздела не последовало [2. Рр. 2–4].

В 2022 г. Министерство по информационным технологиям Индии предложило новые поправки к Акту об информационных технологиях. Во-первых, было предложено закрепить в акте такие понятия как ложная информация, угроза («означает любое выражение посредством слова, звука, жеста или любое аудио-визуальное сообщение с намерением причинить вред, тревогу, запугивание или домогательство, либо подстрекательство к причинению вреда, тревоги, запугивания или домогательства со стороны любого лица»). Во-вторых, в главу XI было предложено добавить новый раздел, в котором будут указаны правонарушениями против женщины с намерением запугать или дискредитировать ее (раздел включает в себя угрозу физического насилия в отношении женщины, ее семьи или ее имущества; угрозу сексуального насилия; угрозу раскрытия личной информации, включая, помимо прочего, ее местонахождение, место работы и любую другую соответствующую информацию, которая может быть использована для причинения ей физического вреда; угрозу распространения о ней ложных сведений и т.д.).

Выводы. Акт об информационных технологиях 2000 г. является главным нормативно-правовым актом, регулирующим отношения в сфере цифровых технологий. Поправка 2008 г. была инициирована с целью решения актуальных заполнения пробелов в праве. Последовали такие изменения как переопределение термина «устройство связи», закрепление четырех типов электронной подписи, разрешение центральному правительству Индии перехватывать, отслеживать, расшифровывать и блокировать данные в Интернете по своему усмотрению. В 2022 г. были предложены новые поправки к Акту об информационных технологиях. Несмотря на то, что Акт об информационных технологиях далек от идеала, его существование необходимо в индийском законодательстве, так как он является символом технологического прогресса и упорядочивает деятельность в сети Интернет. Однако, Акт об информационных технологиях 2000 г. крайне перегружен не только технической терминологией, но и нормами уголовно-правового характера. Также в нем имеются термины, которые не получили раскрытие (например, «кибертерроризм»), поэтому точное их понимание вызывают сложности в области правоприменительной практики.

Список литературы

1. Act of the Indian Parliament No 21 notified on 17 October 2000 (The Information Technology Act, 2000). URL: <https://www.meity.gov.in/content/information-technology-act-2000>.
2. Chanakya J. P., Chanakya A. A. (2021). An Analysis of Constitutional Validity of Section 66A, I.T. Act, 2000 / Volume 15, April 2021, Pen Acclaims, с. 1-12.
3. Halder D. (2021). PUBG Ban and Issues of Online Child Safety During COVID-19 Lockdown in India: A Critical Review from the Indian Information Technology Act Perspectives / Temida 2021 Volume 24, Issue 3, Pages: 303-327.
4. Pandey U., Shukla. S. (2016). E-commerce and mobile commerce technologies. Material type: Text Publication details: New Delhi S. Chand. 2016. 594 с.
5. Praveen Raj S., Rajan A. (2012). Comparison between Information Technology Act, 2000 & 2008, International Journal of Pure and Applied Mathematics, Vol. 119, No. 17, 1743-1744.

6. Rebecca M. K. (2012). The Netizen, *Development* 55(2), 201–204.

7. Концепция цифрового государства и цифровой правовой среды: монография / под общ. ред. Н. Н. Черногора, Д. А. Пашенцева. Москва: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: Норма: ИНФРА-М, 2021. 244 с.

8. Смена технологических укладов и правовое развитие России: монография / Д. А. Пашенцев, М. В. Залоило, А. А. Дорская. Москва: ИЗиСП: Норма: ИНФРА-М, 2021. 184 с.

М. А. Иманалиева,

магистрант,

стажер-исследователь,

Институт исследований национального и сравнительного права

ОСОБЕННОСТИ РЕГУЛИРОВАНИЯ ОНЛАЙН-ИГР ЧЕРЕЗ ПРИЗМУ ЗАЩИТЫ ПРАВ И ИНТЕРЕСОВ НЕСОВЕРШЕННОЛЕТНИХ

Аннотация. В данной статье отмечаются существующие риски участия несовершеннолетних в онлайн-играх и предлагаются способы их минимизации. Российская правовая база взята за основу исследования. В качестве элемента сравнительно-правового анализа используются положения законов КНР. В статье сравниваются подходы к защите прав несовершеннолетних пользователей онлайн-игр в России и КНР.

Ключевые слова: право, цифровые технологии, онлайн-игры, несовершеннолетние, цензура

FEATURES OF REGULATION OF ONLINE GAMES THROUGH THE PRISM OF PROTECTION OF THE RIGHTS AND INTERESTS OF MINORS

Abstract. This article notes the existing risks of minors participating in online games and suggests ways to minimize them. The Russian legal framework is taken as a basis, and the provisions of the laws of the PRC are used as an element of comparative legal analysis. The article gives a general understanding of the approach to protecting the rights of underage users of online games in Russia and China.

Keywords: Law, Digital technologies, Online games, Minors, Censorship

Для многих людей онлайн игры стали частью привычной жизни, без которой они не могут представить свой день. Для многих людей это возможность социализации, для кого-то попытка снять стресс. Так или иначе, онлайн-игры становятся все более и более популярными. Данная тенденция очевидна и среди несовершеннолетних.

Для детей онлайн-игры сопряжены как с положительными аспектами, к примеру, это может обеспечить их общением со сверстниками, развить кругозор и дать понимание того, как работают новые технологии, тем не менее негативные аспекты тоже присутствуют. Видится оправданным сосредоточиться исключительно

на рисках информационной безопасности несовершеннолетних и не углубляться в иные вопросы. Так, к рискам можно отнести:

1. Несанкционированные внутриигровые покупки.
2. Доступ к неприемлемому контенту.
3. Кибербуллинг и домогательства [8].
4. Вербовка и пропаганда нетрадиционных ценностей.
5. Заражение вирусным программным обеспечением.
6. Нарушение режима конфиденциальности [9].

В рамках отечественного правового порядка существует правовая база, которая призвана защитить права и интересы детей в информационном пространстве. Основным законом в данной сфере стоит считать Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию», где закреплена классификация информационной продукции, ранжированная по возрастным группам. А также установлены требования к обороту информационной продукции.

Отдельного внимания заслуживает классификация информационной продукции, поскольку правильная маркировка способна снизить риск наступления неблагоприятных последствий для ребенка. Законодатель выделил четыре категории по возрастному критерию [7]:

- 1) информационная продукция для детей, не достигших возраста шести лет.

К таковой относится не причиняющая вреда здоровью и (или) развитию детей (в том числе информационная продукция, содержащая оправданные ее жанром и (или) сюжетом эпизодические ненатуралистические изображение или описание физического и (или) психического насилия (за исключением сексуального насилия) при условии торжества добра над злом и выражения сострадания к жертве насилия и (или) осуждения насилия).

- 2) информационная продукция для детей, достигших возраста шести лет.

Данная категория дополнена информацией о заболеваниях, катастрофах и описание некоторых насильственных действий используемые с целью их осуждения.

- 3) информационная продукция для детей, достигших возраста двенадцати лет.

Указанная категория дополняется возможным описанием или изображением жестокости и насилия (при условии, что выражается сострадание к жертве), допускается эпизодическое упоминание алкогольных и наркотических веществ, а также упоминание о половых отношениях.

- 4) информационная продукция для детей, достигших возраста шестнадцати лет.

Перечень информации данной категории расширен иллюстрацией насилия и смерти (без показа их последствий), допускается нецензурная брань, информация о наркотических и психотропных средствах (не призывающих к их употреблению) и описание половых отношений.

Ранжирование информационной продукции по возрасту – это воспринятая во всем мире практика. Однако, очевидно, что ранжирование по возрасту не может свести к минимуму все риски, связанные с участием несовершеннолетних в онлайн-играх. Так, к примеру, категоризация информационной продукции по возрасту не способна снизить риск внутриигровых покупок, кибербуллинга, нарушение режима конфиденциальности персональных данных несовершеннолетних и т. д. Иными словами, категоризация лишь ограничивает доступ к неприемлемому контенту.

Защита персональных данных несовершеннолетних в рамках российского правопорядка на данный момент также сопряжена с рядом трудностей. Одной из наиболее существенных можно считать отсутствие четкого закрепления возраста, с которого несовершеннолетний может самостоятельно давать согласие на обработку персональных данных. В ч. 6 ст. 9 Федерального закона «О персональных данных» указана обязанность представительства в отношении недееспособных. Несовершеннолетние же являются ограниченно дееспособными. В возрасте до 14 лет все сделки от имени малолетних совершают их законные представители (п. 1 ст. 28 ГК РФ). В возрасте от 14 до 18 лет объем дееспособности становится существенно шире и включает в себя возможность совершать мелкие бытовые сделки, распоряжаться собственными денежными средствами и т. д. В этой связи можно прийти к выводу, что по достижении 14 лет несовершеннолетний может самостоятельно давать согласие на обработку персональных данных.

В этой связи можно представить ситуацию, в которой двенадцатилетний несовершеннолетний захотел сыграть в онлайн-игру. При регистрации пользователю необходимо указать свой возраст для того, чтобы получить доступ к игре. На данный момент нет какого-либо специального порядка идентификации ребенка в сфере онлайн-игр. Любой несовершеннолетний может создать профиль, отвечающий требованиям поставщика игры и получить доступ. Данная проблема остро стоит не только в рамках российского порядка, но и за рубежом. В качестве положительного примера можно рассмотреть комплексный подход законодателя КНР к регулированию данной проблемы.

Закон КНР «О защите несовершеннолетних» направлен, в том числе на обеспечение защиты персональных данных несовершеннолетних [1]. В ст. 72 указано, что согласие на обработку персональных данных ребенка до 14 лет должны давать его опекуны и родители, удаление или изменение информации должно также проходить по их инициативе. В случае если администратор веб-сайта или поставщик мобильного приложения обнаружит, что несовершеннолетний раскрывает свои персональные данные, он должен принять необходимые меры для обеспечения их безопасности. Более конкретная информация, относительно согласия дается в Положении «О защите персональных данных несовершеннолетних в интернете». В Положении в ст. 10 отмечается, что оператор должен предоставлять возможность отказа и четко информировать родителя и опекуна относительно следующих вопросов:

- 1) цель, метод и объем сбора данных, а также порядок их хранения и использования;
- 2) срок и способ обработки персональных данных;
- 3) меры защиты персональных данных;
- 4) последствия отказа;
- 5) каналы и методы подачи жалоб;
- 6) порядок удаления данных.

Хотя законом предъявляются требования к наличию согласия родителя или опекуна, а также требования к их информированию, какие-либо конкретные способы получения согласия отсутствуют [3]. Некоторые мобильные приложения используют методы мгновенной проверки, к примеру, по номеру телефона или посредством информации о документе, удостоверяющим личность. Однако даже такую

проверку ребенок может пройти самостоятельно без ведома родителей. Более того, сложная система проверки экономически затратная, это может привести к тому, что разработка игровых приложений для детей будет невыгодна. В этой связи, законодатели и правоприменители в различных странах обеспокоены технической стороной порядка получения согласия родителей на обработку персональных данных детей.

Успехов в отношении реальной идентификации детей достигла сфера онлайн-игр. Государство создало единую систему аутентификации личности, через которую пользователь может попасть в игру. Закон КНР «О защите несовершеннолетних» обязал поставщиков онлайн-игр требовать от несовершеннолетних регистрации и прохождения аутентификации [1]. Система аутентификации обязывает поставщика онлайн-игры требовать от несовершеннолетних входа в игры с реальной идентификационной информацией. Поставщики онлайн-игр должны классифицировать игровые продукты и давать соответствующие возрасту напоминания в соответствии с соответствующими национальными правилами и стандартами, а также принимать технические меры для предотвращения доступа несовершеннолетних к ненадлежащим играм или игровым функциям. Поставщикам услуг онлайн-игр не разрешается предоставлять услуги онлайн-игр несовершеннолетним с 22:00 до 8:00 следующего дня [1].

Таким образом, благодаря созданию единой системы аутентификации китайский законодатель свел к минимуму риск наступления таких неблагоприятных ситуаций как кибербуллинг, заражение компьютера вредоносным программным обеспечением, разглашение персональных данных и совершение несанкционированных внутриигровых покупок.

Согласно статистике, среднестатистический пользователь Интернета в возрасте от 16 до 64 лет проводит онлайн 6 часов 43 минуты ежедневно. Конкретной статистики относительно времени, которое пользователи проводят, играя в онлайн-игры, не удалось найти, однако с уверенностью можно сказать, что достаточно для того, чтобы обратить внимание на вопрос цензуры. По мнению И. С. Репина «Интернет является очень «удобной» площадкой для пропаганды экстремистских взглядов среди молодежи. Это объясняется возможностью создавать сообщества вне зависимости от географического положения ее создателя. При этом его личность может оставаться анонимной, участники могут обмениваться различными материалами, оговаривать готовящиеся мероприятия» [5]. С данным мнением сложно не согласиться. Зачастую в онлайн-играх и пользователей есть свой профиль, а также чат для обмена мгновенными сообщениями и в случае, если доступ к онлайн-игре в течение суток имеют более 500 000 пользователей, то ее вполне можно признать социальной сетью [6]. В таком случае поставщик онлайн-игры обязан не допускать к распространению следующий контент:

- 1) призывающий к совершению уголовно наказуемых деяний, разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, распространению материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости и материалов, содержащих нецензурную брань;

2) порочащий честь и достоинство человека или группы людей по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства и работы, а также в связи с их политическими убеждениями.

Помимо этого предусмотрена обязанность по мониторингу и своевременному удалению определенного контента:

- 1) содержащие порнографические изображения несовершеннолетних;
- 2) информация о наркотических средствах;
- 3) информация о способах совершения самоубийства и содержащая призывы к совершению самоубийства;
- 4) информация, направленная на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий;
- 5) информация, содержащая призывы к массовым беспорядкам, осуществлению экстремистской деятельности;
- 6) информация, унижающая человеческую честь и достоинство и т. д.

Такого рода цензуру можно охарактеризовать как последующую легитимную цензуру, т. е. ту, которая направлена на удаление уже существующей информации. Однако в законе не содержится упоминания об активной предварительной цензуре, цель которой – регулирование создания контента, а не последующая реакция на него [2].

В данном случае интересен подход КНР. Онлайн-игры, игры, фильмы, литература и так далее урегулированы специальным актом – Указом об управлении публикациями [4]. Фактически, это ключевой акт о цензуре. Основная идея закреплена в ст. 3 Указа – «Издательская деятельность должна соответствовать целям:

- служению людям и социализму;
- придерживаться истоков марксизма-ленинизма, мысли Мао Цзэдуна, теории Дэн Сяопина;
- быть направленной на реализацию научного развития;
- способствовать экономическому и социальному развитию».

Более того, деятельность должна быть направлена на пропаганду национальной культуры, содействию международному культурному обмену и иметь целью обогащение и улучшение духовной жизни людей, что, по мнению китайских ученых, позитивно сказывается на формировании культурных ценностей и ценностных ориентаций у несовершеннолетних [10].

Ответственный за цензуру орган – Отдел управления публикациями при Государственном Совете. Данный отдел вправе проводить ежедневную проверку на предмет соответствия цензуре. Важно понимать, что требования о соответствии цензуре фактически переданы на усмотрение уполномоченного органа, поскольку требования закона сформулированы максимально широко.

В случае выявления несоответствий уполномоченный орган вправе требовать прекращения распространения незаконного контента и привлекать к ответственности владельцев игр и иных ресурсов. Штрафы за незаконное распространение материалов очень высокие и достигают десятикратного размера от незаконного оборота.

Установлены требования цензуры к произведениям, а именно произведения не должны:

- 1) нарушать основные принципы, установленные Конституцией;
- 2) создавать угрозу национальному единству, суверенитету и территориальной целостности;
- 3) разглашать государственную тайну, создавать угрозу национальной безопасности или риск причинения ущерба чести и интересам государства;
- 4) разжигать этническую ненависть или создавать этническую дискриминацию, подрывать национальное единство или ущемлять национальные традиции и обычаи;
- 5) продвигать культы и суеверия;
- 6) распространять слухи, нарушать общественный порядок и подрывать социальную стабильность;
- 7) поощрять непристойности, порнографию, азартные игры, насилие или подстрекательство к преступлениям;
- 8) поощрять оскорбление или клевету на других или ущемление законных прав и интересов других лиц;
- 9) нарушать социальную мораль;
- 10) содержать контент, запрещенный законом, административными правилами и государственными правилами.

Помимо этого, если содержание публикации является ложным или несправедливым, что приводит к нарушению законных прав и интересов граждан, юридических лиц или других организаций, то лицо, опубликовавшее материал обязано публично исправить, устранить последствия и возместить вред в соответствии с законом.

Так, в законодательной базе большее внимание уделяется активной предварительной цензуре, которая формирует необходимое общественное мнение на этапе его зарождения. Сложно дать однозначную оценку тому, насколько это соотносится с такими фундаментальными правами, как свобода мысли и слова, однако, в рамках рассмотрения проблематики регулирования онлайн-игр, предварительная цензура выглядит оправданной. Данный подход призван нивелировать риски, отмеченные в Указе Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» где указано, что: «Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутривосточной и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств».

Подводя итог, важно отметить, что отечественная законодательная база, призванная регулировать сферу онлайн-игр, достаточно слаба, тем не менее, все же способна обеспечить определенный уровень защиты прав несовершеннолетних пользователей. В виду определенной геополитической ситуации, которая существенно ограничила возможность поступления новых онлайн-игр на российский рынок, видится разумным развивать и совершенствовать данную отрасль внутри России, снизить возможные риски к минимуму и создавать контент, который обеспечит формирование нравственно патриотических чувств.

Наиболее важным для регулирования данной отрасли является баланс между интересами государства, бизнеса и конечных пользователей. Законодательное закрепление тех или иных требований не должно быть чрезмерным и отягчающим существование индустрии онлайн-игры, но в то же время важно, чтобы определенные цели достигались посредством правоприменения.

Список литературы

1. Закон Китайской Народной Республики «О защите несовершеннолетних», пересмотрен и принят на 22-м заседании Постоянного комитета Всекитайского собрания народных представителей 13-го созыва 17.10.2020 Вступает в силу с 1 июня 2021 г. / 《中华人民共和国未成年人保护法》已由中华人民共和国第十三届全国人民代表大会常务委员会第二十二次会议于2020年10月17日修订通过，现予公布，自2021年6月1日起施行

2. Левченко, И. Е. Виды цензуры / И. Е. Левченко. – Текст: непосредственный // Уральский госуниверситет. – 2002.

3. Положение «О защите личной информации детей в Интернете» выпущены на исполнительном заседании Администрации киберпространства Китая 01.10.2019/ 《儿童个人信息网络保护规定》已经国家互联网信息办公室室务会议审议2019年10月1日起施行 URL: http://www.cac.gov.cn/2019-08/23/c_1124913903.html (дата обращения: 19.09.2022).

4. Положение об издательском управлении (Указ № 343 Государственного совета Китайской Народной Республики от 25.12.2001) / 出版管理条例 (2001年12月25日中华人民共和国国务院令 第343号公布 -URL: <https://www.pkulaw.com/chl/9bc2f1a9f76ec1d4bdfb.html> (дата обращения: 19.09.2022).

5. Репин, И. С. Использование сети Интернет в целях распространения экстремистской идеологии / И. С. Репин. – Текст: непосредственный // Вестник ЯрГУ. Серия Гуманитарные науки. – 2022. – № 2.

6. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

7. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

8. One in two young online gamers bullied, report finds. – Текст: электронный // BBC: [сайт]. URL: <https://www.bbc.com/news/technology-40092541>.amp (дата обращения: 19.09.2022).

9. K-12 Cyber Awareness Month 2020. – Текст: электронный // ECNO: [сайт]. URL: <https://ecno.org/cyber-security/k12cam2020-en/> (дата обращения: 19.09.2022).

10. 叶雅冰 流量时代网络直播内容管制制度评述 – 基于未成年人权益保护之探讨 / 叶雅冰. – Текст: электронный // PKULAW: [сайт]. URL: <https://www.pkulaw.com/qikan/28cb24d577ef524c5dd73ce500ebc0debdff.html?keyword=%E5%84%BF%E7%AB%A5%E7%BD%91%E7%BB%9C&way=listView> (дата обращения: 19.09.2022).

А. Е. Иртегова,

студент,

Институт прокуратуры,

Уральский государственный юридический университет

имени В. Ф. Яковлева

О ПРИДАНИИ ОФИЦИАЛЬНОГО СТАТУСА МАЙНИНГУ В РОССИИ

Аннотация. В статье обращается внимание на то, что майнинг не имеет в российском государстве официального статуса, описывается необходимость введения в законодательство России понятия «майнинг», анализируются законопроекты и принятый федеральный закон, посвященные цифровой валюте, приводится статистика оборотных мощностей криптовалют в России на 2022 г. На основании полученных данных делается вывод о скорейшем законодательном закреплении майнинга с целью устранения правовых пробелов в этой области и устранения в связи с этим нарушений прав граждан Российской Федерации.

Ключевые слова: блокчейн, криптовалюта, майнинг, биткоин, цифровые технологии, пробельность, Банк России

ON GIVING AN OFFICIAL STATUS TO MINING IN RUSSIA

Abstract. The article draws attention to the fact that mining does not have an official status in the Russian state, describes the need to introduce the concept of “Mining” into the legislation of the Russian Federation, analyzes draft laws and federal law on digital currency, provides statistics on the working capacity of cryptocurrencies in Russia for 2022. Based on the data obtained, a conclusion is made about the early legislative consolidation of mining in order to eliminate legal gaps in this area and eliminate violations of the rights of citizens of the Russian Federation in this regard.

Keywords: Blockchain, Cryptocurrency, Mining, Bitcoin, Digital technologies, Whitespace, Bank of Russia

2002 г., в котором разработана Федеральная целевая программа «Электронная Россия (2002–2010 гг.)», считается годом начала цифровизации в России. В 2018 г. Президент России издал Указ от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», ставя одной из целей осуществление прорывного научно-технологического и социально-экономического развития Российской Федерации. Постепенно в общество внедряются цифровые технологии, становясь неотъемлемой частью жизни многих людей. Прогресс не стоит на месте, и с помощью цифровых сетей можно не только искать информацию (как это задумывалось ранее), но и осуществлять свою трудовую функцию на легальной основе. Кроме того, в 21 веке также реально иметь электронные кошельки, осуществлять платежи при помощи ИТС Интернет и др. Неудивительно, что технологии настолько продвинулись вперед, что появилась не только электронная национальная валюта, но и криптовалюта, а также и люди, которые ее «добывают». Деятельность по «добыче» такой валюты принято называть «майнинг», а людей, которые ее осуществляют, – «майнеры».

Получается, что такое понятие как «майнинг» де-факто устойчиво существует, но де-юре на сегодняшний день в нашей правовой системе отсутствует. Также тема, связанная с майнинг, имеет особую актуальность и потому что значительная часть граждан России осуществляет деятельность, связанную с криптовалютой. В отношении майнинга в мире сложилось неоднозначное мнение. В некоторых странах, таких как, например, США майнинг – это легальная деятельность, охраняемая законом. А в КНДР она же запрещена под угрозой юридической ответственности. В России же на сегодняшний день остро стоит вопрос ввода в правовой оборот майнинга и связанных с ним явлений, поскольку иначе вся вышеупомянутая деятельность в нашей стране считается незаконной. Однако существуют различные мнения о том, стоит ли вводить майнинг в наш правовой оборот. К примеру, Банк России высказался на этот счет вполне однозначно – он отмечает необходимость полного запрета такой деятельности на территории нашей страны. Стоит при этом сказать, что даже для того, чтобы признать майнинг нелегальным, необходимо его определить, обозначить как термин, что и делает Банк России в одном из своих докладов за январь 2022 г. Орган указывает, что майнинг представляет собой процесс, при котором специальные компьютеры производят и выпускают криптовалюту. То есть майнинг представляет собой один из способов выпуска криптовалюты, а также контроля транзакций. Банк, определяя майнинг, предлагает ввести за него ответственность. При этом обращается внимание на последствия использования явления в России, которые выражаются в форме «потенциальных системных угроз», как например, угроза благосостоянию граждан или угроза окружающей среде (в связи с увеличением потребления электроэнергии для майнинга). Стоит отметить, что Банк России по понятным причинам придерживается отрицательной позиции насчет легализации майнинга в РФ, поскольку является основным государственным органом, отвечающим за финансовую безопасность и валютную стабильность нашей страны. Однако есть и обратные мнения на этот счет, например, как заметил финансовый директор пула EMCD, с созданием правовых возможностей для существования майнинга на территории РФ может решиться проблема с профицитом электроэнергии на территории нашего государства (24 млрд кВт в год), т. е. майнинг может стать одним из способов получения экспортной выручки, тем самым повысив статус РФ на мировом рынке.

В ответ на предложение Банка России представитель Минфина России высказал противоположное мнение, указывая на легализацию рассматриваемого понятия и присвоение ему кода определенной экономической деятельности в целях пополнения государственной казны (с помощью получения налога). Более того, по поручению Правительства РФ Министерство финансов подготовило и направило законопроект, суть которого заключалась в том, чтобы рассматривать такую валюту в качестве инструмента для инвестиций, по-прежнему запрещая ее использование как средство платежа на территории России. Законопроект дает определение майнинга, представляет процесс, посредством которого будет происходить взаимодействие участников деятельности, направленной на получение цифровой валюты, с налоговыми органами. В целом указанный акт показателен, ведь его содержание позволяет создать легальный рынок криптовалюты, сформулировать

правила ее оборота, а также установить права и обязанности участников данной деятельности (их круг).

Не стоит забывать, что все же были предприняты попытки закрепить майнинг на федеральном уровне. К примеру, обратим внимание, что цифровым технологиям посвящен ФЗ от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты РФ». Данным актом частично охватываются отношения по выпуску и генерации цифровых финансовых активов, однако, как уже отмечалось ранее, вне правового регулирования данного закона остаются еще многие виды деятельности, и в их числе находится майнинг. Нельзя не согласиться с мнением о том, что майнинг на сегодня является одной из важнейших отраслей, которая нуждается в законодательном закреплении. Анализируя нормы рассматриваемого нормативного акта, стоит заметить, что также нет положений, касающихся налогообложения цифровых финансовых активов (глава 25 НК РФ не предусматривает налогообложение криптовалюты). Подобное лишь доказывает важность введения майнинга в правовое поле, обратное же порождает все большие проблемы в законодательстве.

Обратим внимание на майский законопроект № 127303–8 «О майнинге в Российской Федерации». Авторы данного законопроекта основной своей задачей ставили возможность включения понятий «майнинг», «организация обращения (включая обмен) в РФ цифровой валюты», «майнинг-пул», а также «оператор майнинга» в действующее законодательство. К сожалению, уже в мае 2022 г. сами авторы отозвали его, однако внесением такой инициативы в законодательный орган в научных кругах была показана важность постепенно назревающей проблемы определения правового статуса майнинга, а также были сделаны первые шаги в направлении его идентификации. Согласно данным, представленным Центром альтернативных финансов Кембриджского университета, в январе 2022 г. Россия остается на третьем месте в мире по майнингу биткоина, однако доля майнеров с августа 2021 г. (11, 43 %) значительно снизилась и на сегодняшний день составляет 4,6 % (т. е. сокращение произошло как минимум в 2 раза за полугодие). Те же данные за 2021 г. приведены и в Пояснительной записке к майскому законопроекту 127303–8. В ней обращается внимание, что подобная неурегулированность влечет появление выпуска криптовалюты в «серой зоне», которая возникла в результате отсутствия легально закрепленного механизма осуществления операций с такой валютой. Итогом становится увеличение мошенничества в отношении граждан, притом последние не обладают достаточными инструментами для защиты своих нарушенных прав. Действительно, если бы майнинг был легализован на территории России, ситуация с уголовной ответственностью граждан-майнеров была бы более стабильна, нежели сегодня.

Также широко обсуждается факт наличия в законодательной плоскости технологии «блокчейн», но при этом отсутствует связанное с ним понятие «майнинг». Косвенное упоминание блокчейна (точнее, запрета на его использование на территории РФ) содержится в пункте 1 ст. 10 ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты РФ»

(далее – ФЗ «О ЦФА»). В ФЗ «О ЦФА» в императивном порядке определяется, что любые сделки, связанные с цифровыми финансовыми активами, совершаются через оператора обмена цифровых финансовых активов. Таким образом, такая технология, как блокчейн, запрещается, поскольку подчиняется иностранному праву, не совершается централизованно, как того требует закон (через оператора обмена цифровых финансовых активов), но сам факт, что наша страна упоминала и ранее в нормативных актах блокчейн, говорит о том, что Россия принимает его как технологию, однако возникает вопрос, почему до сих пор нет законодательного закрепления данного понятия.

Подводя итоги, необходимо отметить следующее. Отсутствие нормативного закрепления понятия «майнинг», «блокчейн» и прочих значительно затрудняет знание своих прав и обязанностей майнерами, а вследствие этого и применение ответственности за нарушение законодательства. Да и как можно нарушить то, что еще не урегулировано законом? Важность существования майнинга в законодательстве России определяет формирование грамотной принимающей деятельности в указанной сфере.

Список литературы

1. Кузменкин, И. В. Потенциал применения и реализации цифровых финансовых активов в связи с принятием закона № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты РФ / И. В. Кузменкин // Государство и право: Материалы 59-й Международной научной студенческой конференции, Новосибирск, 12–23 апреля 2021 года. – Новосибирск: Новосибирский национальный исследовательский государственный университет, 2021. – С. 51–52.

2. Мамитова Н. В., Селиверстова А. Д. Цифровое государство: проблемы построения в Российской Федерации // Государственная служба. 2019. № 2 (118). URL: <https://cyberleninka.ru/article/n/tsifrovoye-gosudarstvo-problemy-postroeniya-v-rossiyskoy-federatsii> (дата обращения: 10.08.2022).

3. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 10.08.2022).

4. Риски криптовалют и возможные меры регулирования: Доклад для общественных консультаций от 20.01.2022. URL: https://cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf (дата обращения: 13.09.2022).

5. Bitcoin Mining Map Cambridge Bitcoin Electricity Consumption Index The Cambridge Centre for Alternative Finance. – 2022. – January. URL: http://www.cbr.ru/Collection/Collection/File/32190/Review_of_transactions_2020.pdf (дата обращения: 12.09.2022).

Н. А. Калашников,

магистрант,

Тюменский государственный университет

О. Е. Козлова

магистрант,

Тюменский государственный университет

АНАЛИЗ И ВЫЯВЛЕНИЕ ЭКСТРЕМИСТСКИХ РИСКОВ В РАБОТЕ НЕЙРОСЕТЕЙ

Аннотация. Гипотетический искусственный интеллект может быть как безусловным благом для человечества, так и откровенным злом. В зависимости от использования будет определяться его предназначение и результаты работы. Самообучаемая нейронная сеть (нейросеть) хоть и является по сути своей математическим алгоритмом, но может рассматриваться как первоначальная ступень искусственного интеллекта, поскольку использует в работе процессы, основанные на человеческом мышлении. Цель исследования – ответить на вопрос, может ли искусственный интеллект или его автор нести ответственность за созданные им высказывания или выражения. Работа основана на результатах работы популярной нейросети, способной генерировать самостоятельные новостные заголовки. Также в исследовании подробно проанализированы составы преступлений, предусмотренных уголовным законодательством Российской Федерации и их относимость к экстремистским высказываниям нейросети.

Ключевые слова: нейронная сеть, информационные технологии, экстремизм, искусственный интеллект, преступление, разработчик, программирование

ANALYSIS AND IDENTIFICATION OF EXTREMIST RISKS IN THE WORK OF NEURAL NETWORKS

Abstract. Hypothetical artificial intelligence can be both an absolute boon for humanity and an outright evil. Depending on the path of use, its purpose and results of work will be determined. Although a self-learning neural network (neural network) is essentially a mathematical algorithm, it can be considered as the initial stage of artificial intelligence, since it uses processes based on human thinking in its work. The purpose of our research is to answer the question whether artificial intelligence or its author can be responsible for the statements or expressions created by it. The work is based on the results of a popular neural network capable of generating independent news headlines. The study also analyzes in detail the corpus delicti provided of the Criminal Code of the Russian Federation and its relevance to extremist statements of the neural network.

Keywords: Neural network, Information technology, Extremism, Artificial intelligence, Crime, developer, Programming

В современном мире стремительно развиваются почти все сферы общества, особенно касающиеся технологической составляющей жизни. Появляется все больше удобных и полезных технологий, некоторые из них даже называют «революционными». Раньше такими технологиями являлись конвейерное производство

и появление компьютеров. Сейчас это автоматизация больших данных, создание приложений-услуг, а также развитие искусственного интеллекта. Технология самообучающегося интеллекта, имитирующего человеческий, представляет собой настоящее технологическое чудо [1. С. 1–14]. Однако мы должны разобраться и в возможных рисках данного явления. В теории такая технология может быть очень полезной во многих отраслях человеческой деятельности, однако на практике все оказывается куда сложнее.

Наше исследование основывается на анализе и глубоком изучении одной из популярных самообучающихся нейронных сетей (разновидности искусственного интеллекта, который не разрабатывается в привычном понимании, а обучается и самостоятельно принимает некоторые решения на основе предыдущего опыта, который задал автор сети). Необходимо рассмотреть в каких ситуациях нейросети представляют опасность для человечества и способны на совершенно странные поступки с точки зрения человека [3]. Задачей исследования является оценка результатов деятельности конкретной нейросети на соответствие действующему законодательству в области противодействия экстремизму. В работе также изучается проблема субъектности преступлений, предусмотренных ст. 205.2, 280, 280.1 Уголовного кодекса Российской Федерации (УК РФ) [7].

Для наглядности, в целях исследования, будет взята конкретная нейросеть Neural Meduza [8], которая на основе анализа новостных заголовков пишет собственные «новости» в публичном пространстве сети Интернет. Результаты работы данной нейросети не претендуют на какую-то достоверность и должны восприниматься только как непонятный продукт компьютерного обучения, однако стоит и помнить, что такая нейросеть не может отличить добро от зла, смешное от грустного, поэтому некоторые заголовки, хотя и воспринимаются как шуточные, могут нести в себе явные экстремистские подтексты. Иногда полученные результаты работы даже по сути своей и являются чисто экстремистскими. Для примера рассмотрим несколько новостей: пост от 3 мая 2022 г.: «Патриарх Кирилл предложил лишить россиян права голоса на выборах», пост от 23 июня 2021 г.: «Путин потребовал срочно вернуть Крым Украине», пост от 1 ноября 2021 г.: «Довольно сильно умных людей нужно принудительно отстреливать», пост от 12 апреля 2022 г.: «Дамы и господа! В кризис нужно срочно менять Конституцию!», пост от 5 августа 2021 г.: «Московские депутаты предложили переработать бедных россиян».

Даже без особых познаний в науке уголовного права, можно понять, что эти новости как минимум звучат странно, а как максимум – содержат в себе экстремистские высказывания. Для того чтобы подтвердить наши суждения, обратимся к законодательству в этой сфере жизни общества. Так, в соответствии с п. 1 ст. 1 ФЗ «О противодействии экстремистской деятельности» понятие экстремистской деятельности включает в себя множество категорий. В их числе возбуждение социальной, расовой, национальной или религиозной розни, призывы к нарушению территориальной целостности РФ, а также пропаганда неполноценности человека и нарушение его прав и свобод по этим признакам, и многие другие категории [4]. Как мы видим, некоторые из упомянутых «новостей», созданных нейросетью,

очевидно содержат экстремистские высказывания или призывы к ним. Так как подобные новости выкладываются в абсолютно свободный доступ любых лиц, всегда доступны для просмотра и комментирования, можно говорить, что такие высказывания являются публичными. Уже сам факт публичности должен постепенно приближать читающего к процессу осознания потенциальной опасности таких высказываний.

Для полноты исследования необходимо внимательно рассмотреть условия наступления уголовной ответственности за них. Ч. 2 ст. 280 УК РФ предусматривает уголовную ответственность за публичные призывы к осуществлению экстремистской деятельности, в том числе в сети Интернет, что и ставит под вопрос наличие признаков состава преступления в действиях публичной нейросети, провозгласившей экстремистские лозунги.

Итак, во-первых, с точки зрения объективной стороны, публичные призывы выражаются, в том числе с использованием технических средств в форме обращения к другим лицам. Признак публичности устанавливается из конкретных обстоятельств совершенного деяния, однако Пленум ВС РФ приводит некоторые примеры, характеризующие публичность деяния, предусмотренного ст. 280 УК РФ. А именно – обращение к группе людей в общественных местах, распространение обращений путем массовой рассылки сообщений и т. п. [5]. Такая публичная нейросеть, которую мы рассматриваем, как раз таки занимается рассылками информации, и ее деятельность направлена на неограниченный круг лиц, что, по нашему мнению, относится к признаку публичности.

Следует отметить, что состав преступления, предусмотренного ст. 280 УК РФ, формальный, а это означает, что преступление окончено с момента публичного провозглашения обращения (отправки сообщения) независимо от того, удалось побудить граждан к осуществлению экстремистской деятельности или нет.

Во-вторых, для нас главным вопросом основания уголовной ответственности за публичные призывы к осуществлению экстремистской деятельности является наличие субъекта преступления. В данном преступлении, в соответствии с Общей частью УК РФ, субъектом является физическое вменяемое лицо, достигшее 16-летнего возраста. Однако нейросеть является искусственным интеллектом, который на данный момент не обладает правовым статусом в РФ. Следовательно, нами ставится вопрос о посредственном исполнителе осуществления публичных призывов к осуществлению экстремистской деятельности в лице разработчика соответствующей нейросети.

Как правило, при создании подобных нейросетей, разработчики не задумываются о том, что работа нейросети может повлиять на жизнь и здоровье людей, правоотношения, правовые последствия осуществления поставленных перед ней задач. Это происходит как минимум потому, что отсутствует качественная правовая регламентация деятельности по созданию искусственного интеллекта. Тем самым, закладывая определенный механизм работы нейросети и «обучая» ее, разработчик допускает совершение нейросетью действий, противоречащих законодательству об экстремистской деятельности. К тому же, исходя из правил и возможностей использования самой социальной сети Telegram, возможность от-

правки сообщения в публичный канал остается в любом случае за человеком, ведь даже в случае установленного таймера на выкладывание поста, сам пост предварительно проходит через человека.

Тут уже возникает вопрос о виновности. С точки зрения субъективной стороны, разработчик нейросети при ее создании не обязательно должен считать, что его нейросеть точно создаст экстремистский контент, однако уже при публикации созданной «новости», он должен был понимать и осознавать, что публикует призыв к экстремизму или собственно экстремистское высказывание, а потому и должен осознавать общественную опасность своих действий, предвидеть возможность наступления общественно опасных последствий в виде пропаганды экстремизма, но при этом он может безразлично относиться к возможным последствиям. Все эти признаки характеризуют совершение преступления, предусмотренного ст. 280 УК РФ, с косвенным умыслом разработчика нейросети.

По смыслу ст. 280 УК РФ преступление может быть совершено только путем активных действий с прямым умыслом, равно как и преступление, предусмотренное статьей 205.2 УК РФ, поскольку публичные призывы предполагают желание достижения определенных последствий, например, в виде возбуждения вражды или ненависти по национальному признаку, если разработчик действительно самостоятельно и осознано публиковал спорные результаты работы нейросети, то может идти речь о наличии признаков рассматриваемых составов преступлений.

Действия, противоречащие законодательству, совершаемые с прямым умыслом, характерны так называемым «хакерам», которые используют нейронную сеть для кражи ценных данных, заражения компьютеров вредоносными программами и др. Однако группа израильских исследователей считает, что создание нейросети для вышеуказанных действий – очень долгое и дорогое занятие, поэтому совершение умышленных преступлений с использованием искусственного интеллекта распространяется не очень быстро. При этом не стоит расслабляться, поскольку развитие технологий может значительно упростить процедуру создания нейронных сетей и открыть страшную угрозу нарушения прав человека, в том числе при совершении экстремистских преступлений [2].

Если посмотреть на ситуацию развития современного общества с другой более позитивной стороны, то следует отметить, что в декабре 2022 г. в Российской Федерации главный радиочастотный центр, подведомственный Роскомнадзору, планирует запустить систему автоматического поиска противоправного контента на фото и видео в Интернете под названием «Окулус». Нейросеть будет выявлять в том числе и экстремистские материалы [6]. Тут сразу возникает вопрос о возможности нейросети, выявляющей противоречащие закону публикации в сети Интернет, обнаружить такие публикации, созданные другой нейросетью.

Получается достаточно интересная ситуация, при которой получается так, что экстремистские высказывания есть, а субъекта преступления нет. Ведь даже в случае предварительного одобрения человеком-разработчиком нейросети экстремистского материала он, скорее всего, не задумывается о потенциальной опас-

ности данного материала, не предвидит каких-либо последствий от публикаций результатов обучения и работы нейросети. Поэтому и рассматривать такого человека в качестве субъекта преступлений, проанализированных нами ранее, мы не можем. Считаем правильным относиться к подобным материалам, кажущимся экстремистскими, как к шуточной версии новостей из реального мира, но тем не менее, с должной осмотрительностью и внимательностью, чтобы данные новости не стали причиной негативных последствий, как от настоящих экстремистских материалов.

Таким образом, в настоящее время невозможно и в целом не нужно привлекать, собственно, нейросеть за публичные призывы к экстремистской деятельности в виду отсутствия в таких действиях признаков состава преступления. Однако нужно помнить, что публикация подобных материалов человеком, имеющим прямой умысел на негативные последствия, перечисленные в рассмотренных составах преступлений, может рассматриваться в качестве экстремистских высказываний.

Список литературы

1. Иванова Л. В., Калашников Н. А. Пределы ответственности автопилота. Журнал правовых вопросов Ассоциации общества и права Великобритании (UK LSA). 2022. № 9 (1).

2. Коняев А. Преступная нейросеть. Могут ли хакеры обратить во зло искусственный интеллект. URL: <https://nplus1.ru/material/2019/09/09/are-criminal-networks-real> (дата обращения: 16.09.2022).

3. Николаева Д. А. «Мы в ответе за тех, кого обучили. Юридическая ответственность разработчиков нейросетей». URL: <https://vc.ru/legal/69572-my-v-otvete-za-teh-kogo-obuchili-yuridicheskaya-otvetstvennost-razrabotchikov-neyrosetey> (дата обращения: 21.05.2022).

4. О противодействии экстремистской деятельности: Федеральный закон от 25.07.2002 № 114-ФЗ // Российская газета. № 138–139, 30.07.2002.

5. О судебной практике по уголовным делам о преступлениях экстремистской направленности: Постановление Пленума Верховного Суда РФ от 28.06.2011 № 11 // Российская газета. № 142, 04.07.2011.

6. Стали известны подробности о системе по контролю за россиянами в интернете. URL: <https://lenta.ru/news/2022/08/17/oculus/> (дата обращения: 16.09.2022)

7. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. № 25. ст. 2954. 17.06.1996 г.

8. Neural Meduza: Социальная сеть Telegram. URL: t.me/neuralmeduza/7611 (дата обращения: 20.05.2022).

Е. В. Калинин,

студент,

Северо-Западный институт (филиал)

Московского государственного юридического университета
имени О. Е. Кутафина

ЦИФРОВЫЕ ТЕХНОЛОГИИ В НОТАРИАЛЬНОЙ ЗАЩИТЕ ПРАВ ПРЕДПРИНИМАТЕЛЕЙ

Аннотация. Целью данной статьи является исследование современных цифровых технологий в системе нотариальных действий при защите прав предпринимателей. Для достижения данной цели раскрыта специфика нотариальных действий, дана характеристика особенностей удостоверения сделок в электронном виде. Особое внимание уделено цифровым технологиям в системе обеспечиваемых нотариусом доказывания бесспорных юридических фактов, дана правовая характеристика нотариального осмотра электронных доказательств в сфере защиты прав предпринимателей.

Ключевые слова: право, цифровые технологии, нотариат, права предпринимателей, бесспорные юридические факты, осмотр электронных доказательств

DIGITAL TECHNOLOGIES IN THE NOTARIAL PROTECTION OF THE RIGHTS OF ENTREPRENEURS

Abstract. The purpose of the given article is research of modern digital technologies in system of notarial actions at protection of the rights of businessmen. For achievement of the given purpose the specificity of notarial actions is opened, the characteristic of features of certification of transactions in electronic form is given. Special attention has been paid to the digital technologies in the system of proving of indisputable legal facts which are provided by the notary, the legal characteristic of notarial examination of electronic proofs in the sphere of entrepreneurs' rights protection has been given.

Keywords: Law, Digital Technologies, Notary, Entrepreneurs rights, Indisputable legal facts, Examination of electronic evidence

Нотариат в Российской Федерации сегодня призван осуществлять защиту имущественных прав и законных интересов физических и юридических лиц – в первую очередь субъектов предпринимательства, предупреждать правонарушения путем совершения нотариальных действий, в том числе по обеспечению доказательств прав предпринимателей [7. С. 133].

Нотариус выполняет задачу, в целом схожую с задачей суда: защита прав граждан и организаций. Однако нотариус, решая вопросы, относящиеся к его компетенции, не исследует и не выясняет спорные вопросы, а делает выводы только на основании имеющих фактов, непосредственно представленными ему.

Нотариальной деятельности присущи следующие принципы: законности; совершение особых нотариальных действий специальными субъектами; независимость и беспристрастность; равенство перед законом; в соответствии с установленной процедурой в сфере бесспорной юрисдикции. Право, которое необ-

ходимо защитить, должно быть бесспорным. Право должно быть документально подтверждено и не должно оспариваться третьими лицами.

Ни в одном законодательном акте не закреплено понятие нотариальных действий. ГПК РФ, Основы законодательства о нотариате не имеют легальной дефиниции нотариальных действий. Это понятие установлено только в Модельном законе о нотариате (принят в г. Санкт-Петербурге 27.03.2017 Постановлением 46–9 на 46-м пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ) [6. С. 120].

Различают такой вид нотариальных действий, как удостоверение сделок, договоров, завещаний, доверенностей. Данный вид нотариальных действий регламентирован главой X Основ законодательства Российской Федерации о нотариате (ст. 53–60) [3]. Многие сделки не требуют обязательного нотариального удостоверения, но это можно сделать добровольно. Нотариусом удостоверяются сделки, для которых законом Российской Федерации установлена обязательная нотариальная форма (к таким относятся договоры, завещания, доверенности).

Внедрение в практику гражданского товарооборота и развитие института нотариального удостоверения сделок в электронном виде является возможным при условии комплексной легализации этого нотариального действия в условиях законодательства о нотариате, гражданского и гражданско-правового законодательства. Одной из проблем, которая вытекает из нотариального удостоверения сделки в электронном виде, является то, что невозможно привлечь к ответственности при недобросовестном или неполном исполнении обязательства контрагентов. Это происходит потому, что в момент обращения в суд с исковым заявлением необходимо доказать указанные в исковом заявлении обстоятельства и факт, и, так как сделка заключена в электронном виде, то у истца возникают проблемы с доказыванием обстоятельств, на которые он сослался. На современном этапе в гражданском процессе могут быть использованы электронные документы в качестве доказательств.

К нотариальным действиям также относится удостоверение бесспорных фактов, которое регламентировано статьями 82–85, Основ законодательства Российской Федерации о нотариате. Такое нотариальное действие необходимо в удостоверении времени. Нотариус не обеспечивает доказательства по делу, которое при обращении уже находится в судопроизводстве. Данные действия совершаются до возбуждения дела в суде или другом юрисдикционном органе. Нотариус дает разъяснения свидетелю и эксперту о даче заведомо ложных показаний и ответственности за это (статья 307 УК РФ).

В практике можно встретить случаи, когда стороны недобросовестно используют институт нотариата, совершая неправомерные сделки. Так было рассмотрено дело по исковому заявлению прокурора к ООО «Веритас», Анчугову А. В. о признании договора займа недействительным и применении последствий недействительности сделки. С учетом доказательств в совокупности, анализа действий ООО «Веритас» по попыткам обналичить денежные средства в размере более 25 000 000 рублей, поступившие на только открытый банковский счет в один день от 15 различных юридических лиц, суд справедливо решил, что действительная цель сделки – договора займа – иная, чем заявлено ООО «Веритас»

и Анчуговым А. В. Эта цель – обналичивание денежных средств в обход банковских механизмов и обязанности владельца счета подтвердить законность операций и обладания денежными средствами – с нарушением действующего законодательства. При этом стороны, заключая такой договор, осуществили попытки использовать институт нотариата и ФССП России для обналичивания денежных средств, находящихся на расчетном счете ООО «Веритас». В случае достижения цели денежные средства, поступившие на расчетный счет ООО «Веритас», могли быть обналичены в обход закона. При таких обстоятельствах сделка была верно признана ничтожной как заведомо противная основам правопорядка. Суд установил, что, заключая такую сделку, и ООО «Веритас», и Анчугов А. В. действовали умышленно, заведомо определяя цель сделки, противоречащую основам правопорядка. Таким образом, суд применил последствия признания сделки недействительной, предусмотренные статьей 169 Гражданского кодекса Российской Федерации, а именно – взыскание 25 600 000 рублей в доход Российской Федерации. Применение иных последствий, в том числе двусторонней реституции, позволило бы сторонам достичь противных основам правопорядка целей сделки – легализация и обналичивание денежных средств [5].

Цифровые технологии позволяют реформировать правовое регулирование нотариальной деятельности – актуализируются новые нотариальные действия, в том числе обеспечение доказательств, размещенных в сети Интернет.

Следует отметить следующую специфику нотариальной деятельности по обеспечению доказательств: применение как общих правил гражданского процессуального законодательства, так и специальных правил Основ законодательства о нотариате; отсутствие срока действия доказательств, обеспеченных нотариусом; оформление нотариальных средств доказывания на основе процессуальных требований по месту требования обеспечиваемых доказательств; совершение данных нотариальных действий каждым нотариусом соответствующего нотариального округа.

Реализуя предусмотренные правом возможности цифровых технологий в первую очередь субъекты предпринимательства создают объекты интеллектуальной собственности, заключают смарт-контракты, осуществляют электронный обмен информацией и т. д. [4. С. 56–58].

При посягательстве на их права и законные интересы субъекты предпринимательской деятельности прибегают к защите судов и компетентных органов.

Важные для предпринимателей сведения содержатся в разнообразных цифровых технических устройствах: стационарных вычислительных машинах, персональных компьютерах, ноутбуках, гаджетах, электронных носителях информации и т. п.

К сожалению, в цифровой среде совершаются правонарушения, нарушающие личные права, связанные с информацией порочащей честь, достоинство и деловую репутацию предпринимателей. Кроме того распространено нарушение авторского права.

Сосредоточим внимание на характеристике нотариального осмотра электронных доказательств. Во-первых, с учетом ст. 64 АПК РФ изучение информации нотариусу необходимо проводить, только используя лицензионную программу на сертифицированном должным образом техническом устройстве. При обращении

к интернет-странице проводится ее осмотр на экране девайса и копирование в том виде, в котором она открывается.

При наличии на интернет-странице звукозаписей или видеофайлов допустим их осмотр в силу того, что в российском законодательстве нет прямого запрета на такие действия.

Переписка в электронной почте или в видеоконференции может быть осмотрена нотариусом по заявлению лица, обладающего правом пользования данными ресурсами, соблюдая при этом, охраняемую федеральным законодательством тайну переписки. Электронная почта может быть осмотрена нотариусом и с помощью находящейся в свободном обороте компьютерной программы Team Viewer (teamviewer.com), позволяющей проводить удаленный доступ.

Доступ в закрытые группы социальных сетей и соответствующий осмотр совершается с аккаунта имеющего доступ к необходимому сообществу заявителя, по причине того, что нотариус не имеет права совершать нотариальные действия от своего имени и на свое имя (ст. 47 Основ законодательства РФ о нотариате).

Возможен также осмотр и запись имеющихся в сотовом телефоне письменных SMS- и MMS-сообщений или информации, полученной с помощью специальных программ-мессенджеров. Телефон и SMS-карты должны принадлежать заявителю на законных основаниях. Фиксация сообщений осуществляется с указанием даты и времени в порядке возрастания [1. С. 90–93].

Благодаря цифровизации сформировалась целая совокупность предпринимателей, применяющих бизнес-подходы, возникшие на границе высоких технологий и бизнеса, или использующих интернет-формат [2. С. 167].

Юридическая практика вскрыла пробелы в эффективном правовом регулировании обеспечиваемых нотариально электронных средств доказывания:

1. Список нотариальных действий, содержащийся в законодательстве, не точен в части сбора электронных доказательств. Следовательно, требуется расширение перечня нотариальных действий в данном направлении, например, следует включить туда осмотр видеофайла.

2. Прогресс цифровых технологий предопределяет необходимость быстрой своевременной фиксации юридически значимых фактов в связи с угрозой их утраты, что вызывает потребность законодательного закрепления специального упрощенного порядка сбора электронных доказательств.

3. Принципиально важно закрепить возможность начала сбора электронных доказательств после направления электронного заявления нотариусу.

Список литературы

1. Бегичев А. В. Современные технологии в системе обеспечиваемых нотариусами средств доказывания // Российская правовая систем в условиях четвертой промышленной революции. XVI Международная научно-практическая конференция (Кутафинские чтения): материалы конференции: в 4 ч. Часть 4. Москва: РГ-Пресс, 2019. С. 90–93.

2. Колодня Г. В., Королева И. В. Орусова О. В. Рынок и государство: проблемы взаимодействия в современной России: монография. – Москва: Проспект, 2022. – 184 с.

3. Основы законодательства Российской Федерации о нотариате (утв. ВС РФ 11.02.1993 № 4462-1) // Ведомости съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1993. № 10. Ст. 357.

4. Полежаев О. А. Право новых технологий, практика комплексной юридической проверки (due diligence) при подготовке сделок в сфере новых технологий, новые технологии автоматизации юридической работы (Legal Tech): учебное пособие. – Москва: Проспект, 2021. 80 с.

5. Решение Кировского районного суда г. Екатеринбурга от 26.05.2020 по делу № 2-1487/2020 // URL: <https://sudact.ru/regular/doc/yKfv4wNjMoH5/> (дата обращения: 18.09.2022).

6. Фролович Э. М. Нотариальные действия как основание возникновения процессуальных отношений // Пробелы в российском законодательстве. Юридический журнал. – 2017. – № 1. С. 120–123.

7. Эффективность правового регулирования: монография / под общ. ред. А. В. Полякова, В. В. Денисенко, М. А. Беляева. Москва: Проспект, 2022. 240 с.

М. А. Калмыкова,
магистрант,

Волгоградский институт управления – филиал Российской академии
народного хозяйства и государственной службы
при Президенте Российской Федерации»

ОТСУТСТВИЕ ЕДИНЫХ СТАНДАРТОВ РАБОТЫ МАРКЕТПЛЕЙСОВ КАК ПРАВОВАЯ ПРОБЛЕМА

Аннотация. В современном мире дистанционная торговля набирает все большую популярность. Этот способ реализации товаров имеет ряд преимуществ, но также у него есть и недостатки. Одним из ключевых правовых пробелов в регулировании дистанционной купли-продажи товаров является отсутствие единых стандартов осуществления торговой деятельности маркетплейсами. В силу этого каждый из них имеет возможность самостоятельно устанавливать требования, которые могут ущемлять потребителя. Выходом из сложившейся ситуации служит внесение соответствующих изменений в нормативно-правовые акты, регулирующие защиту прав потребителей и осуществление дистанционной купли-продажи товаров.

Ключевые слова: дистанционная торговля, потребитель, стандарты, требования, маркетплейсы, интернет-торговля, защита прав

THE LACK OF UNIFORM STANDARDS FOR THE OPERATION OF MARKETPLACES AS A LEGAL PROBLEM

Annotation. In the modern world, distance trading is gaining more and more popularity every day. This method of selling goods has a number of advantages, but it also has disadvantages. One of the key legal gaps in the regulation of the remote purchase and sale of goods is the lack of uniform standards for the implementation

of trade activities by marketplaces. Because of this, each of them currently has the opportunity to independently establish requirements that may infringe on the consumer. The way out of this situation is the introduction of appropriate amendments to regulatory legal acts regulating the protection of consumer rights and the implementation of remote purchase and sale of goods.

Keywords: Distance trading, Consumer, Standards, Requirements, Marketplaces, Online commerce, Protection of rights

В настоящее время дистанционный способ продажи товаров находится на пике своего развития. С каждым днем увеличивается количество покупателей, которые предпочитают приобретать необходимую продукцию и вещи в удаленном формате, чаще всего, посредством сети Интернет. Для этой цели они используют различные маркетплейсы: «Валдберис», «Озон», «Яндекс.Маркет», «Сбер.Маркет», также сайты различных магазинов одежды и обуви, электроники, заказа продуктов и т. д. Для продавцов дистанционная торговля стала новым каналом сбыта продукции. Они могут как создать свой сайт для продвижения своих товаров, так и начать сотрудничество с разными площадками интернет-торговли.

Удобство приобретения и сбыта продукции служат несомненным плюсом дистанционного способа продажи товаров, но у него также есть и минусы, которые еще только предстоит исправить. Одной из проблем реализации товаров дистанционно является отсутствие единых требований к работе маркетплейсов, нет единых стандартов.

Ни в ч. 2 Гражданского кодекса Российской Федерации, ни в Законе Российской Федерации от 07.02.1992 № 2300–1 «О защите прав потребителей», ни в постановлении Правительства от 31.12.2020 № 2463 «Об утверждении Правил продажи товаров по договору розничной купли-продажи...» не содержится норм, прописывающих правила работы торговых интернет-площадок. Из-за этого каждая из них может сама устанавливать минимальную сумму заказа для бесплатной доставки, сумму за возврат товара в случае отказа от него, самостоятельно регулировать ценовую политику доставки товаров по определенному адресу курьером [1, 2, 3].

Одним из наиболее известных примеров установления фиксированной суммы за возврат товара в случае отказа от него служит случай «Валдберис». Сначала маркетплейс установил сумму возврата в 100 руб., затем снизил до 50, а потом вновь поднял, но уже до 75 руб. за возврат каждой единицы товара, а за возврат крупногабаритного товара покупателю придется уже заплатить 1 000 руб. [4].

Таким образом, отсутствие единых стандартов работы маркетплейсов относительно установления единых тарифных планов доставки товаров, их возврата существенно влияет на потребителей. Они могут в таких случаях либо выбрать интернет-площадку, где будет меньшая сумма за возврат товара или где не будет ее вообще, даже при условии, что на этой площадке товар будет дороже того, который продается на площадке с платным возвратом. Либо потребитель вообще предпочтет купить товар в обычном магазине. Это, несомненно, дает выбор покупателю, где ему приобретать товары, но установление единой суммы возврата товара без учета его стоимости не послужит эффективным инструментом развития маркетплейса, а, скорее наоборот, будет уменьшать спрос на приобретение товаров посредством

него. Именно поэтому необходимо внести изменения в нормативные документы, которые бы создали единые требования к работе торговых интернет-площадок.

Список литературы

1. Гражданский кодекс Российской Федерации // СПС «Гарант».
2. О защите прав потребителей: Закон Российской Федерации от 07.02.1992 № 2300-1 // СПС «Гарант».
3. Об утверждении Правил продажи товаров по договору розничной купли-продажи, перечня товаров длительного пользования, на которые не распространяется требование потребителя о безвозмездном предоставлении ему товара, обладающего этими же основными потребительскими свойствами, на период ремонта или замены такого товара, и перечня непродовольственных товаров надлежащего качества, не подлежащих обмену, а также о внесении изменений в некоторые акты Правительства Российской Федерации: постановление Правительства РФ от 31.12.2020 № 2463 // СПС «Гарант».
4. TexTerra – агентство интернет-маркетинга. URL: <https://texterra.ru/blog/platnyu-otkaz-vozvrat-v-vayldberriz-problema-i-reshenie.html> (дата обращения: 19.09.2022).

М. А. Кантаев,
магистрант,

Российская государственная академия интеллектуальной собственности

ДЕПОНИРОВАНИЕ ОБЪЕКТОВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ С ПРИМИНЕНИЕМ ТЕХНОЛОГИИ-БЛОКЧЕЙН

Аннотация. В статье рассматривается сфера интеллектуальной собственности и вопросы обеспечения защиты авторских прав, анализируются подходы к депонированию авторских прав, акцентируется внимание на существующих проблемах и предлагается решение для предоставления дополнительной правовой охраны объектам интеллектуальной собственности и обеспечения доказательств авторских прав.

Ключевые слова: депонирование, цифровое депонирование, интеллектуальная собственность, авторские права, блокчейн, IT-решения

DEPOSITING OF OBJECTS OF INTELLECTUAL PROPERTY USING BLOCKCHAIN TECHNOLOGY

Abstract. Considering the field of intellectual property and issues of ensuring copyright protection, the author analyzes approaches to copyright registration, focuses on existing problems and proposes a solution for providing additional legal protection to intellectual property and providing evidence of copyright.

Keywords: Depositing, Digital depositing, Intellectual property, Copyright, Blockchain, IT-solutions

Одним из принципов Бернской конвенцией по охране литературных и художественных произведений от 9 сентября 1886 г. (далее – «Конвенция») [1], объединяющей 193 государства-члена, является принцип автоматической охраны, исключающий соблюдение каких-либо формальностей для возникновения, осуществления и защиты авторских прав.

Российская Федерация, являющаяся страной-участницей Конвенции, помимо всего прочего, также является государством-участником Соглашения стран СНГ от 24.09.1993 «О сотрудничестве в области охраны авторского права и смежных прав» [2], согласно ст. 3 которого участники соглашения обязываются предпринимать меры, направленные на обеспечение охраны авторского права и смежных прав на уровне требований Конвенции.

Вместе с тем, возвращаясь к принципу автоматической охраны, нельзя не отметить его неоднозначность. С одной стороны, принцип автоматической охраны способствует активному обороту объектов авторского права, поскольку отсутствует необходимость в прохождении длительной процедуры регистрации – авторские права возникают в силу создания произведения. С другой стороны, подобный заявительный порядок признания авторских прав создает почву для злоупотреблений и, как следствие, споры и разногласия между авторами.

В качестве подтверждения актуальности вопроса защиты авторских прав рассмотрим анализ судебной практики за 2020 г. по спорам, связанным с защитой авторских прав на фотографические произведения, размещенных в сети Интернет [8]. Данный анализ был проведен экспертами департамента по правовым вопросам компании RTM Group на основании опубликованных решений судов Российской Федерации.

Так, в 2019 г. в Российской Федерации было вынесено 203 акта по спорам о защите авторских прав на фото-произведения. Вместе с тем в 2020 г. этот показатель вырос на 40 % и составил 334 акта, среди которых 89,2 % требований истцов были удовлетворены полностью или частично. Более того, общая сумма требований по данным искам достигла отметки в 93 854 950 руб.

Важно иметь в виду, что вышеприведенные данные охватывают только споры, связанные с защитой авторских прав на фото-произведения. Тем не менее статистические данные за 2019 г. и 2020 г. наглядным образом демонстрируют, что количественный показатель споров имеет тенденцию к росту как по количеству исков, так и по сумме исковых требований. Логичным представляется предположить, что количественные показатели будут намного существеннее и масштабнее при более широком охвате споров по защите авторских прав, которые связаны не только с фото-произведениями, но и рядом других объектов авторского права: литературные, драматические, музыкальные, аудиовизуальные, географические произведения.

Кроме того, справедливым представляется утверждение о том, что проблема роста споров обусловлена, в том числе стремительной цифровизацией общественных отношений, поскольку одна часть произведений имеют свои цифровые аналоги, а другая часть произведений в принципе невозможна вне цифрового пространства (авторский онлайн-курс, блог, статья, страница в социальных сетях и пр.).

Таким образом, отсутствие обязательной регистрации объектов авторского права, несмотря на позитивный аспект данного положения с точки зрения теории, на практике порождает ряд проблем в части предоставления охраны и защиты авторских прав, среди которых представляется возможным выделить следующие проблемы:

- 1) определения автора;
- 2) определения исходного содержания произведения;
- 3) определения даты создания произведения.

Отметим, что вышеперечисленные положения в совокупности определяют основную проблему отрасли, а именно – обеспечение защиты авторских прав, связанное с доказыванием и подтверждением авторских прав. Ведь главное, с чем сталкивается автор в случае возникновения спора, заключается именно в доказывании своих авторских прав.

При этом следует разграничивать понятия «охрана» и «защита» авторских прав. Несмотря на наличие позиции, отождествляющей данные понятия, в юридической науке доминирует положение о том, что «охрана» и «защита» авторских прав обладают самостоятельным содержанием. Так, охрана авторских прав характеризуется пассивной функцией и имеет своей целью «недопущение посягательств на субъективное право, предохранение его от нарушений» [7. С. 165]. Вместе с тем защита авторских прав характеризуется активной функцией, возникает в момент нарушения права и представляет собой совокупность действий, направленных на восстановление нарушенных прав автора.

Говоря о доказывании авторских прав, действующее российское законодательство не содержит исчерпывающего перечня доказательств авторства, что подчеркивается в Постановлении Пленума Верховного суда РФ № 10. Кроме того, в продолжение рассмотрения примера с подтверждением авторства на фотографическое произведение в Постановлении Пленума Верховного суда РФ № 10 также отмечается, что «об авторстве конкретного лица на фотографию может свидетельствовать в числе прочего представление этим лицом необработанной фотографии» [5].

Судебная практика применения подтверждает актуальность положений Пленума Верховного суда РФ. Например, в деле № 2–1636/2020, рассмотренным Октябрьским районным судом г. Барнаула Алтайского края, исключительные права на фотографию были подтверждены с помощью CD-диска с оригиналом фотографии, «где через вкладки Свойства => подробно можно видеть, что фотография создана 31 января 2019 г., 12:45, фотоаппаратом Sony NEX-5N» [15]. В другом деле 2–654/20, рассмотренным Куйбышевским районным судом г. Санкт-Петербурга, авторство было подтверждено «наличием компьютерного цифрового файла с исходным произведением» [14].

Решение Ленинского районного суда г. Краснодара по делу № 2–3845/2020 [13] подтверждает, насколько важно определить идентичность произведений, если спор связан с литературными произведениями. Так, полное удовлетворение исковых требований судом было связано, в том числе с тем, что совокупностью доказательств была установлена идентичность спорного произведения, содержащегося в печатном издании и незаконно опубликованного на сайте ответчика.

Так, несмотря на то, что в спорных ситуациях для защиты авторских прав используются необработанные материалы произведений, черновики, первоначальные файлы и прочее, представляется необходимым формирование таких способов доказывания, чья достоверность не будет вызывать сомнений и будет упрощать порядок разрешения спора относительно авторских прав.

Одним из инструментов, позволяющих зафиксировать свои авторские права, является депонирование (от лат. *dēponō* – «кладу, оставляю»), под которым понимается своеобразная процедура регистрации экземпляра произведения.

Заслуживающим внимания является решение по охране и защите авторских прав, реализованное на государственном уровне в США, где функционирует Бюро авторского права США, в котором авторы могут зарегистрировать свои произведения. Процедура регистрации имеет сходство с депонированием и подразумевает под собой несколько простых действий: подача заявления, предоставление экземпляра работы, оплата государственной пошлины [11]. По итогу процедуры автору выдается свидетельство о регистрации авторских прав. Подобное свидетельство позволяет автору быть уверенным в надежности правовой охраны своих произведений, а при необходимости защитить свои авторские права, имея доказательство в виде свидетельства.

Кроме того, отличается от ряда стран законодательство об авторском праве Республике Казахстан, в гражданском кодексе которой предусмотрена статья, регламентирующая депонирование. Так, в ст. 979 Гражданского кодекса Республики Казахстан, посвященной депонированию произведений, предусмотрено, что «депонирование рукописей произведений, других произведений на материальном носителе, в том числе на машинном, признается использованием произведения, если такое депонирование произведено в открытом для доступа каждом хранилище (депозитариум) и допускает получение по договору с депозитарием экземпляра произведения любым лицом» [6]. В законодательстве иных государств, в частности стран-участниц Евразийского экономического союза, подобных положений не предусмотрено, что позволяет сделать вывод о целесообразности рассмотрения вопроса и включения подобной нормы в национальное законодательство.

Говоря о гражданском законодательстве Российской Федерации, посвященном авторскому праву, необходимо отметить, что в России государственная регистрация авторских прав предусмотрена только для такого объекта авторского права, как программа для ЭВМ, причем, как указано в п. 1 ст. 1262 ГК РФ, по желанию правообладателя [4]. Благодаря данной статье авторы программ для ЭВМ имеют возможность подтвердить свои авторские права в заявительном порядке и получить от Роспатента документ, подтверждающий их права на произведение – программу для ЭВМ. Таким образом, фактически заявительный характер подтверждения авторских прав в отношении программ для ЭВМ напоминает собой процедуру депонирования.

Для иных объектов авторского права подобной возможности не предусмотрено, в связи с чем депонированием объектов авторского права, прежде всего, занимаются частные компании.

Ранее депонирование осуществлялось с помощью нотариуса, либо посредством направления письма с вложенным произведением самому себе. Однако подобные способы представляются в настоящее время архаичными, неоправданно дорогими и длительными по времени. Логично предположить, что в век высоких технологий наиболее целесообразным является осуществление цифрового депонирования путем внедрения и использования передовых технологий в сфере интеллектуальной собственности.

Так, одной из технологий, обладающей внушительным потенциалом для интеграции в сферу интеллектуальной собственности, является технология блокчейн (blockchain). Согласно глоссарию с официального сайта Федеральной службы по интеллектуальной собственности под блокчейном понимается «способ хранения данных при помощи программных шифров и цифровых записей, представляющий собой непрерывную цепь блоков, выстроенных по определенным правилам» [12].

В настоящее время блокчейн-технологии уже активно используются в области защиты интеллектуальной собственности. По заявлению Всемирной организации интеллектуальной собственности (ВОИС), международное патентное ведомство будет и далее тесно сотрудничать с государствами-членами и другими партнерами в деле организации и координации работы по вопросам управления, регулирования и стандартизации применения блокчейна в экосистемах интеллектуальной собственности [10].

Применение блокчейна в сфере интеллектуальной собственности, в частности для депонирования объектов интеллектуальной собственности, представляется вполне обоснованным, поскольку специфика данной технологии, характеризующаяся децентрализованностью, независимостью и публичностью, позволяет формировать доказательства, позволяющие подтвердить авторские права еще до обнародования произведения.

Так, ряд компаний в России и в мире уже оказывают услуги по депонированию объектов интеллектуальной собственности как с помощью технологии блокчейн, так и путем использования иных цифровых инструментов, например, облачных сервисов.

Среди зарубежных сервисов, фактически осуществляющих депонирование, целесообразным представляется отметить следующие:

1. Proof of Existence – один из первых сервисов, предоставляющих возможность подтвердить авторские права с помощью технологии блокчейн. Благодаря использованию криптографического хеша и технологии блокчейн сервис предоставляет возможность удостовериться, что файл определенного содержания существовал в определенный момент времени.

2. Virtual Notary – аналогичный указанному выше сервис, который, помимо прочего формирует сертификат, который фиксирует содержание файла в заданное время.

Важным представляется отметить, что перечисленные компании не единственные и охватывают сферу шире, чем просто интеллектуальная собственность. Количество компаний, использующих блокчейн, в частности в целях осуществления депонирования, имеет тенденцию к росту, в том числе ввиду дифференциации

на различные отрасли: интеллектуальная собственность, фотография, валютный рынок, юридический документооборот и др.

В России сервисов, осуществляющих цифровое депонирование немного. Обратим внимание на АО «Национальный реестр интеллектуальной собственности» (n'RIS) и ООО «Айрег» (Интеллектуальный регистратор авторских прав IREG). Данные организации предоставляют авторам возможность осуществить цифровое депонирование и тем самым зафиксировать права автора, обеспечив доказательства посредством свидетельства о депонировании.

Другой заслуживающей внимания российской компанией, осуществляющей цифровое депонирование объектов интеллектуальной собственности на основе технологии блокчейн, является сервис MAGNUM OPUS (ООО «МАГНУМ ОПУС АКП»)

Базовой технологией, выступающей в качестве отличительной особенности сервиса от аналогичных российских сервисов, является использование открытого (публичного) блокчейна, распределенного на сотнях узлов по всему миру. Признак открытости (публичности) характеризует блокчейн как децентрализованный реестр, к которому может присоединиться каждый, а это значит, что никто не имеет контроля над сетью (в отличие от использования закрытого блокчейна), что обеспечивает максимальную независимость и конфиденциальность данных, внесенных в реестр.

Цифровое депонирование на сервисе MAGNUM OPUS осуществляется следующим образом. Пользователь загружает файл. При этом копия самого файла не загружается на сервис, загружается только цифровой отпечаток (хеш), сгенерированный криптографическим алгоритмом SHA-256. Далее, цифровой отпечаток (хеш) вносится в распределенный реестр записей блокчейн-платформы, где создается транзакция с меткой времени, являющейся своеобразной датой приоритета, благодаря которой автор может подтвердить свои авторские права даже на необнародованное произведение, поскольку результаты депонирования дополнительно отражаются в свидетельстве о депонировании.

Говоря о хеше, он представляет собой длинную (64 символа) последовательную цепочку символов, не имеющих какого-либо значения. Причем изначально это абсолютно нормальные данные, из которых создается уникальная комбинация. Особенность хеширования в том, что благодаря ему полностью скрываются исходные данные, что невозможно воссоздать исходный файл. Так, хеш файла выступает в роли своеобразного идентификатора файла. Например, если провести хеширование настоящего документа, то получится следующий хеш: dsubl235uin52ljhb46j2l4bh5poektw342ojipodfhj3i4jn7ysoij4n3d7eku6.

Два цифровых отпечатка (хэша) могут совпасть только в том случае, если в точности совпадают данные, использованные для их вычисления. Таким образом, хэш непосредственно зависит от содержания файла. Если функция хеширования получит тот же документ, она выдаст тот же результат, подтверждающий, что документ не изменился. Если же документ был изменен хотя бы на один символ, новый хэш не совпадет с предыдущим. Так выполняется проверка документов.

Описанные и указанные выше компании свидетельствует о наличии современных механизмов для предоставления дополнительной правовой охраны объектам интеллектуальной собственности. Однако компании, осуществляющие цифровое депонирование, являются по своей природе частными, что позволяет сделать вывод о целесообразности рассмотрения вопроса о формировании в Российской Федерации государственной системы депонирования. Например, в рамках деятельности Роспатента, где можно осуществить регистрацию авторских прав на программу для ЭВМ, что по своей сути напоминает процедуру депонирования. Важным представляется подчеркнуть, что речь идет именно о формировании государственной цифровой системы депонирования путем использования технологии блокчейн.

Использование современных цифровых технологий (блокчейн, хеш-функция и др.) в сфере интеллектуальной собственности представляется обоснованной и необходимой мерой, которая также не противоречит международно-правовым актам. Например, в договоре ВОИС по авторскому праву (ДАП) (1996 г.) отмечается, что сторона договора должна обеспечить наличие процедур защиты прав, позволяющих принимать эффективные меры против любого нарушения прав. «Такие меры должны включать как оперативные меры, предотвращающие нарушения, так и меры, служащие сдерживающим средством против дальнейших нарушений» [3]. Таким образом, свидетельства, которые формируются в результате цифрового депонирования, в полной мере коррелируют с положениями Договора ВОИС по авторскому праву и способствует как дополнительной правовой охране, так и обеспечению эффективных мер защиты.

Итак, в сфере интеллектуальной собственности актуальной остается проблема обеспечения защиты авторских прав. Действительно, международное и национальное законодательства ряда стран предоставляет авторам автоматическую охрану их произведений, однако с практической точки зрения подобный подход обуславливает ряд проблем в осуществлении защиты авторских прав. Представляется, что использование современных цифровых технологий в виде блокчейна и хеш-функции позволит обеспечить благоприятный эффект на развитие интеллектуальной собственности и, в частности, на развитие авторского права.

Список литературы

1. Бернская Конвенция по охране литературных и художественных произведений от 09.09.1886 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_5112/ (дата обращения: 05.09.2022).
2. Соглашение стран СНГ от 24.09.1993 «О сотрудничестве в области охраны авторского права и смежных прав» СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_5865/ (дата обращения: 05.09.2022).
3. Договор ВОИС по авторскому праву (ДАП) (1996 г.) WIPO. URL: https://www.wipo.int/treaties/ru/ip/wct/summary_wct.html (дата обращения: 05.09.2022).
4. Гражданский кодекс Российской Федерации (часть четвертая): Федеральный закон от 18.12.2006 № 230-ФЗ // Собрание законодательства РФ. 2006. № 52 (Часть 1). Ст. 5496.

5. Постановление Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_323470/ (дата обращения: 05.09.2022).

6. Гражданский кодекс Республики Казахстан // Ваш гид в законодательстве Казахстана. URL: https://kodeksy-kz.com/ka/grazhdanskiy_kodeks_osobennaya_chast/979.htm (дата обращения: 05.09.2022).

7. Москаленко А. И. «Гражданско-правовая охрана и защита авторских прав в сети Интернет» // Журнал «Образование и право». 2020. № 8. С. 165.

8. Анализ судебной практики за 2020 год по спорам, связанным с защитой авторских прав на фотографические произведения, размещенные в сети «Интернет» // RTM Group. URL: <https://rtmtech.ru/research/analiz-sudebnoj-praktiki-za-2020-g-zashhita-avtorskih-prav-na-foto/> (дата обращения: 05.09.2022).

9. Блокчейн и интеллектуальная собственность // WIPO. URL: <https://www.wipo.int/cws/ru/blockchain-and-ip.html> (дата обращения: 05.09.2022).

10. Бюро авторского права США // COPYTRUST. URL: <https://www.copytrust.ru/articles/Byuro-avtorskogo-prava-SShA> (дата обращения: 05.09.2022).

11. Глоссарий // Роспатент. Федеральная служба по интеллектуальной собственности. URL: <https://rospatent.gov.ru/ru/glossary> (дата обращения: 05.09.2022).

12. Решение Ленинского районного суда г. Краснодара от 2 июля 2020 г. // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/fCbVB85P6wJp/?regular-txt=®ular-case_doc=2-3845%2F2020+®ular-lawchunkinfo=®ular-date_from=®ular-date_to=®ular-workflow_stage=®ular-area=®ular-court=®ular-judge=&_=1663511453092 (дата обращения: 05.09.2022).

13. Решение Куйбышевского районного суда г. Санкт-Петербурга от 06.07.2020 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/YyDt80yMQNxV/?regular-txt=®ular-case_doc=2-654%2F20®ular-lawchunkinfo=®ular-date_from=®ular-date_to=®ular-workflow_stage=®ular-area=1013®ular-court=®ular-judge=&_=1663511335528 (дата обращения: 05.09.2022).

14. Решение Октябрьского районного суда г. Барнаула Алтайского края от 30.07.2020 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/1dBC3Mf19dxC/?regular-txt=®ular-case_doc=2-1636%2F2020®ular-lawchunkinfo=®ular-date_from=®ular-date_to=®ular-workflow_stage=®ular-area=®ular-court=®ular-judge=&_=1663511276078 (дата обращения: 05.09.2022).

М. Н. Каргин,

студент,

Удмуртский государственный университет

Д. В. Хижняков,

студент,

Удмуртский государственный университет

Н. Н. Щенин,

студент,

Удмуртский государственный университет

ПРОБЛЕМЫ ВНЕДРЕНИЯ ДИСТАНЦИОННОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ В ПРАВОВУЮ СИСТЕМУ ИЗБИРАТЕЛЬНОГО ЗАКОНОДАТЕЛЬСТВА И ЕГО ПРИМЕНЕНИЯ НА ПРАКТИКЕ

Аннотация. Цель исследования – выявить и описать проблемы внедрения дистанционного электронного голосования в законодательство Российской Федерации. Акцентируется внимание на зарубежном и российском опыте внедрения дистанционного электронного голосования; выделяются как универсальные проблемы, характерные для любого государства, использующего дистанционное электронное голосование, так и частные проблемы, которые характерны для Российской Федерации. Анализируется уровень влияния такого формата голосования на электоральное поведение избирателей.

Ключевые слова: право, цифровые технологии, конституционное право, избирательное право, выборы, дистанционное электронное голосование

PROBLEMS OF INTRODUCING THE ONLINE VOTING IN THE LEGAL SYSTEM OF THE ELECTORAL LEGISLATION AND ITS APPLICATION IN PRACTICE

Abstract. The purpose of the study is to identify and describe the problems of introducing remote electronic voting into the legislation of the Russian Federation. The article focuses on foreign and Russian experience in implementing remote electronic voting; both universal problems characteristic of any state using the online voting, and particular problems that are typical for the Russian Federation are singled out. The level of influence of such a voting format on the electoral behavior of voters is analyzed.

Keywords: Law, Digital technologies, Constitutional law, Suffrage, Elections, Remote electronic voting

В наши дни развитие и распространение цифровых технологий влияет, в том числе и на правовые отношения. Во всем мире государства начали активно внедрять цифровые технологии как в сфере частного права, так и в сфере публичного. Пожалуй, самым революционным и неоднозначным применением цифровых технологий в системе правовых отношений можно считать внедрение дистанционного электронного голосования (ДЭГ) в Российской Федерации.

Легальное понятие дистанционного электронного голосования закреплено в п. 62.1 ст. 2 ФЗ «Об основных гарантиях избирательных прав и права на уча-

стие в референдуме граждан Российской Федерации», согласно данной статье, дистанционное электронное голосование – голосование без использования бюллетеня, изготовленного на бумажном носителе, с использованием специального программного обеспечения [5].

В 2022 г. был принят и опубликован законопроект № 40921–8 «О внесении изменений в отдельные законодательные акты Российской Федерации», который был направлен на совершенствование законодательства в части дистанционного электронного голосования [1]. Документом унифицируются правила и процедуры при проведении выборов разных уровней с использованием дистанционного электронного голосования как в целом в России, так и в регионах.

Одной из целей, которая может быть достигнута путем введения дистанционного электронного голосования, является облегчение осуществления активного избирательного права граждан – дистанционное электронное голосование должно сделать процедуру доступнее для лиц, которые по каким-либо причинам не могут лично посетить избирательный участок.

Некоторые ученые также отмечают, что введение дистанционного электронного голосования должно привести к повышению явки на выборах [7]. Однако с этим можно согласиться лишь отчасти. Так, на выборах в Московскую городскую Думу шестого созыва в 2014 г. явка избирателей составила 21,04 %, в то время как на выборах в Мосгордуму седьмого созыва в 2019 г., на которых впервые в России использовалось дистанционное электронное голосование, явка составила 21,77 %.

Исследуя опыт других стран в части введения дистанционного электронного голосования, можно заметить, что использование его помогает понизить расходы на организацию выборов, поскольку со временем снизится количество избирателей, голосующих бумажными бюллетенями. Так, к примеру, на выборах в парламент Эстонии в 2007 г. доля избирателей, голосовавших электронным способом, составляла 5,5 %, а на выборах 2019 г. эта доля составляла уже 43,75 % [8].

Неудивительно, что дистанционное электронное голосование с каждым годом становится все более актуальным. Во многом это связано с появлением новых технологий, которые направлены на создание возможности проголосовать удаленно безопасно и анонимно, но, помимо этого, в России на внедрение дистанционного электронного голосования сильно повлияла и пандемия COVID-19.

Но, несмотря на все вышеизложенное, следует отметить, что у дистанционного электронного голосования есть ряд проблем, с которыми сталкивались во многих странах, введивших в свое национальное законодательство институты похожие на дистанционное электронное голосование.

Ряд стран исследовали и опробовали системы интернет-голосования с начала 2000-х гг.

Например, Штат Женева в Швейцарии ввел электронное голосование в 2003 г. Другие швейцарские кантоны последовали этому примеру, однако, доля голосов, поданных через Интернет, оставалась низкой и составляла около 2 % по всей стране, а в 2019 г. дистанционное электронное голосование было приостановлено после обнаружения недостатков безопасности в используемых системах голосования [15].

Норвегия экспериментировала с интернет-голосованием на выборах, состоявшихся в 2011 и 2013 г., но отказалась от программы из-за опасений, что анонимность голосования не гарантируется [13].

Интернет-голосование было опробовано на местных выборах в Соединенном Королевстве в период с 2002 по 2007 г., но от него отказались.

Франция разрешила интернет-голосование на выборах в законодательные органы заморских территорий с 2012 г., но прекратила эту практику из-за опасений кибератак в 2017 г. [22].

В то время как некоторые европейские страны, такие как Литва, планируют внедрить системы электронного голосования для зарубежных избирателей, другие, такие как Финляндия, по-прежнему скептически относятся к электронному голосованию, поскольку рабочие группы, созданные правительствами, утверждают, что риски перевешивают преимущества. Небольшие автономные финские острова Аландские острова отказались от своих планов по использованию интернет-голосования на местных выборах по соображениям безопасности всего за пару дней до начала избирательного периода [14, 20].

За пределами Европы интернет-голосование использовалось на муниципальных выборах в канадских провинциях Онтарио и Новая Шотландия [17]. В нескольких штатах США, в том числе в Нью-Джерси, Делавэре и Западной Вирджинии, иностранным избирателям, военным и инвалидам разрешено голосовать через Интернет, и еще несколько штатов рассматривают такую возможность. В Азии Пакистан недавно провел небольшие испытания интернет-голосования для зарубежных избирателей; в Индии испытания проводились в штате Гуджарат. В Австралии два крупных региона, Новый Южный Уэльс и Западная Австралия, позволяют определенным группам избирателей, в том числе избирателям с ограниченными возможностями и отсутствующим избирателям, дистанционно голосовать через Интернет на региональных выборах.

Таким образом, большинство экспериментов с интернет-голосованием в мире были ограничены по масштабу, проводились на уровне субъектов и в большинстве случаев были прекращены.

Но единственным государством, в котором прочно закрепился способ дистанционного электронного голосования, является Эстония [18].

Выборы в национальный парламент, проводятся каждые четыре года. Советы местного самоуправления сроком на четыре года также избираются на общенациональных выборах. С тех пор как Эстония присоединилась к ЕС в 2004 г., выборы в Европейский парламент проводятся каждые пять лет. Избирательная система представляет собой форму пропорционального представительства с открытыми списками: избиратели голосуют за кандидата по партийному списку, и партии получают места пропорционально доле полученных голосов. Список избирателей составляется на основании Регистра населения; регистрация избирателя не требует каких-либо действий со стороны гражданина. Механизмы обычного бумажного голосования заключаются в следующем. День выборов – воскресенье. Досрочное голосование доступно в течение назначенной недели. Избиратели с особыми потребностями могут получить урну для голосования на дом или по месту жительства. Избиратели, постоянно или временно проживающие за границей (которых

на недавних выборах насчитывалось более 80 000 человек), могут проголосовать в дипломатическом представительстве Эстонии или заказать бюллетень для голосования по почте [18].

Интернет-голосование используется на национальных, европейских и местных выборах с 2005 г. Дистанционное электронное голосование, являющееся дополнительной альтернативой обычному бумажному голосованию, доступно в течение установленного периода досрочного голосования (с десятого по четвертый день до дня выборов). Избиратели могут проголосовать с любого компьютера, подключенного к Интернету, из любой точки мира. С веб-страницы выборов избиратели сначала загружают приложение для голосования и запускают его на своих компьютерах. Затем они аутентифицируют себя с помощью эстонской ID-карты или мобильного ID, просматривают список кандидатов, баллотирующихся в их округе, делают свой выбор, шифруют его и подтверждают свой голос цифровой подписью. Весь процесс занимает в среднем менее двух минут [19]. Примечательно, что избиратели могут изменять свои электронные голоса неограниченное количество раз в течение периода досрочного голосования, при этом каждое новое голосование аннулирует предыдущие. Голосование на избирательном участке в период досрочного голосования аннулирует бюллетень, поданный через Интернет. Эти положения введены для защиты тайны голосования: избиратель, которого принуждали или запугивали голосовать определенным образом, может подать новый бюллетень и перезаписать свой предыдущий голос. До 2021 г. избиратели не могли проголосовать в день выборов, так как их имена были удалены из соответствующих списков избирателей. С 2021 г. избиратели могут подавать бумажные бюллетени в день выборов, тем самым аннулируя свой электронный голос.

В результате сложившейся практики проведения ДЭГа, а также исследований, проведенных европейской комиссией, у голосования, проведенного с помощью интернет-технологий, существуют преимущества и недостатки. Среди преимуществ можно выделить следующие [21]:

- ДЭГ может включать функции, позволяющие лицам с ограниченными возможностями голосовать без посторонней помощи;
- ДЭГ могут использовать люди, проживающие в отдаленных районах, – им могут пользоваться люди, живущие за границей, в том числе те, у кого поблизости нет консульства;
- сокращает время, затрачиваемое избирателями на дорогу, поскольку люди могут голосовать из любого места, где есть подключение к Интернету;
- компьютерная система может проверить, проголосовал ли человек более одного раза;
- нет зависимости от избирательных комиссий;
- может уменьшить количество ошибок при подсчете;
- результаты могут быть подсчитаны автоматически;
- предположительно, может быть увеличена электоральная явка.

К недостаткам голосования, проведенного при помощи интернет-технологий, можно отнести [21]:

- голосование происходит в неконтролируемой среде. Трудно обеспечить, чтобы люди голосовали свободно;

- усложняется администрирование выборов;
- существует риск кибератак со стороны внутренних или внешних субъектов, которые могут манипулировать голосами;
- атаки типа «отказ в обслуживании» могут помешать гражданам проголосовать;
- ошибки программного обеспечения или вредоносные программы на устройствах избирателей могут повлиять на голосование. От избирателей может потребоваться обновить свое программное обеспечение или браузеры;
- может быть трудно одновременно гарантировать точную идентификацию избирателя и сохранение тайны;
- идентификационные коды могут быть украдены или проданы;
- трудно наблюдать за процессом, не полагаясь на опыт специалиста;
- может быть трудно проверить, прибыло ли голосование;
- пересчет голосов может быть затруднен, что усложняет проверку результатов;
- существуют некоторые расходы, связанные с разработкой и обслуживанием программного обеспечения, а также с обеспечением безопасности, доступностью Интернета и использованием услуг электронного правительства в той или иной связи.

В России дистанционное электронное голосование начало приобретать определенную роль начиная с 2019 г., когда идею проведения эксперимента по дистанционному электронному голосованию была формализована депутатами Государственной Думы, а также Центральная избирательная комиссия Российской Федерации в форме федерального закона «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва» [4]. Закон был опубликован и утвержден Президентом РФ 29 мая 2019 г. Система электронного голосования с применением платформы блокчейн применялась в трех избирательных округах Москвы. Избиратели могли использовать специально созданный для выборов сервис, посредством которого осуществлялось голосование. Итогом применения указанной технологии стал рост явки избирателей на тех участках, где она была реализована [6]. Минусом тестовой технологии стали многочисленные несовершенства технического характера, например, при проведении голосования часть граждан, участвующих в выборах, не могла зайти в систему для голосования, к тому же часть лиц, обладающим статусом «наблюдатель» были лишены реальной возможности получить ключи для входа в систему. Вопреки проблемам, которые появляются в результате применения блокчейна, практика, показала, что система весьма востребована – участвовали свыше десяти тысяч человек (10 % от общего количества принявших участие в выборах избирателей).

Следующий этап применения ДЭГ – общероссийское голосование по вопросам поправок в Конституцию, состоявшееся 1 июля 2020 г. Центральная избирательная комиссия Российской Федерации приняла решения применять данную форму голосования в двух субъектах: Москве и Нижегородской области [3]. Тогда уже свыше миллиона избирателей проголосовали дистанционно (17,5 % от числа

принявших участие). В этом же 2020 г. ДЭГ было задействовано на дополнительных выборах депутатов Госдумы в Ярославской и Курской областях, где практически 9 % избирателей использовали дистанционный способ голосования.

В 2021 г. технология дистанционного электронного голосования использовалась на выборах депутатов нижней палаты федерального парламента, а также региональных и муниципальных органов власти. По решению ЦИК РФ от 25 мая 2021 г. электронное голосование в эти дни проводилось в семи субъектах Федерации: городах Москве и Севастополе, Нижегородской, Ярославской, Курской, Мурманской и Ростовской областях [2]. Итогами ДЭГ 2021 г. стало то, что уже каждый третий избиратель, имевший доступ к ДЭГ, предпочел именно такой формат голосования.

Применение системы дистанционные электронного голосования повлекло амбивалентное отношение общественности к данному явлению. Центральное место в общем дискурсе, касающемся ДЭГ, заняло голосование в Москве по причине наличия в ней уникальной платформы, отличной от той, которая применялась в Российской Федерации. Результаты голосования сохранялись на дискете и передавались в ГАС «Выборы», по этой причине процесс подведения итогов стал более продолжительным, что превысило ожидания организаторов и вызвало дискуссии о причинах длительности процесса [9]. Итоги ДЭГ существенно повлияли на 7 из 15 столичных одномандатных округов. Это вызвало критику со стороны оппозиционных партий и общественный резонанс, что вылилось в непризнание некоторыми политическими силами результатов ДЭГ и множество административных исков от оппозиции.

Исходя из вышеизложенного, следует резюмировать: дистанционное электронное голосование оказывает существенное влияние на ход избирательного процесса.

Во-первых, это выражается в его влиянии на общую явку избирателей. Так, директор Центра политического анализа и социальных исследований, политолог П. В. Данилин, отмечая итоги выборов 2021 г., заявил, что ДЭГ крайне положительно влияет как на общую явку по проходящим в России выборам в Госдуму, так и на явку граждан в региональные законодательные собрания. При этом экспертом отдельно выделяется удобство самой процедуры: «Электронное голосование, безусловно, удобно, в частности, тем, что некоторые люди, например, боятся выходить из дома из-за коронавируса, им удобно делать выбор, сидя на диване. Им комфортно просто нажать несколько клавиш на компьютере. Это голосование будущего» [11].

В частности, аналогичное мнение приводит В. И. Федоров в своей работе «Дистанционное электронное голосование и явка избирателей: опыт Эстонии и Москвы». Он приводит статистические данные, согласно которым явка на выборах в Мосгордуму в 2019 г. по сравнению с 2014 г. выросла на 0,60 % в связи с применением упомянутой ранее формой голосования [8].

Во-вторых, некоторые эксперты отмечают отдельную прозрачность и порядок процедуры голосования с применением ДЭГ. Например, Д. А. Журавлев политолог, генеральный директор Института региональных проблем считает, что дистанционное электронное голосование не только гарантирует порядок и прозрачность выборного процесса, но и исключает возможности для спекуляций с бюллетенями [10].

В-третьих, эксперты отмечают инновационность такого формата голосования, что в значительной мере может повлиять на явку молодежи на выборы. По мнению проректора Саратовского института развития образования, доктора политических наук, профессора М. В. Данилова, за дистанционным электронным голосованием – будущее. «Опыт пилотных регионов, где такая технология уже применялась, показывает, что возможность проголосовать с помощью различных гаджетов была позитивно воспринята обществом». При этом он подчеркнул, что ДЭГ является действенным методом вовлечения в избирательный процесс молодых граждан. Этот факт отмечает, в том числе ВЦИОМ в аналитическом докладе, который касается позиции жителей России к такому формату голосования, существующих барьеров данного формата, а также долгосрочных последствий внедрения электронного голосования в будущем. В частности, отмечается, что ДЭГ больше всего поддерживают лица в возрасте от 18 до 34 лет, упомянутые субъекты избирательного процесса меньше других участвуют в обычной форме голосования и, как правило, используют тактику ситуативного участия. Отсюда следует, что лица, относящиеся к возрастной группе молодежь, в результате внедрения ДЭГ увеличат свою электоральную активность.

В связи с этим можно предположить, что в результате обеспечения возможности голосовать дистанционно через Интернет электоральное поведение молодежи может стать более активным [13].

Таким образом, при введении и использовании ДЭГ субъекты проведения голосования, а также избиратели столкнутся со следующими проблемами:

1. Интернет-голосование усложняет администрирование выборов, а не упрощает его. Внедряя электронное голосование, публичные правовые субъекты берут на себя долгосрочное обязательство по развитию технологий, созданию правовой базы, корректировке управления выборами и защите системы от атак, критики и дезинформации как на внутренней, так и на международной арене. Разработка нормативно-правовой базы для электронного голосования требует времени, влечет за собой значительные нормативные инновации и требует постоянных усилий по разъяснению и защите системы в соответствии с установленными стандартами демократических выборов. В то время как широкомасштабное электронное голосование может снизить потребность в развертывании избирательных участков и персонале, не следует недооценивать проблему развертывания электронного голосования и его администрирования параллельно с традиционной системой голосования на бумажных носителях. В частности, Эстонский опыт показывает, что широкомасштабное внедрение интернет-голосования увеличивает административную сложность и увеличивает нагрузку на избирательные органы [18].

2. Интернет-голосование не гарантирует повышение явки [16]. В частности, данные по одиннадцати эстонским выборам показывают, что, несмотря на массовое распространение интернет-голосования, уровень участия в выборах остается стабильным. Также это подтверждается выводами исследований о том, что использование интернет-голосования является самым низким среди тех сегментов эстонского электората, которые менее всего склонны голосовать. То есть ДЭГ не

повышает общую явку избирателей, а лишь заменяет очную явку на заочную посредством ДЭГ, так как облегчает участие в выборах тех, кто все равно собирался голосовать, но оно не стимулирует лиц, обладающих активным избирательным правом и относящихся к выборам индифферентно, участвовать в избирательном процессе. Обратимся к российскому опыту, например, в 2022 г. ДЭГ широко применялся в избирательном процессе в Российской Федерации и по результатам выборов с применением данной технологии далеко не во всех случаях выросла явка избирателей: в Калининградской области явка по сравнению с предыдущими выборами сократилась на 0,84 %, а в Ярославской области на 7,2 %, в то же время в других регионах явка увеличилась.

3. Еще одной не менее важной проблемой внедрения дистанционного электронного голосования является уязвимость активного и пассивного избирательных прав при сбоях. Безусловно, никто не застрахован от технических проблем и неполадок, так и дистанционное электронное голосование, как и любая система, напрямую связанная с техническим фактором, способна показывать нарушения в работе, что, разумеется, может отразиться как на волеизъявлении граждан, так и на конечный результат выборов, который окажет влияние уже на кандидатов на ту или иную выборную должность [6].

4. Обеспечение анонимности избирателей при дистанционном электронном голосовании является одной из главных проблем. Поскольку для предоставления избирателю возможности проголосовать дистанционно ему необходимо подтвердить свою личность, предоставив личные данные системам проверки, возможны проблемы с обеспечением безопасности его персональных данных и вследствие с анонимностью голосования.

При дистанционном электронном голосовании система онлайн-голосования должна подтвердить личность избирателя, чтобы убедиться, что лицо имеет право голосовать на данных выборах. При этом система также должна гарантировать анонимность избирателю, отделяя его личность от его волеизъявления, чтобы никто не мог связать его бюллетень с его личностью. Необходимость подтвердить личность и при этом разорвать связь между личностью избирателя и бюллетенем, который он подал, является уникальной проблемой дистанционного электронного голосования [6].

Проблема соблюдения принципа анонимности при проведении дистанционного электронного голосования не исчерпывается только лишь риском потери или утечки данных. Другое выражение данной проблемы заключается в возможности слежки и давления на избирателя непосредственно при голосовании. В частности, на избирателей может оказываться давление на месте работы, службы, учебы при котором руководитель под угрозой применения каких-либо дисциплинарных мер будет требовать от своих подчиненных голосовать под его наблюдением за нужный вариант в бюллетене.

5. Чтобы обеспечить надлежащую безопасность дистанционных выборов, потребуется надежная система проверки личности. В Российской Федерации нет федеральной избирательной инфраструктуры, позволяющей достоверно идентифицировать пользователя. В частности, в отличие от стран, которые начали онлайн-голосование, таких как Эстония, Российская Федерация не выдает на-

циональные удостоверения личности со встроенными верифицирующими интернет-ключами (ID-карты). Кроме того, компьютеры и мобильные устройства в РФ не оснащены устройствами для безопасного считывания этих карт.

6. К тому же среди основных проблем, возникающих при применении дистанционного электронного голосования, эксперты выделяют слабую проработанность закона, курирующего процедуру проведения и формат проведения такого голосования. В частности, выделяются: отсутствие гарантий правовой определенности и стабильной системы голосования – документ не описывает сроки подачи заявления на голосование, порядок аутентификации, установления итогов и так далее; отсутствие четкой регламентации системы наблюдения; отсутствие гарантии контрольного подсчета голосов – процедура должна быть воспроизводима в суде при спорах. Ряд экспертов считают, что на практике это может привести к снижению эффективности наблюдения за ДЭГ, трудностям при подготовке наблюдателей и недостаточной прозрачности процедуры голосования, особенно в случае использования региональных систем.

Резюмируя, следует сказать, что дистанционное электронное голосование, безусловно, является передовым и инновационным способом организации избирательного процесса, который способен потенциально увеличить степень участия граждан в выборах, обеспечить доступность активного избирательного права. Однако данный способ организации избирательного процесса имеет определенные риски, которые способны негативно повлиять на ход избирательного процесса. В частности, исказить результаты выборов, уменьшить уровень доверия избирателей к их результатам, поставить под сомнение честность и прозрачность самых выборов, а также повышает расходы на организацию избирательного процесса (в случае сохранения традиционного формата выборов), усложняет администрирование выборов. Формат дистанционного электронного голосования требует значительной законодательной и подзаконной доработки.

Список литературы

1. О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 14.03.2022 № 60-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_411443/ (дата обращения: 16.09.2022).

2. О дистанционном электронном голосовании на выборах 19 сентября 2021 года: Постановление Центральной избирательной комиссии Российской Федерации от 25.05.2021 № 7/49-8.

3. О Порядке дистанционного электронного голосования при проведении общероссийского голосования по вопросу одобрения изменений в Конституцию Российской Федерации: Постановление Центральной избирательной комиссии Российской Федерации от 04.06.2020 № 251/1850-7.

4. О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва: Федеральный закон от 29.05.2019 № 103-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_325552/ (дата обращения: 16.09.2022).

5. Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации: Федеральный закон от 12.06.2002 № 67-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_37119/ (дата обращения: 16.09.2022).
6. Алексеев Р. А., Абрамов А. В. Перспективы и проблемы применения технологии блокчейн на выборах в России и за рубежом // Журнал Гражданин. Выборы. Власть. – 2020. – № 1 (15) – С. 9–21.
7. Закускин А. А. Внедрение электронных технологий в российский избирательный процесс // Вестник Марийского государственного университета. Серия «Исторические науки. Юридические науки». 2019. № 3 (19). URL: <https://cyberleninka.ru/article/n/vnedrenie-elektronnyh-tehnologiy-v-rossiyskiy-izbiratelnyuy-protsess>
8. Федоров В. И. Дистанционное электронное голосование и явка избирателей: опыт Эстонии и Москвы // Организация выборов и избирательные технологии. 2019. № 4. С. 37–42.
9. Федоров В. И., Ежов Д. А. Эволюция электронного голосования в России: проблемы классификации и периодизации // Вестник Московского государственного областного университета. 2021(1):146–162. <https://doi.org/10.18384/2224-0209-2021-1-1055>
10. Политолог назвал ДЭГ гарантией порядка и прозрачности голосования». URL: <https://lenta.ru/news/2022/08/08/vbr22/> (дата обращения: 16.09.2022).
11. Политолог оценил влияние ДЭГ на общую явку на выборах. URL: <https://iz.ru/1223849/2021-09-19/politolog-otcenil-vliianie-deg-na-obshchuiu-iavku-na-vyborah> (дата обращения: 16.09.2022).
12. Эксперты заявили о необходимости разъяснения процедуры электронного голосования. URL: <https://lenta.ru/news/2022/02/02/deg1/> (дата обращения: 16.09.2022).
13. Bull C., Gjosteen K., Nore H. *Faults in Norwegian Internet Voting*; TUT Press: Lochau, Austria; Bregenz, Austria, 2018.
14. Duenas-Cid D., Krivosova I., Serrano R., Freire M., Krimmer R. *Tripped at the Finishing Line: The Aland Islands Internet Voting Project*. In Krimmer. R. et al. (eds) *Electronic Voting. Fifth International Joint Conference, E-Vote-ID 2020*. Springer International Publishing, Cham: pp. 33–49.
15. Germann M. & Serdült U. (2017). *Internet voting and turnout: Evidence from Switzerland*. *Electoral Studies*, 47, 1–12–1.
16. Solvak M., Vassil K. (2018). *Could Internet Voting Halt Declining Electoral Turnout? New Evidence That E-Voting Is Habit Forming*. *Policy & Internet*, 10 (1), 4–21. DOI: 10.1002/poi3.160.
17. Goodman N., Gabel C. *Internet voting: Strengthening Canadian democracy or weakening it? Digital Politics in Canada: Promises and Realities (2020)*, pp. 90–111.
18. Piret E., Solvak M., Willemson J., Vinkel P. (2022). *Internet voting in Estonia 2005–2019: Evidence from eleven elections*. *Government Information Quarterly*. 39. 10.1016/j.giq.2022.101718.
19. Haenni R., Koenig R., Wikström D. (2015). *E-Voting and Identity: 5th International Conference, VoteID 2015, Bern, Switzerland, September 2-4, 2015, Proceedings*. 10.1007/978-3-319-22270-7.

20. Krimmer R., Dueñas-Cid D., Spycher K., Iuliia Serrano Iova R., Freire M., Wrede C. (2019). Nordic Pioneers: facing the first use of Internet Voting in the Åland Islands (Parliamentary Elections 2019). 10.31235/osf.io/5zr2e.

21. Lupiáñez-Villanueva F., Devaux A., Faulí C., Stewart K., Porcu F., Taylor J., Theben A., Baruch B., Folkvord F., Nederveen F. (2020). Study on the Benefits and Drawbacks of Remote Voting. Brussels: European Commission. DOI 10.2838/677948

22. Reuters Staff. France drops electronic voting for citizens abroad over cybersecurity fears. March 6, 2017 URL: <https://www.reuters.com/article/us-franceelection-cyber-idUSKBN16D233> (дата обращения: 16.09.2022).

Г. Ю. Каримова

доцент, кандидат юридических наук,
Башкирский государственный университет

С. В. Лежнев,

магистрант,
Башкирский государственный университет

ЦИФРОВАЯ ИДЕНТИФИКАЦИЯ НАЛОГОПЛАТЕЛЬЩИКА

Аннотация. Статья посвящена исследованию цифровой идентификации налогоплательщика. Рассмотрены особенности идентификации налогоплательщика, специфичные для налоговой отрасли, сопоставлены выводы схожих исследований проблем цифровой идентификации личности при доступе в государственные информационные системы. На основе исследований подтверждается отсутствие полноты урегулирования в сфере цифровизации налоговых правоотношений по рассматриваемому вопросу и намечается вектор развития. Предложено внесение дополнений в проект нормативно-правового акта, дано обоснование способов цифровой идентификации налогоплательщика и защиты информации.

Ключевые слова: цифровая идентификация, налогоплательщик, электронная подпись, идентификация граждан, информационная система, цифровой паспорт, идентификационный номер налогоплательщика

DIGITAL TAXPAYER IDENTIFICATION

Abstract. The article is devoted to the study of the digital identification of the taxpayer. The features of taxpayer identification specific to the tax industry are considered, the conclusions of similar studies of the problems of digital identification of the individual when accessing state information systems are compared. Based on the research, the lack of completeness of the settlement in the field of digitalization of tax legal relations on the issue under consideration is confirmed and a vector of development is outlined. The introduction of amendments to the draft regulatory legal act is proposed, the justification of the ways of digital identification of the taxpayer and information protection is given.

Keywords: Digital identification, Taxpayer, Electronic signature, Identification of citizens, Information system, Digital passport, Tax identification number

Научно-технический прогресс, явивший миру информационные и коммуникационные технологии, породил посредством последних процесс цифровизации общества, который стремительно развиваясь, трансформирует общественные отношения. Менее чем за полвека коммуникации между людьми приросли новыми способами передачи информации, обрели информационно-технические инструменты, расширив возможности и круг общения. Решение различных вопросов при обращении в органы государственной власти посредством информационно-коммуникационных технологий в режиме удаленного доступа, стало таким же обычным явлением, как и разговор по телефону. Новые реалии повышают роль правового регулирования отношений, требуя научного осмысления феноменов, появившихся в результате стремительной информатизации общества. Необходимы как научные исследования происходящих социально-технологических изменений, так и переосмысление используемых в науке и в текстах нормативных актов классических понятий, внесения соответствующих изменений (например, до сих пор в Кодексе Российской Федерации об административных правонарушениях не предусмотрена возможность подачи документов, обращений, жалоб на состоявшиеся по делу об административном правонарушении акты в электронном виде).

Бесспорно, что в любой публично-правовой коммуникации ее неотъемлемой частью является идентификация взаимодействующих сторон. За последнее время феномену удаленной цифровой идентификации личности посвящено большое количество научных исследований. Однако отсутствие исследований относительно цифровой идентификации налогоплательщика не свидетельствует об отсутствии необходимости таких исследований. Следует отметить, что личность и налогоплательщик соотносятся как своего рода часть и целое. Цифровая идентификация налогоплательщика шире личности не только по субъектному составу (например, налогоплательщиком может быть юридическое лицо, физическое лицо, индивидуальный предприниматель), но и по способам идентификации (например, идентификация по идентификационному номеру налогоплательщика (ИНН)).

Для налоговой службы во многих случаях «отправной точкой» идентификации налогоплательщика служит ИНН. К примеру, налоговая декларация (расчет) представляется с указанием идентификационного номера налогоплательщика (ст. 80 НК РФ) [3].

Но идентификация налогоплательщика по ИНН с использованием сведений, полученных через сеть Интернет (например, принадлежность определенному лицу налоговой декларации), является, по сути, юридической фикцией (или презумпцией) определенного лица. Суждения о юридической природе идентификации налогоплательщика по ИНН без придания ей значения юридического факта законодателем оказываются не чем иным, как схоластикой.

Особенность идентификации налогоплательщика проявляется на практике с ракурса специфики работы налоговых органов и внешнему наблюдателю по отношению к ФНС России не видна. По запросам уполномоченных органов (например, по запросам от органов МВД [6]), налоговая служба осуществляет информационный обмен сведениями, в том числе в электронном виде, представ-

ляющими интерес для сторон и непосредственно связанными с выполнением задач и функций, возложенных на них законодательными и иными нормативными правовыми актами Российской Федерации. Одними из таких сведений являются сведения об операторе связи и об IP-адресах, через которые происходила отправка налоговой отчетности по телекоммуникационным каналам связи (IP-адрес, дата и время отправки, отпечаток электронной цифровой подписи) за определенный период времени. Возможность предоставить упомянутые сведения ограничена, во-первых, техническими особенностями передачи данных по телекоммуникационным каналам связи и связана со сложностями в однозначном определении местонахождения IP-адреса отправителя налоговой декларации, а, во-вторых, недостаточностью необходимых полномочий [3] налоговых органов по запросу соответствующей информации у провайдера. Потребность в сведениях (об IP-адресах, о местонахождении устройств, с которых осуществлялся доступ, о дате и времени активности пользователя) возникает у налоговых органов и при обращениях граждан, например, информационное обращение гражданина об уклонении интернет-магазина от уплаты налогов. При этом данными сведениями, опять же в силу технических особенностей передачи данных, может обладать в совокупности несколько операторов связи, к тому же один из операторов связи может оказаться за пределами юрисдикции Российской Федерации (например, сервер интернет-магазина физически находится в г. Москве, а его администрирование ведется из другой страны). Следовательно, данные правоотношения налоговых органов Российской Федерации следует рассматривать и в международно-правовой плоскости.

При этом тезис о том, что налоговые правоотношения в информационной среде Интернета носят международно-правовой характер, подтверждает анализ модели угроз информационной безопасности. Хакерские атаки осуществляются с территории недружественных стран, и личные кабинеты физических, самозанятых лиц и индивидуальных предпринимателей уязвимы, так как доступ в личные кабинеты, среди прочих вариантов, может быть осуществлен и с использованием простой электронной подписи (набора реквизитов: логин и пароль). Доступ в личный кабинет юридического лица более защищен, для подключения к сервису «Личный кабинет юридического лица» необходимо получить квалифицированный сертификат ключа проверки электронной подписи (далее КСКПЭП) в удостоверяющем центре, аккредитованном в сети доверенных удостоверяющих центров Минкомсвязи России, участником которой является и ФНС России, в соответствии с требованиями Федерального закона от 6 апреля 2011 г. № 63-ФЗ. В любом случае доступ в любой из личных кабинетов осуществляет реальный человек: физическое или должностное лицо. В этой связи представляется целесообразным в первую очередь проанализировать вопрос цифровой идентификации личности.

Сравнительный анализ ряда соответствующих исследований показывает схожесть авторских подходов при рассмотрении технических аспектов цифровой идентификации. Однако аналогичной схожести подходов не наблюдается при рассмотрении правового регулирования – в исследованиях предлагаются как различные пути решения, так и выводы. Данная тенденция свидетельствует о неоднозначности и от-

сутствии полноты урегулирования общественных отношений по данному вопросу. Практически все отечественные авторы рассматривают следующие технические средства идентификации (перечислено в порядке частоты упоминаний):

- электронная подпись;
- персональные и биометрические данные;
- абонентский номер клиента – физического лица, пользующегося услугами подвижной радиотелефонной связи;
- электронные идентификационные карты (ЭИК).

А. В. Баринов в своем исследовании регулирования отношений, связанных с электронной идентификацией граждан, видит императивный подход, состоящий в приоритете «Единой системы идентификации и аутентификации» (ЕСИА), Единой биометрической системы (ЕБС) при информационном взаимодействии частных субъектов с использованием информационно-телекоммуникационной сети. И приходит к выводу, что законодательство должно обеспечивать возможность идентификации и аутентификации субъектов любыми технически возможными способами: электронной подписью; персональными и биометрическими данными; ЭИК; абонентским номером клиента – физического лица, пользующегося услугами подвижной радиотелефонной связи; совершением действий, однозначно идентифицирующих лицо и позволяющих достоверно установить его волеизъявление на совершение юридически значимых действий [1. С. 47].

А. Н. Прокопенко, А. А. Страхов считают, что необходимо в три этапа осуществить унификацию систем доступа физических лиц в государственные информационные системы. На первом этапе осуществлять идентификацию граждан во всех государственных информационных системах через портал «Госуслуги». На втором этапе максимально широко использовать в качестве идентификатора физического лица на портале «Госуслуги» усиленную квалифицированную электронную подпись. На третьем этапе применить для идентификации новую единую биометрическую систему [5. С. 79].

Академик РАЕН А. А. Фатьянов предлагает не слишком углубляться в перспективы цифровой идентификации, а на обозримое будущее ограничиться разработкой нового бланка внутреннего российского паспорта, в котором, по аналогии с паспортом, удостоверяющим нашу личность за пределами государства, будет содержаться микрочип, дублирующий текстовую запись и цифровую фотографию владельца паспорта. Информация на этом чипе должна быть гарантированно защищена от копирования неуполномоченными лицами и возможности несанкционированного изменения. Эту же информацию можно представлять в виде генерируемого чипом через специальную программу разового QR-кода, используемого для подтверждения личности при электронном взаимодействии с органами публичной власти и организациями. Этого на обозримый период времени будет вполне достаточно для решения проблемы цифровой идентификации личности [7. С. 49].

Применение к цифровой идентификации личности классической теории права и модели правового регулирования не работает, поскольку осуществить контроль отношений в виртуальной среде по аналогии реального мира значительно сложнее. Кроме того, правовое регулирование налоговых правоотношений в виртуальном

мире не ограничивается национальным законодательством и выходит на международно-правовое поле. Вместе с тем использование такого механизма правового регулирования идентификации личности, который не только отвечал бы интересам национального законодательства, но и признавался мировым сообществом, на текущем этапе международного сотрудничества трудно осуществимо. Более реальным представляется осуществить надлежащую правовую и техническую защиту цифровой идентификации личности.

Таким образом, следует согласиться с позицией Академика РАЕН А. А. Фатьянова, предложения которого в полной мере отражены в проекте Указа Президента РФ «О паспорте гражданина Российской Федерации, содержащем электронный носитель информации» (по состоянию на 19 марта 2021 г.) (подготовлен Минцифры России, ID проекта 04/14/03–21/00114294). Несмотря на приостановку проекта на неопределенный срок как по финансовым, так и по техническим причинам, разработка концепции электронного паспорта в России ведется уже около десяти лет [10], что свидетельствует о его необходимости. Представляется, что данный проект следует дополнить диспозитивной нормой (аналогично отметке об идентификационном номере налогоплательщика в бумажном бланке паспорта [4]) о «привязке» к электронному паспорту дополнительных способов идентификации и защиты информации, таких как:

- запись/перезапись усиленной квалифицированной электронной подписи (УКЭП), при этом УКЭП должна быть исключительно отчуждаемой;
- привязка абонентского номера клиента – физического лица, пользующегося услугами подвижной радиотелефонной связи;
- ведение лога юридически значимых действий (по аналогии с банковской выпиской операций по счету);
- осуществление юридически значимых действий с применением технологии блокчейн [9].

Относительно записи лога юридически значимых действий, А. В. Лисаченко справедливо отмечает, что к защите юридически значимых документов длительного хранения (например, удостоверяющих вещные права в отношении недвижимости) традиционный принцип криптографии – «Процесс расшифровки файла без ключа должен занять больше времени, чем срок актуальности содержащейся в этом файле информации» – вряд ли применим [2. С. 97]. То есть хранение электронных документов во внешней среде вне непосредственного контроля таких электронных документов самим налогоплательщиком представляется рискованным. Следует обратить внимание на фискальный накопитель онлайн-касс, в данном случае ключевая особенность которого – запись фискальных данных в некорректируемом виде (статья 1.1 № 54-ФЗ) [8]. На взгляд автора, лог юридически значимых действий, записанный в некорректируемом виде, защитит налогоплательщика от противоправных действий, направленных на искажение информации во времени. Сверка с логом юридически значимых действий, докажет факты подделки, либо искажения ранее подписанных документов, хранящихся в разного рода базах данных, на серверах, т. е. вне непосредственного контроля таких электронных документов самим налогоплательщиком. А осуществление

юридически значимых действий с применением технологии блокчейн дополнительно усилит защиту.

Проанализировав взгляды и подходы различных ученых, учитывая международный характер налоговых правоотношений, мы пришли к выводу о необходимости дальнейшего развития направления цифровой идентификации налогоплательщика, не только посредством ИНН, но и в симбиозе с цифровым паспортом гражданина Российской Федерации.

Список литературы

1. Баринов А. В. Правовое регулирование электронной идентификации граждан как основа правоотношений в информационном обществе // Ученые записки. 2021. № 3 (39). С. 47.

2. Лисаченко А. В. Идентификация субъектов гражданских правоотношений: новые проблемы и некоторые решения // Российский юридический журнал. 2019. № 5 (128). С. 97.

3. Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru/> (дата обращения: 01.05.2022).

4. Описание бланка паспорта гражданина Российской Федерации: Постановление Правительства РФ от 8 июля 1997 года № 828 «Об утверждении Положения о паспорте гражданина Российской Федерации, образца бланка и описания паспорта гражданина Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru/> (дата обращения: 06.01.2022).

5. Прокопенко А. Н., Страхов А. А. Проблемы административно-правового регулирования идентификации граждан при доступе в государственные информационные ресурсы // Вестник Белгородского юридического института МВД России имени И. Д. Путилина. – 2021. – № 2. – С. 79.

6. Соглашение о взаимодействии между Министерством внутренних дел Российской Федерации и Федеральной налоговой службой: Совместный приказ МВД России № 1/8656, ФНС России № ММВ-27-4/11 от 13.10.2010. Доступ из справ.-правовой системы «КонсультантПлюс».

7. Фатьянов А. А. Цифровая идентификация личности (некоторые юридические проблемы) // Ученые труды Российской академии адвокатуры и нотариата. 2021. № 2 (61). С. 49.

8. О применении контрольно-кассовой техники при осуществлении расчетов в Российской Федерации: Федеральный закон от 22 мая 2003 г. № 54-ФЗ (с посл. изм. и доп. от 3 июля 2018 года № 192-ФЗ) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru/> (дата обращения: 01.05.2022).

9. Fincult.info. Блокчейн: что это такое и как его используют в финансах. URL: <https://fincult.info/article/blokcheyn-chto-eto-takoe-i-kak-ego-ispolzuyut-v-finansakh/> (дата обращения: 10.02.2022).

10. Forbes. Минцифры заморозило проект электронного паспорта из-за «спецификации». URL: <https://www.forbes.ru/tekhnologii/468447-mincifry-zamorozilo-proekt-elektronnogo-pasporta-iz-za-specoperacii/> (дата обращения: 06.09.2022).

А. Н. Карпов,

аспирант,

Санкт-Петербургский государственный экономический университет

ПРОБЛЕМЫ ЦИФРОВИЗАЦИИ ПРАВА В РОССИИ

Аннотация. В современных условиях цифровизация формирует новую реальность. Цифровизацией (диджитализацией) в привычном понимании является процесс проникновения цифровых технологий во все сферы жизни общества, и прежде всего в сферу экономики, финансов и торговли. При этом любое изменение экономической модели влечет соизмеримое изменение ее правовой составляющей, а также модификацию принципов и механизмов действия гражданского права. Предметом исследования выступает право Российской Федерации в условиях технологического прогресса, геополитических и наднациональных угроз (пандемии, санкций и т. д.) и его перспективы развития. Цель – исследовать текущее состояние права в части применения цифровых механизмов и в целом влияние цифровизации на различные отрасли права, выявить проблемы и дать соответствующие рекомендации.

Ключевые слова: цифровые технологии, право, персональные данные, цифровая подпись, документооборот, click-wrap соглашения, единая биометрическая система

PROBLEMS OF DIGITALIZATION OF LAW IN RUSSIA

Abstract. In modern conditions, digitalization forms a new reality. Digitalization (digitalization) in the usual sense is the process of penetration of digital technologies into all spheres of society and, above all, into the spheres of economics, finance and trade. At the same time, it should be noted that any change in the economic model entails a commensurate change in its legal component, as well as a modification of the principles and mechanisms of civil law. The subject of this study is the law of the Russian Federation in the context of technological progress and various types of geopolitical and supranational threats (pandemics, sanctions, etc.) and its prospects for development. The purpose is to investigate the current state of law in terms of the use of digital mechanisms and, in general, the impact of digitalization on various branches of law, identify problems and make appropriate recommendations.

Keywords: Digital technologies, Law, Personal data, Digital signature, Document management, Click-wrap agreements, Unified biometric system

В России важным нормативным правовым актом в области регламентации и определения направления развития права в части диджитализации можно назвать распоряжение Правительства Российской Федерации от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации». Основопологающими мерами для развития экономики страны в части ее цифровой составляющей, с точки зрения государства, являются:

– создание независимых правовых институтов, которые позволят решить основополагающие задачи становления цифровой экономики;

- снятие основных правовых барьеров для развития цифровой экономики;
- мотивация и поощрение экономической деятельности субъектов, использующих современные технологии, в том числе в области больших данных;
- развитие цельного законодательства, относящегося и развивающего цифровую экономику.

Что касается практического применения государственными органами современных технологий, то в данном случае позитивное влияние оказала пандемия COVID-19. Так, в разгар коронавирусной инфекции начиная с 2020 г. суды активно практиковали дистанционные судебные заседания. Законодательство в указанной сфере, с задержкой практического применения, было разработано и принято лишь в конце 2021 г. (Федеральный закон от 30.12.2021 № 440-ФЗ). В рамках указанного закона участникам спора предоставлена возможность подавать документы в суд с помощью портала Госуслуг и получать судебные извещения. При наличии технической возможности стороны судебного разбирательства могут получить доступ к материалам дела в цифровой форме, а также принимать участие в заседании с помощью мобильных и портативных средств связи.

В части взаимосвязи договорного права и цифровизации важными источниками права, регулирующими договорные отношения с применением цифровых технологий, являются ст. 141.1 ГК РФ, Федеральный закон от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации», Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

При этом цифровизация не ограничивается сферой государственных услуг, она также актуальна для гражданских и договорных правоотношений.

Новые цифровые сервисы порождают новые возможности, что в свою очередь совершенствует функционирование документооборота. Оперативность взаимодействия сторон правоотношений приводит к появлению новых способов заключения сделок. Так, введение биометрической и цифровой подписи в электронный документооборот участников гражданского оборота позволило заключать договор в электронной форме, что, безусловно, увеличивает скорость как заключения, так и исполнения договора сторонами [1. С. 39–46].

Для получения квалифицированной электронной подписи (КЭП) и сертификата ключа проверки электронной подписи удостоверяющий центр должен идентифицировать клиента. Раньше существовал только один способ сделать это – проверить паспорт при личном визите заявителя в удостоверяющий центр. В соответствии с ФЗ от 27.12.2019 № 476-ФЗ появился новый способ юридически значимой проверки личности – идентификация в Единой биометрической системе. Такая проверка проводится онлайн и занимает несколько секунд. Квалифицированная электронная подпись, полученная по биометрии, ничем не отличается от подписи, полученной традиционным способом – лично в удостоверяющем центре. Так, банки начали активно использовать удаленную идентификацию новых клиентов через Единую биометрическую систему (ЕБС). Благодаря этому оформить потребительский кредит, открыть счет или оформить ипотеку можно будет без посещения офиса.

Также наблюдается рост объемов электронной торговли на различного рода интернет-площадках. В процессе использования электронной площадки покупатель совершает конклюдентное действие, акцептуя оферту с соответствующими условиями с помощью клика. Данный способ соглашения сторон в интернет-магазинах можно назвать как *click-wrap* соглашения.

В российском праве данные соглашения не получили своего освещения в законодательстве, поэтому можем обратиться к зарубежной научной литературе. Так, в США *click-wrap*-соглашение определяется как соглашение, которое заключается участниками гражданских правоотношений в сети Интернет и в котором оговорены права и обязанности участников сделки [4].

Данное соглашение используется для определения условий поставки и купли-продажи товара в онлайн-среде, а также вопросы инсталляции программного обеспечения (при необходимости) и условия пользовательского соглашения. С учетом оперативности взаимодействия сторон сделки можно с уверенностью сказать, что *click-wrap*-соглашения являются оптимальным способом ведения переговоров и заключения сделок между сторонами онлайн.

Таким образом, *click-wrap*-соглашения по своей сути являются способом заключения договора в электронном виде, в котором сторона выражает волеизъявление посредством осуществления конклюдентных действий в рамках п. 3 ст. 434 и п. 3 ст. 438 ГК РФ.

На основании вышеуказанного исследования можно сделать вывод о том, что в России довольно успешно внедряются и применяются цифровые технологии, как в сфере публичного права, так и в сфере предпринимательских правоотношений. При этом хотелось бы выделить некоторые проблемные вопросы. Одним из них является доступность цифровых инструментов и доступность сети «Интернет». Так, по состоянию на 2021 г., по данным Росстата, в городах доступ к Интернету отсутствует у 24 % домохозяйств, а в сельских населенных пунктах – у 43,5 % [2]. Также у части жителей страны отсутствуют знания для использования множества различных, специализированных платформ в сети. В данном случае задачей государства является проведение соответствующего обучения и обеспечения доступа к Интернету в любой точке страны. В противном случае стороны спора или участники гражданских правоотношений будут находиться в неравных условиях (возможность ознакомления с материалами дела, подача ходатайств, заключение договоров и т. д.).

С учетом разрозненных источников права в части цифровизации права считаю возможным начать формирование и выделение из гражданского права цифрового права. Учитывая колоссальный потенциал цифрового права и его текущее зачаточное состояние, выделение цифрового права в отдельную отрасль права позволит проводить более планомерное его развитие и систематизацию.

Также важнейшей проблемой в области интернета вещей, который представляет собой набор устройств, взаимодействующий совместно с сетью «Интернет» и упрощающий бытовые процессы, является бесконтрольный и неограниченный сбор информации. Речь идет об утечках персональных данных, а также банковских реквизитов. Ответственность в России за данные правонарушения является недостаточной, о чем свидетельствует пример с сервисом «Яндекс.Еда» – в течение

2022 г. (апрель и август) компания была оштрафована за утечку персональных данных пользователей (телефоны, адреса, имена и т. д.), при этом сумма штрафа в пересчете на одного пользователя составила 1 рубль [3]. Подобная ответственность является недостаточной и не мотивирует компании и участников рынка использовать надлежащие механизмы и способы для защиты персональных данных граждан.

Список литературы

1. Пучков О. А. Трансформация договорного права в условиях информационных технологий: новые тенденции // Правовое государство: теория и практика. 2019. № 2. С. 39–46.
2. Росстат: почти треть домохозяйств не имеет доступа к интернету // Коммерсантъ (kommersant.ru). URL: www.kommersant.ru/doc/4900915?ysclid=17q4f9k8qi333549832 (дата обращения: 14.09.2022).
3. «Яндекс.Еду» повторно оштрафовали на 60 тыс. руб. за утечку персональных данных // Коммерсантъ (kommersant.ru). URL: <https://www.kommersant.ru/doc/5492583> (дата обращения: 14.09.2022).
4. Buono F. M., Friedman J. A. (1999). Maximizing the Enforceability of Click-Wrap Agreements // Journal of Technology Law & Policy: Vol. 4: Iss. 3, Article 4 (<https://scholarship.law.ufl.edu/jtlp/vol4/iss3/4>)

Ф. Х. Каюмова,

Ташкентский государственный юридический университет

ЗАЩИТА ЛИЧНОЙ ИНФОРМАЦИИ В ЦИФРОВУЮ ЭПОХУ

Аннотация. В статье рассматриваются семейные и персональные данные, принадлежащие физическому лицу в условиях современного процесса цифровизации, их защита и сохранение в соответствии с национальным и зарубежным законодательством, а также возникающие в связи с этим вопросы владения и контроля данной информацией как одних из наиболее важных.

Ключевые слова: информация, персональные данные, конфиденциальность, цифровые технологии, информационная система

PROTECTING PERSONAL INFORMATION IN THE DIGITAL AGE

Abstract. This article examines family and personal data belonging to an individual in the conditions of the modern process of digitalization, their protection and preservation in accordance with the law, the basics of personal data protection in foreign countries and national legislation, and also analyzes the fact that each person owns them, that the ability to control the desired data becomes one of the most important issues.

Keywords: Information, Personal data, Confidentiality, Digital technologies, Information system

Введение. Сегодня мы живем в быстро развивающемся информационном веке, и нам необходимо уделять больше внимания, чем когда-либо, защите личной информации от информационных атак, ее защите и недопущению использования ее в различных злонамеренных целях. Развитие информационных технологий вместе с возрастающей ценностью информации для людей также является причиной растущей озабоченности по поводу управления конфиденциальностью личной информации. По мере роста этих опасений людям становится все труднее управлять и контролировать свою личную информацию. Международно-правовые документы и национальное законодательство предусматривают право на поиск, хранение, распространение и использование любой информации, что еще больше усложняет вопрос. Если принять во внимание растущий интерес к глобализации информационных систем, то можно увидеть, что в этом отношении проводились различные исследования и возрастает потребность в разработке определенных механизмов. В частности, исследования, проводимые по вопросам защиты информации, изначально ограничивались разработкой механизма регулирования. Однако внешним факторам, влияющим на этот механизм, уделялось мало внимания.

В результате одновременно в разных странах возникали различные проблемы, связанные с конфиденциальностью данных. А. Вестин также пришел к выводу, что разные аспекты конфиденциальности данных могут по-разному восприниматься в разных странах.

Анализ и методы литературы. В данной статье рассмотрена необходимость защиты персональных данных в условиях современной цифровизации, правовые основы защиты персональных данных в зарубежных странах, а также в законодательстве Узбекистана, в частности Закон «Персональные данные достоверны», принятый на 2 июня 2017 г. Обсуждаются содержание и сущность закона, государственная защита персональных данных и их гарантия.

В данной исследовательской работе использовались методы анализа, статистики и обобщения научных знаний.

Обсуждение и результаты. Поскольку человек участвует в различных аспектах жизни общества, он обязан использовать свою личную информацию в своих социальных отношениях с другими. Например, происходит обмен информацией между работодателем и работником, врачом и пациентом, работником банка и клиентом. Такой обмен информацией признается нормальным. Однако нетрудно заметить, что развитие информационных и коммуникационных технологий стремительно превращает персональные данные в объект всех сфер, необходимо определить их строгий охват по типу. Следует отметить, что личная и семейная информация людей, информация, связанная с их статусом, репутацией и ценностью, и раньше охранялась государством. Мы не можем оценивать это явление только по развитию информационных систем. Причина в том, что ранее был разработан ряд нормативных правовых документов о персональных данных. Примеры таких документов включают:

- Европейская конвенция «О защите физических лиц при автоматизированной обработке персональных данных»;
- Директива о защите данных, принятая Европейским сообществом;
- «Рекомендации по защите частной жизни в Интернете», принятые Комитетом министров государств-членов Совета Европы; В Германии действу-

ют законы «О защите граждан от других граждан» и «О распоряжении личной информацией».

Обеспечение правовых основ защиты персональных данных и системы защиты информации еще больше расширяет гарантии безопасности. В связи с тем, что интернет-сети все больше влияют на социальную и экономическую сферы, важность защиты данных была признана почти всеми странами посредством юридических документов, международных соглашений и взаимных соглашений, подписанных странами. Во многих странах созданы правовые рамки не только для информационной системы, но и для защиты общих и персональных данных, связанных с защитой персональных данных других стран. Если мы посмотрим на статистику, то 137 из 194 развитых стран разработали законы о защите права на данные и неприкосновенность частной жизни. Такие законы приняты в 57 % стран Азии и Африки. В настоящее время одним из ведущих регионов с точки зрения защиты данных является Европейский регион. Принятие законов о персональных данных в Европе защищает граждан каждого государства-члена Европейского Союза от нарушений их права на информацию. Если мы посмотрим на страну США, то можем привести пример федеральных законов с общей защитой и специальных законов некоторых штатов. На сегодняшний день в Бразилии разработано более 40 документов с публичными и личными данными. В 2020 г. Всекитайское собрание народных представителей обнародовало законопроект о защите персональных данных, который стал важным импульсом для разработки комплексной платформы управления данными.

Кроме того, эффективность работы, направленной на правовую защиту персональных данных Российской Федерацией, свидетельствует о повышенном внимании к этому вопросу. В связи с развитием системы «Электронное правительство» в Республике Узбекистан большое внимание уделялось правовой защите права граждан на неприкосновенность частной жизни, личную и семейную тайну. В настоящее время практически никто не может участвовать в общественных отношениях без использования информационных технологий, не имея возможности использовать свои персональные данные в той или иной деятельности. Кроме того, невозможно сохранить личные данные во времени и пространстве. Поскольку наша страна постепенно переходит в среду цифровизации всех отраслей, большое значение имеют законы о персональных данных, которые становятся объектом информационной системы. Одним из важнейших документов, направленных на защиту персональных данных в нашей стране, является Закон «О персональных данных», принятый 2 июня 2019 г. Принятие этого закона было абсолютно необходимо. Причина в том, что в эпоху развития информационных и коммуникационных технологий увеличилось количество случаев неправомерного использования и распространения информации, относящейся к частной информации граждан, включая фотографии, сообщения и переписку, телефонные разговоры. Закон создал правовую основу для сбора, распространения, хранения и использования личной информации как оптимального решения.

Закон «О персональных данных» предусматривает соблюдение прав и свобод человека и гражданина, законность целей и способов обработки персональных данных, достоверность и достоверность персональных данных, их конфиденциаль-

ность и защиту, безопасность общества и состояние определяется как основные принципы. В качестве основных задач усилены защита частной информации граждан с помощью правовых и организационных мер через механизмы защиты персональных данных, предотвращение вмешательства в личную жизнь, соблюдение их неприкосновенности и конфиденциальности, предотвращение неправомерной обработки персональных данных. Кроме того, законом устанавливаются государственный контроль за предоставлением и использованием персональных данных третьим лицам, меры ответственности за неправомерное использование персональных данных других лиц.

Создание уполномоченного органа по персональным данным в Узбекистане свидетельствует о расширении масштабов реформ в этом отношении. Государственный центр персонализации при правительстве является компетентным органом в этой области. Эта организация гарантирует защиту личной информации и предотвращение разглашения и распространения информации без согласия физических лиц. В нашей стране закон служит правовой гарантией права на неприкосновенность частной жизни, предотвращение произвольного вмешательства в семейную и личную информацию граждан. Если обратить внимание на существование законов, разработанных большинством стран, то сбор, хранение и использование персональных данных разрешается в случаях, предусмотренных законом, в частности в общественных интересах и для обеспечения прав личности и ее установлено, что это должно быть сделано с согласия лица. Потому что использование персональных данных без разрешения человека может негативно сказаться на праве на неприкосновенность частной жизни, положении, репутации и карьере в общественной жизни. В связи с этим данное правило определено во многих принятых правовых документах по защите персональных данных.

Выводы и предложения. Поскольку мы живем в эпоху передовых цифровых технологий, мы видели выше, что защита персональных данных становится все более важной. Потому что защита прав и интересов более заметна в защите неприкосновенности частной жизни, которая является одним из важнейших прав человека, от различных информационных атак. В связи с этим защита персональных данных, недопущение их использования в различных злоумышленных целях, недопущение использования персональных данных способом и в форме, противоречащей воле человека, становится как никогда актуальной. Развитие информационных технологий увеличивает потребность в защите конфиденциальности. Также расширяющиеся возможности спутников позволяют следить за жизнью человека из любой точки мира. Это, опять же, требует усиления мер защиты конфиденциальности.

Список литературы

1. Конституция Республики Узбекистан. – Ташкент: Узбекистан, 2018. – 28 с.
2. Астанов И., Сафаров Дж., Базаров Д. Конституция Республики Узбекистан и Всеобщая декларация прав человека. – Ташкент: ТДЮ, 2011. – 77 с.
3. Якубова И. Гражданско-правовая защита прав личной собственности в законодательстве Узбекистана и Японии: дис. – Ташкент: 2018. – 179 с.

В. Б. Киракосов,

студент,

Южный федеральный университет

КРИПТОВАЛЮТА: ОПЫТ ПРАВОВОГО РЕГУЛИРОВАНИЯ В РОССИИ И ЗАРУБЕЖНЫХ ГОСУДАРСТВАХ

Аннотация. В статье рассматриваются основные подходы зарубежных государств к правовому регулированию обращения криптовалюты. Целью исследования является определение наиболее благоприятной модели правового регулирования криптовалюты в России на основе опыта иностранных государств. Приводится опыт правового регулирования названного объекта в Великобритании, Японии, Китае и США. Сделаны выводы о недостаточности современного правового регулирования криптовалюты в России, отмечены ключевые положительные и отрицательные черты правового регулирования криптовалюты в вышеупомянутых государствах.

Ключевые слова: криптовалюта, цифровые права, цифровая валюта, цифровая экономика, цифровые технологии, электронное средство платежа, безналичные денежные средства.

CRYPTOCURRENCY: EXPERIENCE OF LEGAL REGULATION IN RUSSIA AND FOREIGN STATES

Abstract. This article reviews the main approaches of foreign countries to the legal regulation of cryptocurrency circulation. The purpose of the study is to determine the most favorable model of legal regulation of cryptocurrency in Russia on the basis of the experience of foreign states. The author examines the legal regulations in the UK, Japan, China, and the USA. The conclusions about the insufficiency of the current legal regulation of cryptocurrency in Russia are made. Furthermore, the key positive and negative features of the legal regulation of cryptocurrency in these states are noted.

Keywords: Cryptocurrency, Digital rights, Digital currency, Digital economy, Digital technology, Electronic means of payment, Non-cash funds

Темпы развития общества и науки на современном этапе порождают появление невиданных до настоящего времени технологий. Процесс глобализации, который предполагает стирание государственных границ и развитие трансграничности, влияет и на мировую экономику. Разумеется, цифровые технологии облегчают человеческую жизнь, но это лишь один аспект их появления и функционирования, другим же являются вопросы принадлежности, оборотоспособности и безопасности. Технологии развиваются слишком стремительно, благодаря им возникают новые общественные отношения, и вне зависимости от их характера возникает необходимость их урегулировать. Одним из таких проявлений научно-технического прогресса является развитие криптовалюты – нового и потенциально востребованного финансового актива, «обладающего рядом исключительных свойств при стремительно меняющемся товарно-денежном обороте» [1. С. 51].

Криптовалюта получает особенное развитие на фоне падения доверия к государственным банкам в связи с экономическим кризисом, нестабильным курсом валют. Это порождает развитие криптовалюты в различных качествах, начиная от особого имущества, заканчивая средством обмена и накопления. Данный факт повышает интерес как с частной, так и с публичной стороны, что напрямую подтверждает актуальность выбранной темы исследования и необходимость более углубленного изучения.

Представляется, что в целом правовое регулирование цифровых прав и цифровых объектов, а не только лишь криптовалюты, предложенное российским законодателем в настоящее время, не является исчерпывающим и не в полной мере соответствует потенциалу современных технологий. Разумеется, законодатель «адаптируется к условиям широкого использования цифровых технологий» [3. С. 43], однако темпы их развития многократно опережают развитие правового регулирования в этой сфере.

Гражданский кодекс РФ с 2019 г. признает имущественную природу цифровых прав, перечисляя их в составе имущественных (ст. 128 ГК РФ). Исходя из понимания цифровых прав как объектов гражданских прав, следует то, что на них распространяются также и положения ст. 129 Гражданского кодекса РФ, регулиющей оборотоспособность объектов. Так, цифровые права, как и любые объекты гражданских прав, могут отчуждаться, переходить от одного лица к другому в порядке универсального правопреемства либо иным способом, если они не ограничены в обороте.

Дальнейшее раскрытие понятие «цифровые права» получает в ст. 141.1 Гражданского кодекса РФ. Под цифровыми правами законодатель понимает «названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам» [2]. Цифровые права имеют и научную классификацию, предложенную С. В. Решетняком:

- цифровое (виртуальное) имущество;
- цифровые активы;
- смарт-контракты;
- цифровые услуги [6. С. 96–97].

Стоит отметить, что указанное понятие является необычайно широким, так как, по сути, под такое определение может подпадать абсолютно любое право, которое в том или ином виде фиксируется в цифровом виде. Тем не менее формулировки, «названные в таком качестве в законе» и «отвечающие установленным законом признакам», позволяют сделать вывод о том, что признание определенного права цифровым произойдет вследствие прямого указания законодателя, т. е. подлежит уточнению. Несмотря на наличие хорошего инструмента для планомерного и контролируемого процесса правового регулирования цифровых технологий, Россия далеко не является лидером в этом векторе развития права.

То или иное право может быть названо цифровым непосредственно в тексте закона, учитывающего признаки и особенности информационной системы, в ко-

торой будут установлены правила определения и осуществления цифрового права. Законодатель идет именно по такому пути и уже постепенно закрепляет такую модель развития правового регулирования.

Например, законодатель в ст. 1 Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [5] напрямую указывает, что цифровые финансовые активы являются цифровыми правами, а также дает определение понятию «цифровая валюта», которое не признает ее денежной единицей и предполагает, что она представляет собой цифровой код или обозначение, которые лишь могут быть приняты в качестве средства платежа, но таковыми не являются.

Исходя из названного определения, можно сделать вывод о том, что законодатель под цифровой валютой понимает особый вид имущества, объект гражданских правоотношений. Однако непосредственно о криптовалюте в данном случае речи не идет, законодатель ее не упоминает напрямую.

Правовое регулирование криптовалюты в России – один из основных проблемных вопросов, так как с момента ее появления неоднократно высказывалась позиция о недопустимости и нелегитимности использования, оборотоспособности криптовалюты. Изначальная позиция Центрального Банка России сводилась к пониманию криптовалюты в качестве денежного суррогата, выпуск которого на территории Российской Федерации запрещен Федеральным законом от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» [4]. Тем не менее такая позиция мегарегулятора не отразилась на повсеместном и возрастающем распространении криптовалюты, что потребовало очередной реакции от органов власти. Тогда позиция Центрального банка России изменилась, отразившись на понимании криптовалюты уже не как денежного суррогата, а как особого объекта цифровых прав [7. С. 229].

Сегодня нам известно, что законодатель слишком широко определяет понятие цифровых прав, что не позволяет с достаточной уверенностью утверждать о легитимности использования криптовалюты на территории России.

На данный момент единственным продвижением в правовом регулировании криптовалют является принятие уже упомянутого Федерального закона № 259, который не определяет криптовалюту, не содержит никакой информации относительно налогообложения, не содержит возможных изменений к тексту Гражданского кодекса РФ, а скорее является лишь «переходным» этапом к признанию криптовалюты.

Одновременно с этим ужесточилась и позиция Центрального Банка России, который хотел вовсе запретить выпуск, обмен и обращение криптовалюты на территории Российской Федерации, так как уклонение от налогов, «финансирование преступной деятельности» (по мнению, Центрального Банка России) представляют собой особенный риск для курса рубля. Единственной надеждой на справедливое разрешение данного вопроса стала позиция Министерства финансов России, которое предложило необходимость не запрета, а тщательного правового регулирования криптовалюты. Обратим внимание на то, что исходя из понимания циф-

ровой валюты по смыслу Федерального закона № 259, криптовалюта (как в перспективе разновидность цифровой валюты) обладает определенными признаками: отсутствие материальной закреплённости; не является денежной единицей; признается имуществом. На этом правовое регулирование и понимание криптовалюты в России на современном этапе заканчивается.

Рассмотрим правовое регулирование криптовалюты в зарубежных правовых системах.

Достаточно интересная правовая позиция складывается в системе права Великобритании, которая признает криптовалюту имуществом [14]. Согласно правовой позиции, которую выражают Sarah Green и Ferdisha Shagg, криптовалюта и физические активы имеют много общего:

- существуют независимо от правовой системы;
- могут быть переданы;
- могут быть украдены или утеряны.

Ученые предлагают также расширить понимание владения, чтобы охватить криптовалюту, не ограничиваясь лишь материально существующими объектами. Физические, материальные активы в данном случае могут служить хорошим ориентиром с точки зрения установления нормативных требований о возникновении права собственности на криптовалюту, поскольку обоснование для присвоения правового титула на физический актив переносится в контекст цифрового. Именно такую позицию выражает Юридическая комиссия Англии и Уэльса [16], и таким образом поступает законодатель, устанавливая, что право собственности на криптовалюту возникает в тот момент, когда она депонируется на адрес электронного кошелька правообладателя. Иной точки зрения придерживается, например Hin Liu, предлагая не распространять концепцию владения на цифровые активы, а применить концепцию контроля, которая поможет определить, было ли изначально приобретено право собственности на криптовалюту [17]. Высказанная концепция предполагает наличие двух уровней контроля над активом:

- *positive control* представляет собой такой набор правомочий собственника криптовалюты, который позволяет передать его другому субъекту, а также иметь какие-либо преимущества в связи с обладанием ей. В качестве примера приводится выкуп монеты другой криптовалюты, отличной от той, которая содержится на электронном кошельке собственника через смарт-контракт;

- *negative control* представляет собой набор правомочий иного уровня, как например, право исключения какого-либо лица из доступа к электронному кошельку, право запрета на передачу криптовалюты в отношении какого-либо лица. Данный вид является наивысшей степенью контроля над активом [22].

Английский законодатель исходит из единого понимания цифрового актива и криптовалюты, понимая под ними также и транзакционные возможности в отношении цифровой записи [12]. Иначе говоря, это исключительно контролируемый актив, находящийся на электронной записи, которая независима от правовой системы и отчуждаема. Стоит сказать о том, что англосаксонское право, действительно, намного преуспевает в вопросах правового регулирования цифровых финансовых активов и криптовалют, нежели российская правовая система. Там на высоком уровне сформулированы основные положения относительно криптова-

лют, а также сформирована точка зрения различных ученых, возникают активные дискуссии относительно необходимого правового режима, в то время как в российском научном сообществе единственной существенной дискуссией относительно цифровых активов и криптовалют является разрешение вопроса о запрете или регулировании рассмотренных объектов.

Тем не менее представляется, что полностью перенять опыт Англии в указанной сфере невозможно. Названные правовые режимы чужды для российского права: хоть криптовалюта и признается имуществом, но на нее распространяется особый расширенный правовой режим владения либо контроля. Представляется, что российскому законодателю необходимо избрать для криптовалюты существующий в отечественной правовой системе режим.

Не секрет, что сторонником использования криптовалюты в качестве законного средства платежа является Япония, которая признает криптовалюту иностранной валютой с 2017 г. В законе «О платежных услугах», который принят в 2017 г., криптовалюта определяется как стоимость имущества, используемая как средство оплаты покупки, которое передается через электронную систему обработки данных [9].

Развитие правового регулирования криптовалюты в Японии является хорошим примером быстрого реагирования на стремительно изменяющиеся правовые отношения. Операторы криптовалютных бирж наделены определенным правовым статусом и подлежат обязательной регистрации в Агентстве финансовых услуг Японии. Само Агентство, в свою очередь, наделено полномочиями по надзору и проверке операций с использованием криптовалюты, а также по применению административных мер.

Японский подход к пониманию криптовалюты отличается дифференцированностью, что представляется обоснованным. Например, лишь две криптовалюты из существующих признаны законным платежным средством – Bitcoin и Ethereum, их используют в розничных магазинах как средство оплаты. Иные криптовалюты законным платежным средством не являются, но они признаются ценностью определенного вида, подобной активам, который приобретает статус средства обмена.

Кроме того, законодателем был официально закреплён принцип KYC – know your customer (знай своего клиента), который применяется к организациям, осуществляющим операции с криптовалютой. Данный принцип является основным механизмом противодействия финансированию терроризма и отмыванию доходов.

Стоит сказать, что японская модель правового регулирования режима криптовалюты может быть признана вполне удачной. Главным преимуществом данной модели является применение подхода дифференциации криптовалют, чего нет, например, в Соединенных Штатах Америки, которые будут рассмотрены нами далее. Японская модель также успешно применяет инструмент по противодействию преступным посягательствам с криптовалютой.

Достаточно интересным представляется также правовое регулирование криптовалюты в Китае.

Известно, что в Китае успешно развивается одна из самых сильных экономических систем и это является одним из факторов необходимости правового ре-

гулирования криптовалюты. Первоначально Китай совершал попытки правового регулирования цифровой валюты Q-Coin, которая возникла из онлайн-видеоигр и успешно перешла в гражданский оборот, но позже был издан полный запрет на использование цифровых валют в связи с высоким ростом популярности и угрозой экономики, а также курсу внутригосударственной валюты. Биткоин, как одна из наиболее развитых и сильных криптовалют, также оставался вне правового регулирования, транзакции с его использованием обрабатывались нелегально через негосударственные финансовые учреждения и третьих лиц [18].

Китайский банк не предоставляет биткоину и иным криптовалютам никакого юридического статуса и отказывается признавать использование биткоина в качестве валюты. Обратим внимание на то, что до такого жесткого запрета на долю Китая приходилось большинство бирж криптовалюты и биткоина, а после запрета их количество значительно сократилось и составило 7 % [18]. По мнению многих ученых такая политика Китая заставляет его отставать от других юрисдикций, которые облагают криптовалюту налогом.

Тем не менее стоит обратить внимание на то, что Китайское правительство высказывает достаточно весомые доводы в пользу своей позиции, одним из которых является рост трансграничной преступности в связи с развитием рынка криптовалют, а также цель по созданию своей национальной криптовалюты. Так, в 2020 г. Сельскохозяйственным банком Китая в тестовом режиме было запущено приложение для использования национальной криптовалюты [23]. Концепция существования национальной криптовалюты позволяет установить четкий и жесткий правовой режим ее обращения:

- отслеживаемость;
- отсутствие анонимности;
- освобождение из-под влияния американского доллара;
- повышенный контроль над обращением криптовалюты.

Такая модель правового регулирования может быть принята и законодателем Российской Федерации. Тем не менее представляется, что это противоречит изначальной «крипто-философии», которая предполагает анонимность и отсутствие контролирующих органов, но такое понимание рынка криптовалют, несомненно, делает его идеальной площадкой для реализации преступных интересов – этот вопрос является таким, в котором сложно найти точки соприкосновения частных и публичных интересов. Нам кажется, что российский законодатель может перенять китайский опыт в области правового регулирования рынка криптовалют, однако устанавливать повышенный, в сравнении с иными валютами, уровень контроля необоснованно.

Рассмотрим правовое регулирование криптовалюты в Соединенных Штатах Америки.

В силу того, что в США штаты правомочны регулировать те или иные вопросы автономно и самостоятельно, там сложилось несколько основных концепций понимания криптовалюты. Разнообразных концепций и правовых режимов придерживаются не только штаты, но и различные государственные органы власти и агентства, что еще больше осложняет ситуацию с установлением надле-

жащего правового режима. Данная проблема в сочетании с тем, что абсолютно все криптовалюты вне зависимости от индивидуальных особенностей сводятся к единому режиму, привела к возникновению дублирующих, повторяющих друг друга и запутанных правовых норм, которыми должны руководствоваться эмитенты, покупатели, а также лица, содействующие покупке и продаже криптовалюты.

Рассмотрим основные позиции в доктрине и законодательстве.

1. Криптовалюта как валюта. Одним из первых регуляторов криптовалюты в США является Министерство финансов, которое действовало через Сеть по борьбе с финансовыми преступлениями (the Financial Crimes Enforcement Network, далее – FinCEN). Миссия FinCEN, в соответствии с Законом «О банковской тайне» заключается в регулировании денежного потока во избежание финансирования незаконных преступных действий, как терроризм или легализация доходов, добытых преступным путем [8]. Данная миссия реализуется посредством наложения на финансовые учреждения обязанностей по мониторингу и учету финансовых операций, а также наличия отчетности перед FinCEN.

С учетом значимости миссии FinCEN, а также того факта, что криптовалюта ранее, действительно, использовалась для финансирования терроризма и для иных преступных целей, Министерство финансов и FinCEN высказывали позицию, согласно которой к криптовалюте необходимо относиться как к виртуальным денежным средствам. Это означало бы, что все операции с криптовалютой попадали бы под юрисдикцию FinCEN, т. е. представлялось возможным установить высокий уровень контроля над оборотом криптовалюты.

В начале 2013 г. FinCEN публикует руководство, которое определяет виртуальную валюту в качестве любого средства обмена, не имеющего статуса законного платежного средства, который либо имеет эквивалентную стоимость в реальной валюте, либо действует как ее заменитель [11]. Так, любой посредник, который содействовал использованию любой виртуальной валюты, приобретал правовой статус денежного переводчика (money transmitter), одной из обязанностей которых является постоянная отчетность перед FinCEN, а также соблюдение требований о противодействии финансированию терроризма и легализации доходов.

Несмотря на то, что у FinCEN есть законные основания для надзора за любыми участвующими в таких правоотношениях субъектами, стоит признать, что данное FinCEN определение понятию «виртуальная валюта» является достаточно широким, как минимум, для достижения своих целей. Как отмечает Carol R. Goforth, криптовалюта всегда имеет стоимость в реальной валюте вне зависимости от того, была ли она предназначена для ее замены или нет, а большинство криптовалют может служить средством обмена вне зависимости от намерений правообладателя, того для чего, кому и как она передается, в то время как у традиционных валют нет другой цели, кроме как выступать в качестве средства обмена, сохранения стоимости или расчетной единицы [13].

Представляется, что вышеназванное определение являлось лишь инструментом для расширения влияния и юрисдикции FinCEN, так как оно распространяет

на посредников криптовалют новое правовое положение. Тем не менее, несмотря на явную заинтересованность FinCEN в использовании именно такого определения, банки некоторых штатов используют именно его. Например, Конференция банковских инспекторов штатов (the Conference of State Bank Supervisor), определяет виртуальную валюту в качестве цифрового представления стоимости, используемого в качестве средства обмена, расчетной единицы или средства сбережения, не имеющего статуса законного средства платежа [10].

Единый закон, разработанный, чтобы помочь штатам решить, когда законы штата о денежных переводах и правовом статусе «переводчиков» должны применяться к предприятиям, связанным с виртуальными валютами, впервые опубликован Комиссией по единообразному законодательству в 2017 г. Названный закон определяет «виртуальную валюту» как «цифровое представление стоимости, которое:

- используется в качестве средства обмена, расчетной единицы или средства сбережения;

- не является законным платежным средством» [21].

Иначе говоря, данное определение ничем не отличается от позиции FinCEN и CSBS, т. е. своей изначальной задачи, по сути, не выполняет. В связи с этим единый закон не был принят ни одним американским штатом.

Законы штатов о криптовалютах и денежном обращении применяются по-разному. Более дюжины штатов требуют получения лицензии или иной формы авторизации предприятия. Например, в Нью-Йорке требуется Bit License 9 (бизнес-лицензия на деятельность в области виртуальной валюты, которая выдается Департаментом финансовых услуг штата Нью-Йорк) для работы предприятия в качестве биржи криптовалют. Уже упомянутый Carol R. Goforth обращает внимание на географию, говоря о том, что на другом конце государства криптовалюта в принципе не признается «суверенной», а штаты, находящиеся посередине, не высказывают никаких позиций относительно правового режима криптовалюты [13].

Основная проблема рассмотренного подхода заключается в том, что организации, которые хотят вести бизнес в сфере криптовалюты, будут вынуждены вести его лишь в небольшом количестве штатов, хотя крипто-бизнес является онлайн-бизнесом. Это означает также и обязательность исполнения требований как федерального уровня, так и разнообразных локальных требований, которые могут не соотноситься между собой.

2. Криптовалюта как собственность. Данной концепции придерживается Налоговая служба США (Internal Revenue Service, далее – IRS), с 2014 г. понимающая под криптовалютой цифровое представление стоимости, которое функционирует как средство обмена, расчетная единица или средство сбережения, и к которой подлежат применению общие принципы налогообложения [15]. В данном случае необходимо обратить внимание на отсутствие указания на то, что виртуальная валюта является средством платежа вне зависимости от его законности, основной уклон уходит в сторону возможности налогообложения. Такое еще более широкое определение применяется к любой валюте и некоторым видам имущества и собственности. Основная проблема в США состоит в том, что к разным

криптовалютам избран один подход (об этом мы говорили, рассуждая о регулировании криптовалюты в Японии), и позиция IRS – не исключение, так как она не допускает различий в обращении, основываясь на предполагаемой функции актива, способе продажи или обмена, а не на материальном воплощении. По сути, термин, определение которому дал IRS, это цифровая собственность.

Соглашаясь с тем, что ко всем валютам стоит относиться одинаково, IRS не квалифицирует криптовалюту в качестве валюты в том понимании, в котором ее понимает налоговое законодательство. Обратим внимание, что позиция FinCEN сводится к тому, что криптовалюта – это валюта, а позиция IRS сводится к тому, что криптовалюта является собственностью. При такой квалификации частные лица не смогут использовать криптовалюту для создания прибыли от курсовой разницы для тех целей, которые установлены подоходным налогом США, так как доходом могут быть лишь денежные средства – такой вывод предполагает позиция IRS. Абсолютно противоположный вывод вытекает из позиции FinCEN, которая считает криптовалюту валютой, хоть и не законным средством платежа, так как на валюте можно создать прибыль от курсовой разницы. Одновременно с этим, лица участвующие в транзакциях с криптовалютой, по мнению IRS, подлежат одинаковому учету и отчетности, как и любой участник биржевой торговли.

Несмотря на общее заявление IRS о том, что криптовалюта является собственностью, сама IRS, как уже стало ясным, непоследовательна в таком понимании криптовалюты. Данный тезис в очередной раз подтверждается в 2016 г., когда IRS через Министерство юстиции США выдало повестку Coinbase, Inc., стремясь заставить их раскрыть данные клиентов, торговавших криптовалютой, чтобы персонально бороться с занижением налоговой базой по криптотранзакции. В данной ситуации IRS признает Coinbase Inc. финансовой компанией, клиенты которой торгуют специальной внутренней валютой (не собственностью), указывая это непосредственно в процессуальных документах [13].

Особенно интересным становится вопрос налогообложения криптовалюты, если идти по концепции, предложенной IRS. В данном случае IRS снова высказывает неоднозначную позицию. Вопрос заключается в следующем, является ли криптовалюта обычной собственностью или она является капиталом, который при продаже приводит к капитальному приросту или убытку. По этому поводу IRS указывает, что акции, облигации и иное инвестиционное имущество рассматривается как капитальный актив, в то время как товарно-материальные ценности и имущество таковыми не являются, что означает, что каждый отдельный налогоплательщик должен самостоятельно сделать независимое определение о том, к какому из двух вышеназванных видов он относит криптовалюту, которой он владеет. Такая позиция нам представляется излишне демократичной, необоснованной и мягкой, она потенциально порождает различное понимание одной и той же нормы права, создание разных правовых режимов для одних и тех же объектов.

Многие штаты ничего не говорят о налогообложении криптовалюты, оставляя открытым вопрос о том, как операции с их участием будут облагаться налогом. Что касается подоходного налога, есть некоторые штаты, которые специально

приняли федеральный подход и применяют его, и немногие прямо отвергли его. Большинство штатов хранят молчание или изучают этот вопрос, все еще подбирая верную модель [13].

3. Криптовалюта как товар. Комиссия по торговле товарными фьючерсами (the Commodity Futures Trading Commission, далее – CFTC) также активно участвует в дискуссии относительно правового положения криптовалюты, и, хотя определение CFTC ничем не отличается от определений, данных FinCEN и IRS, какого-либо существенного вывода относительно изучения данных определений CFTC не дает.

В 2017 г. CFTC выпускает учебник по виртуальным валютам, который очевидно опирается на подход IRS к пониманию криптовалюты. CFTC считает, что она выступает средством обмена, расчетной единицей или средством сбережения, а также действует как настоящая реальная валюта, но не имеет статуса законного средства платежа. В данном случае CFTC делает вывод, что если криптовалюта попадает под это определение, то она является товаром. Иначе говоря, из одного и того же определения уже третье федеральное агентство делает разный вывод. Это связано с тем, что сферой деятельности CFTC является товарный рынок и она изучает ситуацию с мошенничеством и манипуляциями на рынках, находящихся в ее юрисдикции (не только рынки фьючерсов и деривативов, но и спотовые рынки товаров), т. е. CFTC удобно признать криптовалюту товаром, чтобы она попала под сферу реализации полномочий CFTC.

4. Криптовалюта как ценная бумага. Концепции понимания криптовалюты как ценной бумаги придерживается Комиссия по ценным бумагам и биржам (the Securities Exchange Commission, далее – SEC). SEC является последним крупным игроком на федеральном уровне в США, когда дело доходит до регулирования криптовалюты. SEC специально приняла преобладающее определение криптовалюты, соглашаясь с тем, что это «цифровое представление стоимости, которое может быть продано в цифровом виде и функционирует как средство обмена, расчетная единица или средство сбережения» [19]. Там же отмечается, что криптовалюта может представлять и иные права. В связи с этим, SEC смотрит на то, действует ли та или иная криптовалюта как инвестиционный контракт. Такой подход называется тестом *Howey*, разработанный судебной практикой США. В данном тесте элементы инвестиционного контракта переформулированы в вопросы и, если ответ на каждый из них положительный, финансовая операция представляет собой инвестирование в ценную бумагу. Вопросы сформулированы в виде условий:

- инвестируются денежные средства;
- средства инвестируются с расчетом на прибыль;
- средства инвестируются в общее предприятие;
- ожидаемая прибыль связана с предпринимательской деятельностью третьих лиц.

По мнению SEC криптовалюта соответствует всем указанным условиям и является ценной бумагой. Важно сказать о том, что в 2020 г. позицию SEC поддержал Верховный суд США в деле SEC против Telegram [20]. Особенно интересным представляется тот факт, что Telegram ссылался на позицию CFTC, признавшей

криптовалюту биржевым товаром, однако CFTC отметила, что биржевой товар может быть ценной бумагой в один промежуток времени, но в дальнейшем утратить это положение. В качестве примера CFTC приводит цифровой актив, являющийся инвестиционным контрактом при запуске, но впоследствии становящимся обычным средством накопления или платежа, владельцы которого не полагаются на усилия других для получения прибыли.

Итак, исходя из действующего американского законодательства, криптовалюта будет одновременно рассматриваться и как валюта, и как собственность, и как товар, и как ценная бумага. Мало того, что сама криптовалюта по-разному квалифицируется каждым из федеральных агентств, так еще и операции с ними будут подлежать множеству разнообразных требований, которые не всегда совпадают между собой. Одной из самых больших проблем в данном случае является то, что даже когда каждое федеральное агентство высказывает позицию о необходимости развития цифровой экономики и цифровых прав, развитии инноваций в государстве, они все равно не прекращают одновременно регулировать одни и те же правоотношения, что делает это правовое регулирование чрезмерным.

Нам представляется, что опыт Соединенных Штатов Америки в правовом регулировании криптовалюты является примером того, каким образом нельзя подходить к разрешению этого вопроса. Ситуация осложняется не только тем, что каждое федеральное агентство, используя одинаковые определения, делает разные выводы о природе криптовалюты, но еще и тем, что многие штаты не заявляют определенной и твердой позиции относительно того или иного агентства, а некоторые принимают точку зрения каждого. Такая модель правового регулирования показывает пример чрезмерного влияния государственных органов в сферу частных правоотношений.

Полагаем необходимым, в качестве выводов к настоящему исследованию предложить возможные направления совершенствования российского законодательства:

1. Признать криптовалюту особым видом имущества, внося соответствующие изменения в ст. 128 Гражданского кодекса РФ, а также в пункт третий статьи первой от 31 июля 2019 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», определив криптовалюту одновременно и в качестве цифровой валюты. Само определение цифровой валюты представляется необходимым упростить, сформулировав его следующим образом: «Цифровая валюта, в том числе криптовалюта, представляет собой особый вид имущества в виде электронных данных, содержащихся в информационной системе, которые не являются законным платежным средством, но могут быть использованы в таком качестве для целей обмена, накопления, сбережения и инвестирования».

Из такого закрепления будет следовать, что цифровая валюта и является особым видом имущества. Такое изменение позволит установить все основные признаки, присущие криптовалюте: отсутствие материального закрепления, признание криптовалюты в качестве средства обмена, накопления, сбережения

и инвестирования, использование которого предполагает возможность обмена криптовалютой. При этом представляется необходимым разработать режим налогообложения криптовалюты, обязанность по предоставлению отчетности в Федеральную Налоговую Службу, аналогично иным видам имущества, но учитывая возможный уровень недоверия частных лиц необходимо предусмотреть льготный режим налогообложения.

Представляется логичным также разрешить применение криптовалюты при исполнении внешнеторговых сделок. Так, будет сделан первый шаг в признании криптовалюты еще и законным средством платежа, но лишь на ограниченном правовом поле.

2. Интересным с точки зрения частичной рецепции является опыт правового регулирования криптовалюты в Японии. Так, представляется возможным заимствовать систему надзора со стороны государственных финансовых учреждений, которые могут применять к оператору криптовалюты административные меры в случае наличия подозрений в финансировании терроризма и отмывании доходов. Необходимо также перенять опыт Японии в закреплении принципа know your customer, в соответствии с которым оператор криптовалют должен идентифицировать и установить личность контрагента, прежде чем проводить финансовую операцию. Закрепление такого принципа станет еще одним механизмом противодействия преступной деятельности в сфере криптовалюты.

3. Помимо развития сторонних криптовалют, представляется возможным частично пойти и по пути Китая, создав национальную криптовалюту с установлением четкого и жесткого правового режима ее обращения, который будет включать в себя отсутствие анонимности, отслеживаемость, принцип know your customer, повышенный контроль над ее обращением. В отношении иных сторонних криптовалют следует применить японскую модель правового регулирования.

Список литературы

1. Гаврилов В. Н., Рафиков Р. М. Криптовалюта как объект гражданских прав в законодательстве России и ряда зарубежных государств // Вестник экономики, права и социологии. 2019. № 1. С. 51–59.
2. Гражданский кодекс Российской Федерации (часть 1) от 30.11.1994 № 51-ФЗ // Российская газета. 1994. 8 декабря.
3. Карцхия А. А. Цифровые права и правоприменение // Мониторинг правоприменения. 2019. № 2 (31). С. 43–46.
4. О Центральном банке Российской Федерации (Банке России): Федеральный закон от 10.07.2002 № 86-ФЗ // СПС Консультант-Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_37570/ (дата обращения: 11.08.2022).
5. О цифровых финансовых активов, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ // СПС Консультант-Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 10.08.2022).
6. Решетняк С. Р. Классификация цифровых прав // Вестник экспертного совета. 2021. № 1 (24). С. 96–105.

7. Хамидуллина Э. Р. Криптовалюта как объект гражданских прав: проблемы регулирования // Актуальные проблемы права и государства в XXI веке. 2020. Т. 12, № 1. С. 229–232.
8. Bank Secrecy Act 1970. URL: <https://fraser.stlouisfed.org/title/bank-secrecy-act-1025/fulltext> (дата обращения: 16.08.2022).
9. Payment Services Act 2017. URL: <http://www.japanese-lawtranslation.go.jp/law/detail/?id=3078&vm=02&re=02> (дата обращения: 15.08.2022).
10. CSBS, State Regulatory Requirements for Virtual Currency Activities, CSBS Model Regulatory Framework, (Sept. 15, 2015). URL: <https://www.csbs.org/sites/default/files/2017-11/CSBS-Model-RegulatoryFramework%28September%2015%202015%29.pdf> (дата обращения: 16.08.2022).
11. FinCEN, Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FINA-2013-G001 (Mar. 18, 2013). URL: <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> (дата обращения: 16.08.2022).
12. Fox D. Digital assets as transactional power. – 2022. URL: <https://blogs.ed.ac.uk/private-law/2022/01/20/digital-assets-as-transactional-power/> (дата обращения: 15.08.2022).
13. Goforth C., U. S. Law: Crypto is Money, Property, a Commodity, and a Security, all at the Same Time // Journal of Financial Transformation, Forthcoming. – 2015. – October. URL: <https://ssrn.com/abstract=3272975> (дата обращения: 16.08.2022).
14. Green S. and Snagg F. Intermediated Securities and Distributed Ledger Technology in Louise Gullifer and Jennifer Payne (eds), *Intermediation and Beyond* (Hart Publishing 2019) 337.
15. IRS Virtual Currency Guidance, I.R.S. Notice 2014–21, 2014–16 I.R.B. 938 (released March 26, 2014; published April 14, 2014). URL: <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> (дата обращения: 16.08.2022).
16. Law Commission of England and Wales, ‘Electronic trade documents: Report and Bill’ (Law Com No 405, 16 March 2022), chapters 5 and 7.
17. Liu H. Title, control and possession in the digital asset world // Modern Studies in Property Law Conference 2022. – 2022 – March. URL: <https://ssrn.com/abstract=4079185> (дата обращения: 15.08.2022).
18. Ponsford M. A Comparative Analysis of Bitcoin and Other Decentralised Virtual Currencies: Legal Regulation in the People’s Republic of China, Canada, and the United States (July 24, 2015). *Hong Kong Journal of Legal Studies*, (2015) 9 HKJLS 29. URL: <https://ssrn.com/abstract=2554186> (дата обращения: 15.08.2022).
19. SEC Investor Bulletin: Initial Coin Offerings (July 25, 2017). URL: https://www.sec.gov/oiea/investor-alerts-andbulletins/ib_coinofferings (дата обращения: 17.08.2022).
20. U. S. Securities and Exchange Commission (Press Release: Telegram to Return \$ 1.2 Billion to Investors and Pay \$ 18.5 Million Penalty to Settle SEC Charges. FOR IMMEDIATE RELEASE 2020–146). URL: <https://www.sec.gov/news/press-release/2020-146>

21. ULC, Uniform Regulation of Virtual Currency Businesses Act § 102(23) (first published Oct. 9, 2017). URL: http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/URVCBA_Final_2017oct9.pdf (дата обращения: 16.08.2022).

22. Vaudry W. and Green S. Electronic trade documents: the Law Commission's provisional proposals, the MLETR, and the concept of possession. – 2021. – Pp. 631–632.

23. «Цифровой юань: новая финансовая реальность или тайное оружие Китая?» // Официальный сайт информационного агентства ТАСС. URL: <https://tass.ru/ekonomika/12218193> (дата обращения: 19.09.2022).

С. С. Кирей,

магистрант,

Московский государственный юридический
университет имени О. Е. Кутафина

ЦИФРОВЫЕ ТЕХНОЛОГИИ В ПРОЦЕДУРЕ ЗАКЛЮЧЕНИЯ СДЕЛОК И РЕГИСТРАЦИИ ПРАВ НА НЕДВИЖИМОСТЬ

Аннотация. В статье рассматриваются новейшие технологии в сфере заключения сделок и регистрации прав на недвижимость. Рассматриваются способы электронного заключения сделок и внесение данных в единый государственный реестр недвижимости. Среди прочего выделяется технология распределенного реестра (блокчейн) как одна из потенциальных систем взаимодействия между государственными органами и субъектами сделок с недвижимостью, которая на сегодняшний день уже реализована в нескольких процедурах государственной регистрации прав на недвижимость.

Ключевые слова: сделки с недвижимостью, регистрация прав на недвижимость, блокчейн, мастрчейн, госчейн, госключ, ЕГРН

DIGITAL TECHNOLOGIES IN THE PROCEDURE OF TRANSACTIONS AND REGISTRATION OF RIGHTS TO REAL ESTATE

Abstract. The article discusses the latest technologies in the field of transactions and registration of rights to real estate. The author considers the methods of electronic conclusion of transactions and entering data into the unified state register of real estate. Among other, the technology of a distributed registry (blockchain) stands out as one of the potential systems of interaction between state bodies and subjects of real estate transactions, which has already been implemented in several procedures for state registration of rights to real estate.

Keywords: Real estate transactions, Registration of rights to real estate, Blockchain, Masterchain, Goschain, Goskluch, USRRE (EGRN)

Развитие технологий в разы сократило время передачи информации, получения необходимых услуг и товаров. Ситуация в мире меняется стремительно,

что требует не только краткосрочных мер и тактического мышления, а глобального и долгосрочного понимания процессов, принятия решений, руководствуясь принципами устойчивого развития. Парадигмы нового информационного мира диктуют свои требования к механизму государственного управления: информационно-коммуникационные технологии в современной России также стали частью управленческих систем во всех отраслях и сферах государственного управления, обеспечения безопасности и правопорядка [11. С. 193–199].

Правоотношения в области сделок и регистрации прав на недвижимое имущество не являются исключением и подвергаются модернизации путем внедрения информационных технологий в процедуру заключения договоров и регистрацию прав на недвижимость.

Государственная регистрация прав обеспечивает юридическую определенность в сфере сделок с недвижимым имуществом. Презумпция достоверности и защищенности данных в Едином государственном реестре недвижимости (далее – ЕГРН) одна из составляющих такой определенности. Немаловажным аспектом на сегодняшний день являются цифровые технологии, используемые при формировании как самого ЕГРН, так и в более раннем правоустанавливающем юридическом действии – заключении сделки с недвижимостью.

В своей работе Роман Сергеевич Бевзенко высказывает точку зрения, согласно которой развитие компьютерных технологий корректирует традиционные представления о ведении реестров недвижимости. Система распределенных реестров (блокчейн) позволит создавать автономные реестры, содержащие достоверную информацию о правах на недвижимость, для администрирования которой не нужен государственный орган, либо потребность в нем является минимальной [1. С. 41–42].

На данный момент совершение сделки с недвижимостью в электронном формате предполагает два стандартных этапа:

1. Подписание договора между лицами о передаче недвижимости;
2. Регистрация сделки и права на недвижимость в Росреестре и внесение соответствующих данных в ЕГРН.

Заключение договора и передача информации в ЕГРН в электронном (дистанционном) формате на сегодняшний день технологически возможна с помощью использования усиленной квалифицированной электронной подписи.

Так, 13 августа 2019 г. вступил в силу Федеральный закон от № 286-ФЗ «О внесении изменений в Федеральный закон «О государственной регистрации недвижимости», которым была предусмотрена возможность государственной регистрации перехода, прекращения, права собственности гражданина на объект недвижимости на основании заявления, подписанного электронной подписью.

Что касается подписания договора в электронном виде, то для правомерности данной формы заключения сделки необходимо прямо прописать условие о юридической силе и равнозначности электронных подписей сторон письменной подписи на бумаге.

Как многим известно, кризис – время возможностей. И прорывным временем для цифровой трансформации в России стал период пандемии коронавируса, когда в силу введенного режима ограничения физического присутствия людей в общественных местах, возросла необходимость цифровых сервисов, в том числе в об-

ласти электронной регистрации прав на объекты недвижимости. В данный период Росреестр отметил высокий уровень подачи документов в электронном виде [12].

Уже в 2018 г. в Росреестре г. Москвы проводилось экспериментальное использование технологии блокчейн в деятельности Росреестра [9].

После разработки российской децентрализованной сети обмена и хранения информации «Мастерчейн» на базе технологий распределенных реестров блокчейн, с 1 декабря 2021 г. в России начался эксперимент по обмену данными при оформлении цифровой ипотеки между депозитарием, осуществляющим хранение электронных закладных, и Росреестром (рис. 1).

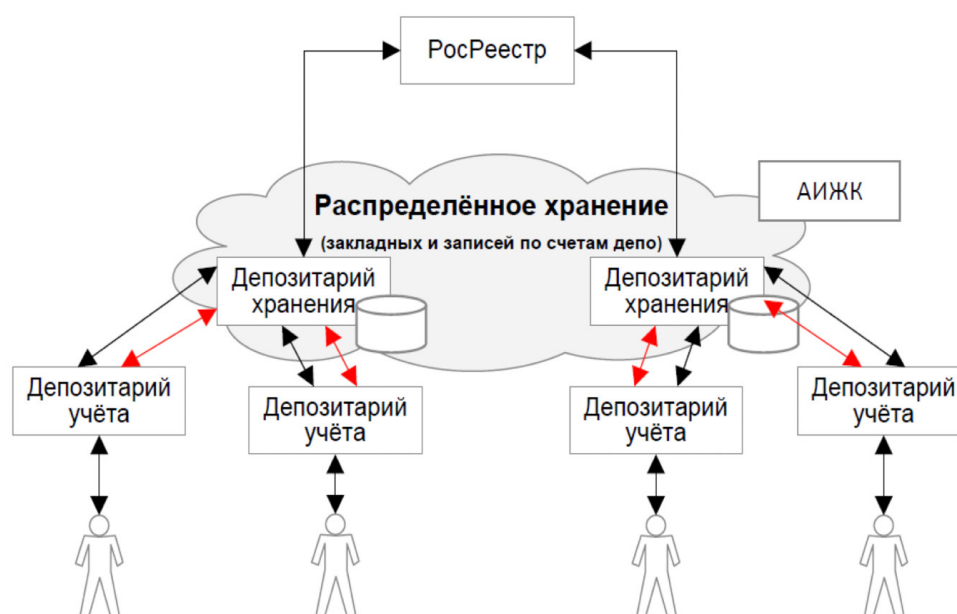


Рис. 1. Схема децентрализованной депозитарной системы для учета закладных на базе «Мастерчейн»

Сама по себе электронная ипотека существует уже с 1 июля 2018 г. [10], и с этого времени Росреестр уже обменивается данными с депозитариями и организациями, которые хранят электронные закладные. Суть указанного эксперимента состоит в использовании при таком обмене технологию распределенного реестра, что позволяет хранить данные не в централизованной базе, которая обновляется периодами и является уязвимой для атак, а у каждого участника системы в его собственной копии. Так, если какой-либо из участников внесет в базу данных новые записи, изменения автоматически появятся и у других участников. Предполагается, что использование такой технологии ускорит информационное взаимодействие между ведомством и участниками процедуры оформления закладных, так как в случае хакерской атаки, необходимо взломать сразу все копии баз данных у всех участников цепочки, что технологически весьма затруднительно на сегодняшний день [2].

В сентябре 2022 г. по предложению Минцифры России было принято решение о продолжении эксперимента до декабря 2023 г. [8]. В реализации эксперимента в на-

стоящий момент участвуют представители Минцифры России, Росреестра, «ДОМ.РФ», Центрального банка России и Ассоциации ФинТех. Уже есть определенные положительные результаты – в тестовом режиме проведена выдача первых электронных закладных с использованием технологии распределенного реестра (блокчейн).

Помимо основного эксперимента согласно проекту [8] до 1 марта 2023 г. возможно внесение предложений по расширению способов применения системы «Мастерчейн».

Таким образом, можно сделать вывод, что существует вполне вероятная возможность принятия решения об использовании технологии «Мастерчейн», основанной на технологии блокчейн, в иных сделках с недвижимостью помимо оформления цифровой ипотеки.

Стоит отметить, что при реализации названного эксперимента, помимо технологии «Мастерчейн», для обмена данными используется также единая система межведомственного электронного взаимодействия и ФГИС «Госчейн». Процесс взаимодействия между тремя технологическими составляющими данного эксперимента в перспективе позволит существенно ускорить информационный обмен между Росреестром и банками, чтобы сделать электронную ипотеку доступнее, понятнее и безопаснее для заемщиков [7].

Особое внимание стоит уделить системе «Госчейн». Согласно Постановлению № 1472 [6], «Госчейн» определяется как единая система межведомственного электронного взаимодействия и информационная система для взаимодействия Росреестра и депозитария. Нормативное положение с более подробным описанием системы «Госчейн» будет подготовлено Минцифрой в течение трех месяцев со дня окончания эксперимента, т. е. в начале 2024 г. Но уже сейчас можно предположить, что Госчейн функционально предназначено для обмена данными между федеральными органами и другими субъектами на базе технологий распределенного реестра, что в очередной раз подтверждает технологическую готовность государства к использованию блокчейна в выполнении своих функций.

Что касается новых технологий в сфере заключения сделок с недвижимостью, то здесь стоит упомянуть про сервис «Мое жилье» и приложению «Госключ».

Так, Минцифры России и Росреестр создают интернет-сервис «Мое жилье», в целях взаимодействия участников рынка на единой цифровой среде. Сервис позволит продавцам недвижимости, интернет-агрегаторам объявлений, застройщикам размещать объявления о продаже жилья на, подтверждая права на него онлайн по ЕГРН. Благодаря взаимодействию с банками и государственными органами на данном сервисе будет возможность оперативно проверить наличие обременений, информацию о зарегистрированных жильцах, наличие задолженностей по оплате ЖКУ и другую необходимую информацию для безопасной оформления сделки с недвижимостью. Также будет внедрен и функционал для покупателей недвижимости: специальный конструктор составляет электронный договор купли-продажи, ипотеки или долевого участия по разработанным Росреестром формам, а подписание документов будет возможно усиленной квалифицированной электронной подписью в мобильном приложении «Госключ».

Относительно приложения «Госключ», то эксперимент по его использованию начался в июле 2021 г. [5]. После успешного эксперимента, использование

системы «Госключ» было внедрено в формат мобильного приложения, функционал которого позволяет получить сертификат и сформировать усиленную квалифицированную или неквалифицированную электронную подпись всем, у кого есть подтвержденная учетная запись Госуслуг, загранпаспорт нового образца и смартфон с NFC-модулем [4].

Таким образом, с помощью приложения «Госключ» возможно подписывать документы, совершать сделки на Госуслугах и иных площадках, интегрированных с приложением «Госключ».

По мнению автора статьи, сервис «Мое жилье» в части заключения сделок с недвижимостью может функционировать на системе распределенного реестра (блокчейн), взаимодействуя с Росреестром по автоматическому внесению записи в ЕГРН по факту заключения сделки. Идентификация пользователей, верификация договора и направление заявления о включении сведений в ЕГРН будут осуществляться посредством приложения «Госключ».

Потенциальными достоинствами рассмотренного варианта функционирования сервиса является:

1. Сокращение времени сделки, регистрации права на недвижимость – возможность оперативного перехода прав на недвижимость;
2. Технологическая безопасность от несанкционированного взлома сервиса, включения в ЕГРН недостоверных данных;
3. Безопасность сделки для продавца и покупателя: до момента заключения договора купли-продажи стороны получают всю необходимую информацию об объекте недвижимости, дееспособности контрагента, юридическое подтверждение действительности договора и отсутствие возможности признания такого договора незаключенным в будущем.

Подводя итоги настоящей статьи, стоит сказать, что на сегодняшний день фактически существуют, а также нормативно закреплены электронные способы оформления сделок и регистрации прав на недвижимость. Как можно заметить в модернизации процедур оформления сделок с недвижимостью в условиях цифровизации большим потенциалом обладают технологии распределенного реестра. Блокчейн является надежной, прозрачной технологией, в основе которой лежит использование электронной подписи и средств криптографической защиты информации, которые требуют прохождения процедур сертификации безопасности. Экспериментальное использование технологии блокчейн в деятельности Росреестра, создание собственной децентрализованной сети обмена и хранения информации «Мастерчейн» на базе технологий распределенных реестров блокчейн, а также федеральной государственной информационной системы «Госчейн» является практическим подтверждением развития и трансформации традиционных способов юридического оформления сделок в России.

Список литературы

1. Ведение в российское право недвижимости. Вып. 3: Государственная регистрация [Электронное издание] / Р. С. Бевзенко. – Москва: М-Логос, 2021. – 210 с.
2. Взломать блокчейн. Возможно ли это? URL: <https://vc.ru/crypto/202105-vzломat-blokcheyn-vozmozhno-li-eto> (дата обращения: 01.09.2022).

3. На Госуслугах появится сервис для сделок с недвижимостью. [Электрон. текстовые данные]. URL: <https://digital.gov.ru/ru/events/41776/> (дата обращения: 01.09.2022).

4. Постановление Правительства Российской Федерации от 01.12.2021 № 2152 «Об утверждении Правил создания и использования сертификата ключа проверки усиленной неквалифицированной электронной подписи в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме». URL: <http://publication.pravo.gov.ru/Document/View/0001202112070018> (дата обращения: 01.09.2022).

5. Постановление Правительства Российской Федерации от 15.07.2021 № 1207 «О проведении эксперимента по использованию усиленной электронной подписи при предоставлении услуг и осуществлении иных действий с использованием федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме». URL: <http://publication.pravo.gov.ru/Document/View/0001202107160047?index=0&rangeSize=1> (дата обращения: 01.09.2022).

6. Постановление Правительства РФ от 02.09.2021 № 1472 «Об определении информационных систем, включенных в инфраструктуру, обеспечивающую информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг...». URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc; base=LAW; n=394499#tj96jHTGEJcSa3cl> (дата обращения: 05.09.2022).

7. Постановление Правительства РФ от 02.09.2021 № 1471 «О проведении эксперимента по апробации способа взаимодействия между депозитарием, осуществляющим хранение электронной закладной, и федеральным органом исполнительной власти, осуществляющим функции по государственной регистрации прав на недвижимое имущество и сделок с ним, с применением информационной системы «Мастерчейн», основанной на технологии распределенных реестров». URL: <http://static.government.ru/media/files/PASmQXnWbXqT5kfQvFLoAFQb7AAVu5HJ.pdf> (дата обращения: 01.09.2022).

8. Проект постановления Правительства Российской Федерации «О внесении изменений в постановление Правительства Российской Федерации от 02.09.2001 № 1471 «О проведении эксперимента по апробации способа взаимодействия между депозитарием, осуществляющим хранение электронной закладной, и федеральным органом исполнительной власти, осуществляющим функции по государственной регистрации прав на недвижимое имущество и сделок с ним, с применением информационной системы «Мастерчейн», основанной на технологии распределенных реестров»: проект постановления Правительства Российской Федерации «О внесении изменений в постановление Правительства Российской Федерации от 02.09.2001 № 1471. URL: <https://regulation.gov.ru/projects#npa=129783> (дата обращения: 01.09.2022).

9. Проект Правительства РФ «О проведении на территории Москвы эксперимента по использованию технологии «Блокчейн» в целях мониторинга достоверности сведений Единого государственного реестра недвижимости». URL: <https://regulation.gov.ru/projects#npr=74195> (дата обращения: 01.09.2022).

10. О внесении изменений в Федеральный закон «Об ипотеке (залоге недвижимости) и отдельные законодательные акты: Российской Федерации» Федеральный закон от 25.11.2017 № 328-ФЗ. URL: <https://rg.ru/documents/2017/11/28/ipoteka-dok.html> (дата обращения: 01.09.2022).

11. Холодная Е. В. О некоторых перспективах развития электронного государственного управления в условиях цифровой трансформации // Гуманитарные и юридические исследования: электронный научный журнал. – 2018. – № 4. – С. 193–199.

12. Эксперимент по обмену данными для электронной ипотеки начнется в РФ до конца года – постановление правительства. [Электрон. текстовые данные]. URL: <https://d-russia.ru/jeksperiment-po-obmenu-dannymi-dlja-jelektronnoj-ipoteki-nachnjotsja-v-rf-do-konca-goda-postanovlenie-pravitelstva.html> (дата обращения: 05.09.2022).

А. Д. Кирилова,
студент,

Вологодский государственный университет

АНАЛИЗ НАЛОГОВОГО СТИМУЛИРОВАНИЯ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Развитие экономики страны связано с постоянным и непрерывным освоением, внедрением инноваций. Наиболее неблагоприятными инвестиционными факторами для предприятия являются дороговизна инноваций, их медленная окупаемость, высокие процентные ставки по кредитам, неопределенность экономического положения в стране. В связи с этим актуальна необходимость усовершенствования инструментов налогового стимулирования научно-технической и внедренческой деятельности предприятий, что является одним из важнейших условий формирования эффективной инновационной среды. Несмотря на большое количество публикаций в области налогового стимулирования инновационной деятельности, неполно и не всесторонне изучена проблема в области разработки и обоснования комплекса мер по налоговому стимулированию инновационной деятельности предприятий. Вышесказанное говорит о том, что есть необходимость углубленного рассмотрения для дальнейшего совершенствования и развития. Целью исследования является анализ налогового стимулирования инновационной деятельности. Для достижения вышеуказанной цели выделены следующие задачи: анализ текущего состояния налогового стимулирования инновационных организаций в России и за рубежом, разработка предложений по усовершенствованию налогового стимулирования инновационных организаций России, позволяющие создать благоприят-

ные условия для инновационной деятельности, что повысит показатели России на мировом рынке.

Ключевые слова: налоговые льготы, налоговые преференции, инвестиционный налоговый кредит, ускоренная амортизация, специальные налоговые режимы, налоговые освобождения, налоговые вычеты, патентное окно.

ANALYSIS OF TAX INCENTIVES FOR INNOVATION

Abstract. The development of the country's economy is connected with the constant and continuous development and introduction of innovations. The most unfavorable investment factors for the enterprise are the high cost of innovations, their slow payback, high interest rates on loans, uncertainty of the economic situation in the country. In this regard, there is an urgent need to improve the tools of tax incentives for scientific, technical and innovation activities of enterprises, which is one of the most important conditions for the formation of an effective innovation environment. Despite a large number of publications in the field of tax incentives for innovation, the problem of developing and justifying a set of measures for tax stimulus for innovative activities of enterprises has not been fully and comprehensively studied. The above suggests that there is a need for in-depth consideration for further improvement and development. The purpose of the study is to analyze the tax stimulation of innovation activity. To achieve the above goal, the following tasks were identified: analysis of the current state of tax incentives of innovative organizations in Russia and abroad; development of proposals for improving tax incentives for innovative organizations in Russia, allowing to create favorable conditions for innovation, which will increase Russia's performance on the world market.

Keywords: Tax benefits, Tax preferences, Investment tax credit, Accelerated depreciation, Special tax regimes, Tax exemptions, Tax deductions, Patent window

Введение. В условиях «четвертой промышленной революции» активно возрастает роль инноваций, выходит на первый план. Для привлечения инвестиций и развития интеллектуального капитала существует совокупность механизмов налогового стимулирования. Данные механизмы требуют усовершенствования.

Основная часть. Налоговое стимулирование инновационной деятельности в России развивается с 2007 г. Рассмотрим методы налогового стимулирования, к ним относятся налоговые льготы и преференции. Вышеперечисленные методы ведут к снижению уровня налоговой нагрузки для определенной группы налогоплательщиков.

В ст. 56 Налогового кодекса Российской Федерации (далее – НК РФ) закреплено понятие налоговой льготы, это предоставляемые отдельным категориям налогоплательщиков и плательщиков сборов предусмотренные законодательством о налогах и сборах преимущества по сравнению с другими налогоплательщиками или плательщиками сборов, в том числе возможность не уплачивать налог или сбор либо уплачивать их в меньшем размере.

Налоговая льгота является необязательной, штраф за неприменение не взимается, срок отмены или окончания действия возможен в любой момент [1. С. 8].

Определение государственной или муниципальной преференции законодательно предусмотрено п. 20 ст. 4 Федерального закона от 26 июля

2006 г. № 135-ФЗ «О защите конкуренции», это предоставление федеральными органами исполнительной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, иными осуществляющими функции указанных органов органами или организациями отдельным хозяйствующим субъектам преимущества, обеспечивающие им более выгодные условия деятельности, путем передачи государственного или муниципального имущества, иных объектов гражданских прав либо путем предоставления имущественных льгот, государственных или муниципальных гарантий.

Налоговая преференция считается обязательной, за неприменение ее взимается штраф, срок отмены или окончания действия не раньше начала следующего налогового периода [1. С. 8].

Рассмотрев понятийный аппарат налоговой льготы и преференции, остаются размытыми их границы, это приводит к выводу о закреплении этих понятий в нормативно правовом акте.

В России существует классификация налоговых льгот по трем направлениям: Основные льготы по налогам для налогоплательщиков, осуществляющих инновационную деятельность.

Льготы по налогу на добавленную стоимость (НДС):

- НДС не подлежит налогообложению налогоплательщикам, выполняющих научно-исследовательские и опытно-конструкторские работы (далее – НИОКР);

- налогоплательщики не облагаются НДС, при реализации исключительных прав на изобретения, секретов производства (ноу-хау), полезные модели, промышленные образцы, программы для ЭВМ и базы данных, топологии интегральных микросхем, использование результатов интеллектуальной деятельности на основании лицензионного договора или коммерческой концессии;

- НДС не подлежит налогообложению налогоплательщикам, импортирующим на территорию России технологическое оборудование, в том числе комплектующие, запасные части к нему, аналоги которого в РФ не производятся.

1.2. Льготы по налогу на прибыль:

- в НК РФ введены льготы на амортизацию основных средств, используемых в научно-технической деятельности, организации обладают правом использовать специальный коэффициент, не превышающий 3, к основной норме амортизации;

- при расчете налоговой базы на прибыль не берутся в расчет доходы, полученные в виде имущества налогоплательщиком в рамках целевого финансирования;

- для целей налогообложения независимо от результата признаются расходы на НИОКР.

1.3. Льготы по страховым взносам (СВ):

- для организаций, занимающихся в сфере информационных технологий, установлен пониженный тариф по СВ.

1.4. Льготы по налогу на имущество:

Размер налога устанавливается в законах субъектов РФ, не выше 2,2 %.

Рассмотрев первую классификацию налогоплательщиков, можем сказать, что предоставляются льготы по НДС, налогу на прибыль, СВ и налогу на имущество. Аналогично первой классификации налогоплательщиков, рассмотрим вторую.

2. Особые льготы для резидентов особой экономической зоны (ОЭЗ).

2.1. Льготы по налогу на прибыль:

– для резидентов ОЭЗ применяется пониженная ставка и в основном не может превышать 15,5 %;

– введены льготы на амортизацию основных средств, резидентам ОЭЗ предоставляется право использовать повышающий коэффициент, не превышающий 2, к основной норме амортизации.

2.2. Земельный налог:

Не облагаются налогом в основном со сроком на 10 лет, налогоплательщики резиденты ОЭЗ в отношении земельных участков, находящихся на этих территориях.

2.3. Налог на имущество:

Не облагаются налогом на имущество в основном со сроком на 10 лет, организации-участники ОЭЗ у которых данное имущество отображено на балансе организации.

Дополнительно необходимо отметить, что каждая ОЭЗ устанавливает свои размеры льгот и сроки их действия.

Во второй классификации льготы коснулись налога на прибыль, земельного налога и налога на имущество [3. С. 99].

3. Налоговые и таможенные льготы для налогоплательщиков, участников проекта Сколково:

3.1. Освобождение от НДС на 10 лет.

3.2. Освобождение на 10 лет налога на прибыль.

3.3. Снижение ставки СВ.

3.4. Возмещение затрат по уплате таможенных платежей в размере 100 %.

Налоговые льготы решают многие экономические проблемы, привлекают капитал и обеспечивают конкурентоспособность национальной экономике.

В России создан довольно обширный спектр инструментов налогового стимулирования инновационной деятельности, впрочем, несмотря на огромное количество льгот эффективность невысокая. На рис. 1 отображен рейтинг 45 инновационных стран 2021 г., первое место занимает Швейцария (индекс 65,5), второе Швеция (индекс 63,1), на третьем США (индекс 61,3), с достаточно большим разрывом Российская Федерация занимает 45 место (индекс 36,6).

В табл. 1 представлен рейтинг отдельных стран по годам. Дополнительно проанализировав глобальный инновационный индекс, можем заметить, что Российская Федерация с 2017 по 2021 г. практически стоит на одном месте (45–47 место). Поэтому есть смысл задуматься о переосмыслении налоговых льгот в сторону ввода действительно эффективных. Для того чтобы механизм работал, необходимо дополнительно со стороны государства осуществлять контроль.

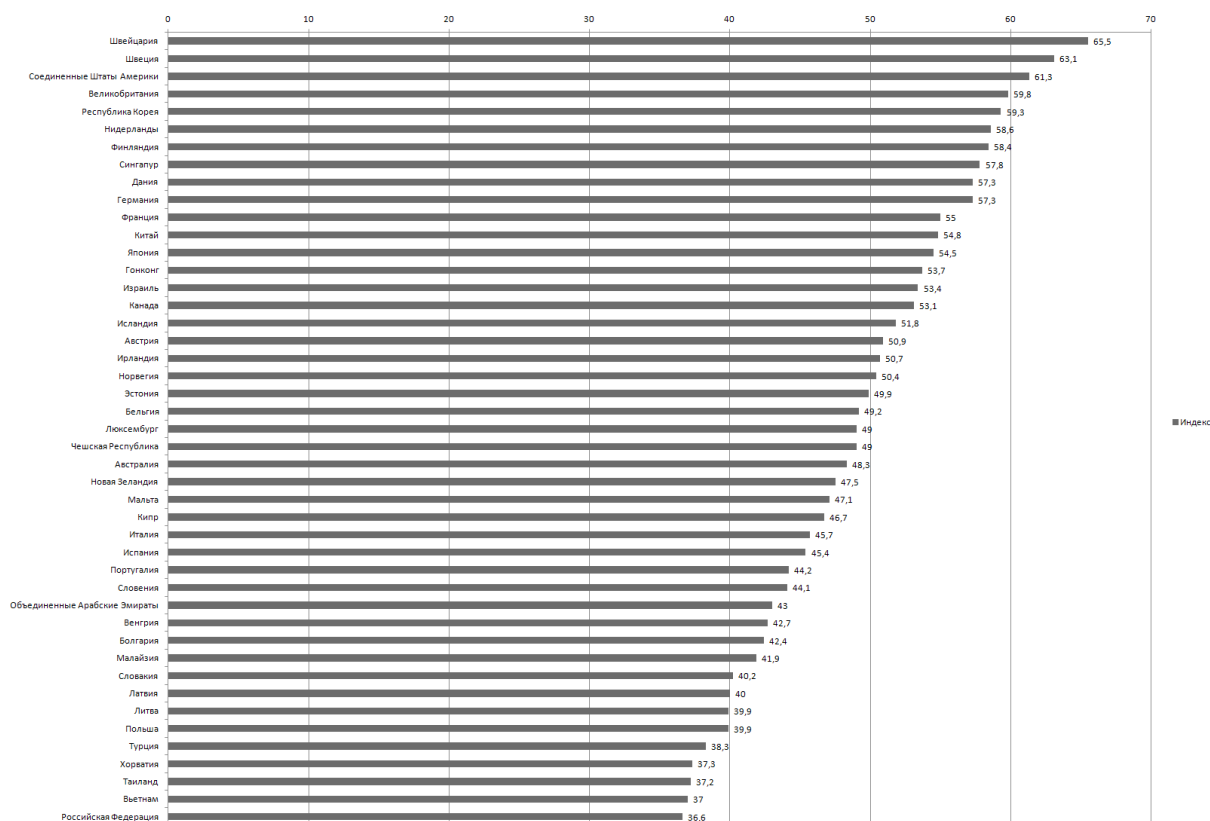


Рис. 1. Рейтинг 45 инновационных стран по данным ГИИ за 2021 г.

Таблица 1

Позиции отдельных стран в рейтингах инновационного развития

Показатель (год)	Глобальный инновационный индекс		
	Россия	США	Китай
2017	45	4	22
2018	46	6	17
2019	46	3	14
2020	47	3	14
2021	45	3	12

Составлено по: Global Innovation Index, <https://www.globalinnovationindex.org/analysis-economy>

Другим важным механизмом являются преференции, рассмотрим некоторые из них: инвестиционный налоговый кредит (ИНК), амортизационная премия.

ИНК – это возможность изменения срока уплаты налога при наличии оснований, указанных в ст. 67 НК РФ, при которых организации могут за определенный срок и в некоторых пределах снизить свои налоговые платежи с последующей поэтапной уплатой начисленных процентов и суммы кредита. ИНК предоставляется на срок от 1 года до 5 лет.

Амортизационная премия ст. 258 НК РФ предусматривает включение организацией в состав расходов затрат капитального характера для 1–2 и 8–10 аморти-

зационных групп в размере до 10 % и для 3–7 амортизационных групп до 30 % от первоначальной стоимости основных средств. Существует проблема нецелевого использования.

Инвестиционный налоговый кредит и амортизационные премии эффективные инструменты, требующие совершенствования. Во-первых, ввести ответственность за нецелевое использование, во-вторых, увеличить срок предоставления инвестиционного налогового кредита, в-третьих, совершенствование амортизационной премии за счет сокращения сроков амортизации оборудования.

Дополнительно необходимо отметить существующие в НК РФ специальные налоговые режимов, к ним относятся:

1. Система налогообложения для сельскохозяйственных товаропроизводителей (ЕСХН). Налогоплательщиками являются сельскохозяйственные товаропроизводители, к видам деятельности относится производство и реализация с/х продукции, налоговая база исчисляется, как доходы, уменьшенные на расходы с установленной налоговой ставкой 6 %.

2. Упрощенная система налогообложения (УСН). Налогоплательщиками выступают организации и индивидуальные предприниматели (ИП), нет ограничений по виду деятельности, налоговая ставка зависит от налоговой базы, ставка 6 %, если налоговой базой выступает доход, 15 %, если налоговая база исчисляется как доходы, уменьшенные на расходы. Дополнительно отметим, что данный режим предоставляет льготы малым инновационным предприятиям, позволяющим списывать расходы на НИОКР с повышающими коэффициентами.

3. Система налогообложения при выполнении соглашений о разделе продукции. Налогоплательщики – организации, выступающие инвесторами соглашения, виды деятельности прописаны в ФЗ «О соглашениях, о разделе продукции», налоговой базой при выполнении соглашения выступает доход, уменьшенный на расход с налоговой ставкой 20 %.

4. Патентная система налогообложения. Налогоплательщики – ИП, налоговой базой является потенциально возможный доход за год по видам деятельности со ставкой 6 % [2. С. 49].

Проанализировав специальные режимы налогообложения, наблюдаем, что наиболее подходящим для инновационного бизнеса является налоговый режим УСН. Также необходимо отметить, что необходима тщательная проработка данного направления и создание нового режима полностью удовлетворяющего потребности налогоплательщика.

Далее рассмотрим опыт зарубежных стран. Широкое распространение в зарубежных странах получили следующие формы льгот: налоговый кредит, ускоренная амортизация, налоговое освобождение, налоговые вычеты, патентное окно (рис. 2).

Разберем подробнее некоторые вышеуказанные формы налоговых льгот.

Налоговый кредит. Впервые в 1967 г. в мировой практике было применено налоговое стимулирование в виде налоговых кредитов национальным компаниям для увеличения финансирования НИОКР. Налоговый кредит – является налоговым стимулом, который позволяет определенным налогоплательщикам вычесть сумму начисленного ими кредита из общей суммы, которую они должны государству.

Это также может быть кредит, предоставляемый в знак признания уже уплаченных налогов, или форма государственной «скидки», применяемая в определенных случаях. Используется в Австралии, Японии, Норвегии, Австрии, Кореи, Бельгии, Канаде, Франции, Мексике, Бразилии, Китае, Индии, Ирландии, Великобритании, США. На текущий момент времени данный вид налоговых льгот является наиболее перспективным и распространенным инструментом в странах с развитой экономикой. В результате предоставления данной льготы предприятие усиливает, укрепляет свои позиции на отечественном и международном рынке инноваций, дополнительно способствует его развитию. Также необходимо отметить, что налоговый кредит не является одним из ключевых стратегических направлений реформирования экономики России.

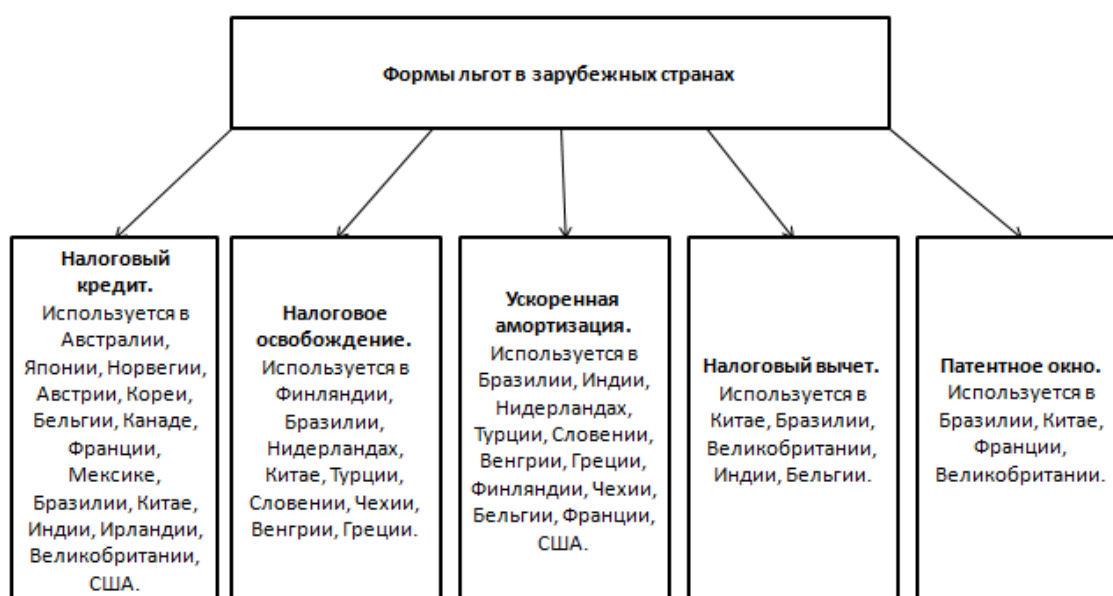


Рис. 2. Формы льгот в зарубежных странах

Дополнительно отметим, что ИНК в России и налоговый кредит в зарубежных странах отличается по смыслу, условиям и порядку применения. В России выступает в качестве займа и предоставляется на условиях платности, срочности и возвратности. В зарубежных странах – это означает уменьшить налоговые обязательства налогоплательщиков на фиксированный процент от суммы расходов на научно-исследовательские и опытно-конструкторские работы.

Ускоренная амортизация. Данная льгота дает возможность производить амортизацию приобретаемых основных средств по высоким ставкам в первые годы эксплуатации актива, позволяя таким образом уменьшать общую налогооблагаемую базу для определенных периодов. Используется в Бразилии, Индии, Нидерландах, Турции, Словении, Венгрии, Греции, Финляндии, Чехии, Бельгии, Франции, США. В подавляющем большинстве стран метод ускоренной амортизации основных средств применяется в налогообложении прибыли инновационных предприятий. В России согласно НК РФ при амортизации основных средств, используемых исключительно для осуществления научно-технической деятельно-

сти, организации имеют право применять специальный коэффициент, не превышающий 3, к основной норме амортизации.

Налоговое освобождение. Предполагает уменьшение размера налога на прибыль компаний, подлежащего уплате. Эта льгота может также применяться для любого налога юридических лиц, к личному доходу ИП, к налогам с заработной платы работников НИОКР. Используется в Финляндии, Бразилии, Нидерландах, Китае, Турции, Словении, Чехии, Венгрии, Греции.

Налоговый вычет. Предполагает снижение налогооблагаемой базы посредством увеличения расходов на НИОКР путем повышения коэффициента. Используется в Китае, Бразилии, Великобритании, Индии, Бельгии.

Патентное окно. Предполагает уменьшение налогооблагаемой прибыли на полные или частичные расходы, понесенные на разработку и реализацию запатентованной продукции. Также компании могут применять значительно сниженную ставку налога на доходы, полученные от своих патентных разработок. В отличие от других инновационных льгот, которые направлены на создание оптимальных условий на начальных этапах инновационного процесса, «патентное окно» создает налоговые стимулы для успешной реализации полученных инновационных результатов. Используется в Бразилии, Китае, Франции, Великобритании [4. С. 127]. Для России внедрение такого режима сомнительно, требуются большие затраты предприятия на инновационные и научные разработки.

В результате анализа наиболее распространенным методом среди вышеуказанных является налоговый кредит.

Заключение. Подведем итог, существующие на территории Российской Федерации механизмы налогового стимулирования инновационной деятельности, в сравнении с зарубежными странами, оказывают недостаточный эффект.

Предложения по усовершенствованию налогового стимулирования:

- закрепить понятия налоговая преференция и налоговая льгота в нормативно правовом акте;
- переосмыслить налоговые льготы в сторону ввода действительно эффективных льгот, которые должны соответствовать приоритетным целям государства, дополнительно со стороны государства осуществлять контроль над применяемыми льготами;
- ввести ответственность за нецелевое использование инвестиционного налогового кредита и амортизационной премии;
- увеличить срок предоставления инвестиционного налогового кредита;
- усовершенствовать амортизационные премии за счет сокращения сроков амортизации оборудования;
- создание нового специального режима полностью удовлетворяющего потребности налогоплательщика.

Список литературы

1. Бобырь Н. С. Льготы и преференции в системе налогового регулирования // Эволюция государства и права: проблемы и перспективы: сборник научных трудов 4-й Международной научной конференции, Курск, 24 марта 2022 года. – Курск: Юго-Западный государственный университет, 2022. – С. 7–10.

2. Бочаров Д. И. Механизмы налогового стимулирования малого инновационного предпринимательства в России и за рубежом: проблемы и перспективы // Экономика и бизнес: теория и практика. – 2021. – № 10–1 (80). – С. 47–51.

3. Джафарова З. К. Влияние уровня воздействия налоговой нагрузки на эффективность налогового регулирования инновационной деятельности // Вестник Дагестанского государственного университета. Серия 3: Общественные науки. – 2020. – Т. 35, № 4. – С. 97–103.

4. Маргарян А. Ш. Зарубежный опыт налогового стимулирования инновационной деятельности // Актуальные научные исследования в современном мире. – 2021. – № 12–8 (80). – С. 126–132.

Н. Н. Киселева,

магистрант,

Санкт-Петербургский политехнический университет Петра Великого

А. Н. Афонин,

кандидат экономических наук, доцент,

Санкт-Петербургский политехнический университет Петра Великого

ЦИФРОВИЗАЦИЯ ЧАСТНЫХ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ С ТОЧКИ ЗРЕНИЯ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. В статье рассмотрены вопросы, связанные с цифровизацией частных медицинских учреждений РФ, автоматизированной обработкой, защитой, хранением, обменом и использованием медицинских данных в здравоохранении. Проанализировано действующее законодательство в отношении защиты персональных данных в медицинских учреждениях. Определены пути решения проблем, связанных с безопасностью сбора, обработки, обмена и хранения медицинских данных пациентов как для отдельно взятых частных медицинских учреждений, так и для всей системы здравоохранения в целом.

Ключевые слова: здравоохранение, цифровизация, персональные данные, медицинские информационные системы

DIGITALISATION OF PRIVATE HEALTHCARE FACILITIES FROM THE PERSPECTIVE OF PERSONAL DATA PROTECTION LEGISLATION

Abstract. The article considers issues related to the digitalisation of private medical institutions in the Russian Federation, automated processing, protection, storage, exchange and use of medical data in healthcare. The current legislation regarding the protection of personal data in medical institutions is analysed. Ways of solving problems related to the security of the collection, processing, exchange and storage of patients' medical data both for individual private medical institutions and for the healthcare system as a whole were identified.

Keywords: Health, Digitalisation, Personal data, Health information systems

Цифровизация здравоохранения имеет важное значение в развитии экономики Российской Федерации (далее – РФ). Большие объемы данных, с которыми

работают медицинские учреждения, продолжают увеличиваться и накапливаться. К ним относятся не только истории болезней пациентов медицинских учреждений со всей сопутствующей информацией, но и вся совокупность результатов научных исследований в различных областях медицины и здравоохранения, объем которых растет экспоненциально.

Статьей 91 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (далее – ФЗ № 323-ФЗ) предусмотрено создание Единой государственной информационной системы в сфере здравоохранения (далее – ЕГИСЗ) [10]. ЕГИСЗ взаимодействует с различными информационными системами министерств и ведомств РФ, таких как: Федеральными фондами обязательного медицинского и социального страхования, системами, содержащими сведения об инвалидах, медико-социальных экспертиз и так далее, это позволит оптимизировать работу всей совокупности участников данной системы. Также к этой системе подключены государственные информационные системы в сфере здравоохранения субъектов РФ, медицинские информационные системы медицинских учреждений государственной, муниципальной и частной форм собственности [7].

Согласно данным Федеральной службы государственной статистики РФ и аналитической компании ООО «БизнесСтат», на конец 2020 г. в РФ насчитывалось 48,26 тыс. медицинских учреждений. За 2017–2020 гг. численность медицинских учреждений в РФ увеличилась на 7,38 % (табл. 1) [3, 4].

Таблица 1

Количество медицинских учреждений РФ (тыс.)

№	Параметр (год)	2017	2018	2019	2020
1	Численность медицинских учреждений	44,87	46,75	47,60	48,26
2	% к предыдущему году	–	4,19	1,81	1,38

Основное влияние на общую численность медицинских учреждений в РФ оказало увеличение числа коммерческих медицинских учреждений, существенный рост наблюдался в 2018 г., замедление роста в 2019–2020 гг. (табл. 2) [13, 4].

Таблица 2

Количество медицинских учреждений РФ

№	Формы собственности	2017 г.	2018 г.	2019 г.	2020 г.
1	Государственная	21 725	21 540	21 606	21 794
2	Частная	22 656	24 682	25 432	25 895
3	Иная	492	529	560	567
4	Всего	44 873	46 751	47 598	48 256

Количество частных и государственных медицинских учреждений почти одинакова в общей совокупности организаций здравоохранения в РФ. В 2017–2020 гг. количество частных медицинских учреждений находилось в пределах 50,5 % – 53,7 % от совокупного показателя. Доля государственных медицинских учреждений в общей их численности снизилась с 48,4 % в 2017 г. до 45,2 % в 2020 г. (рис. 1).



Рис. 1. Численность медицинских учреждений по формам собственности в 2017 и 2020 гг.

Таким образом, можно отметить тенденцию устойчивого роста количества частных медицинских учреждений в РФ.

По оценкам аналитических компаний, на начало 2021 г. потенциал рынка коммерческой медицины в РФ составил порядка 738–740 млрд руб. [5]. На развитие рынка коммерческой медицины будет влиять дальнейшее укрепление конкурентных преимуществ частных медицинских учреждений, в том числе в части цифровизации (рис. 2):

- внедрение телемедицинских консультаций;
- внедрение дистанционных сервисов обслуживания: чат-боты сопровождения, онлайн-запись, мобильные приложения и т. д.;
- внедрение систем поддержки принятия решений на основе алгоритмов машинного обучения и искусственного интеллекта, осуществляющих вспомогательную функцию при постановке диагноза и назначения дальнейшего лечения [6].

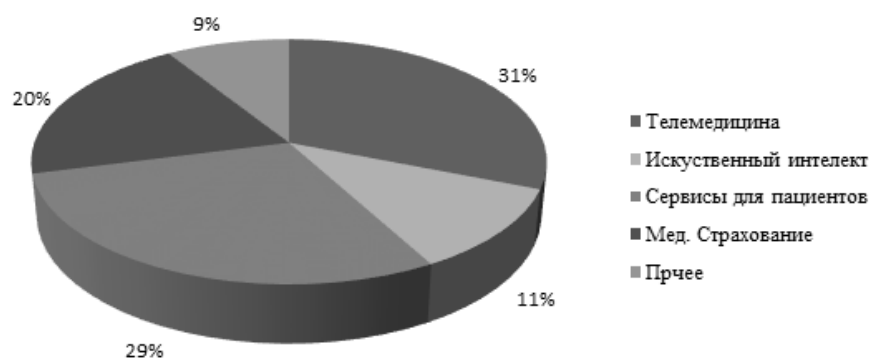


Рис. 2. Инвестиции в цифровизацию здравоохранения по секторам рынка в 2014 и 2021 гг.

Увеличение количества пациентов, пользующихся платными медицинскими услугами, будет обеспечено за счет развития цифровизации частных медицинских учреждений и внедрения инновационных технологий в части диагностики и лечения.

При дальнейшей цифровизации угроза конфиденциальности при увеличении объема персональных данных, циркулирующих в различных медицинских информационных системах при взаимодействии государства, частных медицинских учреждений и физических лиц – пациентов, в дальнейшем будет нарастать. Архитектура информационных систем, содержащих персональные данные пациентов, должна быть выстроена в соответствии с предотвращением следующих угроз:

- в части целостности: искажения медицинской информации, в случае совершения врачебной ошибки в процессе лечения, постановки диагноза и так далее недопустимы, система должна препятствовать изменению данных в истории болезни пациентов;

- в части конфиденциальности: хищение персональной информации о пациентах, несанкционированный доступ должны быть предотвращены;

- в части доступности: предотвращение угроз внешних сетевых атак и проникновения в системы вредоносного ПО.

В соответствии с Федеральным законом № 160-ФЗ от 19.12.2005 года «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», основным нормативным документом, регламентирующим защиту персональных данных в РФ, является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ № 152-ФЗ). Статья 3 ФЗ № 152-ФЗ определяет понятие персональных данных [11]. Под обработкой персональных данных понимаются такие действия, как: систематизация, накопление, хранение, уточнение, использование, распространение, обезличивание, блокирование, а также уничтожение данных.

В соответствии с Федеральным законом РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» для защиты информации в т. ч. персональных данных пациента используются [12]:

- организационно-правовые методы защиты: приказы, положения, инструкции, регламенты и так далее, охватывающие весь спектр цифрового документооборота медицинского учреждения;

- технические меры: межсетевые экраны, криптосредства, детекторы атак, сканеры уязвимостей и т. д.

Следует отметить, что действующее законодательство РФ защищает права граждан на сохранность их конфиденциальной информации. Основным объектом преступного посягательства выступают общественные отношения, складывающиеся в связи с реализацией конституционного принципа неприкосновенности частной жизни, личной и семейной тайны (ч. 1 ст. 23, ч. 1 ст. 24 Конституции РФ) [3]. За нарушение норм, регулирующих различные действия с персональными медицинскими данными пациентов, предусмотрена ответственность:

- дисциплинарная (ст. 90, 192 Трудового кодекса РФ);

- административная (ст. 13.11 Кодекса об административных правонарушениях РФ);

- гражданско-правовая (ст. 15, 151 Гражданского кодекса РФ);

- уголовная (ст. 137 Уголовного кодекса РФ), в соответствии с федеральным законодательством [8, 2, 1, 9].

Таким образом, можно выделить пути решения проблем, связанных с безопасностью сбора, обработки, обмена и хранения медицинских данных пациентов:

- в рамках разработки архитектуры медицинских информационных систем, в том числе сервисов ЕГИСЗ, а также непосредственно в информационных системах самих медицинских учреждений, создание подсистем по обезличиванию персональных данных, а также защищенной сети передачи данных;

- разработка и принятие нормативных актов федерального, регионального, отраслевого уровня по регулированию использования и обращения медицинских данных;

- разработка внутренних регламентов в медицинских учреждениях, определяющих право доступа к данным пациента, а также запрет на изменение данных в истории болезни пациента.

Рассмотренные выше вопросы не охватывают всего спектра проблем, связанных с цифровизацией частных медицинских учреждений РФ, автоматизированной обработкой, защитой, хранением, обменом и использованием медицинских данных в здравоохранении. Однако огромный потенциал имеют технологии для работы с большими данными. Сбор данных о пациентах, их передача и последующее использование поможет, например, разработать системы поддержки принятия решений, а также модели прогнозной аналитики на основе искусственного интеллекта, что, в свою очередь, позволит снизить нагрузку на врачей и уменьшить медицинские расходы. В этом критерии кроется актуальность рассматриваемой проблемы, связанной с безопасным обменом медицинскими данными как для отдельно взятых частных медицинских учреждений, так и для всего здравоохранения в целом.

Список литературы

1. Гражданский кодекс РФ. URL: <https://www.garant.ru/> (дата обращения: 06.09.2022).

2. Кодекс об административных правонарушениях РФ. URL: <https://www.garant.ru/> (дата обращения: 06.09.2022).

3. Конституция РФ. URL: <https://www.garant.ru/> (дата обращения: 06.09.2022).

4. Обзор Группы «ДЕЛОВОЙ ПРОФИЛЬ»/MGI Worldwide. Рынок коммерческой медицины в России: тенденции и перспективы развития. URL: https://delprof.ru/upload/iblock/e17/DelProf_Analitika_Rynok-kommercheskoj-meditsiny.pdf (дата обращения: 06.09.2022).

5. Обзор рынка BisnesStat. Анализ рынка медицинских услуг в России в 2016–2020 гг., оценка влияния коронавируса и прогноз на 2021–2025 гг. URL: https://bisnesstat.ru/images/demo/medicine_russia_demo_bisnesstat1.pdf (дата обращения: 06.09.2022).

6. Обзор TAdviser «Цифровизация здравоохранения». URL: [https://zdrav.expert/index.php/Статья: Обзор_Цифровизация_здравоохранения](https://zdrav.expert/index.php/Статья:Обзор_Цифровизация_здравоохранения) (дата обращения: 06.09.2022).

7. Постановление Правительства РФ от 09.02.2022 № 140 «О единой государственной информационной системе в сфере здравоохранения» (вместе с «Положением о единой государственной информационной системе в сфере здравоохранения»). URL: <https://www.garant.ru/> (дата обращения: 06.09.2022).

8. Трудовой кодекс РФ. URL: <https://www.garant.ru/> (дата обращения: 06.09.2022).

9. Уголовный кодекс РФ. URL: <https://www.garant.ru/> (дата обращения: 06.09.2022).
10. Федеральный закон РФ от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации». URL: <https://www.garant.ru/> (дата обращения: 06.09.2022).
11. О персональных данных: Федеральный закон РФ от 27.07.2006 № 152-ФЗ. URL: <https://www.garant.ru/> (дата обращения: 06.09.2022).
12. Об информации, информационных технологиях и о защите информации: Федеральный закон РФ от 27.07.2006 № 149-ФЗ. URL: <https://www.garant.ru/> (дата обращения: 11.09.2022).
13. Федеральная служба государственной статистики РФ. Российский статистический ежегодник 2021. URL: https://rosstat.gov.ru/storage/mediabank/Ejegodnik_2021.pdf (дата обращения: 06.09.2022).

М. Ю. Комова,

студент,

Московский государственный юридический университет
имени О. Е. Кутафина

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ VPN-ТЕХНОЛОГИЙ В РОССИИ

Аннотация. Анализируются актуальные изменения законодательства об информации, информационных технологиях и о защите информации, которыми закреплен запрет использования VPN в России и установлена обязанность владельцев анонимайзеров и VPN-сервисов сотрудничать с правоохранительными органами и ограничивать доступ ко всем сайтам, запрещенным на российской территории. Делается вывод о необходимости принятия подзаконных актов, подробно регламентирующих вопросы борьбы с обходом заблокированных веб-сайтов.

Ключевые слова: цифровое право, VPN-технологии, веб-сайт, поисковые системы, Интернет, Роскомнадзор

LEGAL REGULATION OF THE USE OF VPN TECHNOLOGIES IN RUSSIA

Abstract. The article analyzes the current changes in legislation on information, information technologies and information protection, which are fixed the ban on the use of VPNs in the country and established a duty the owners of anonymizers and VPN services to cooperate with law enforcement agencies and restrict access to all sites prohibited on Russian territory. The author concludes that it is necessary to adopt by-laws that regulate in more detail the issues of combating bypassing blocked websites.

Keywords: Digital law, VPN technologies, Website, Search engines, Internet, Roskomnadzor

Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» с изменениями, внесенными в него Федеральным законом от 29.07.2016 № 276 [3], запрещено использование специаль-

ного программного обеспечения или услуг, если они позволяют пользователям получить доступ к заблокированным в России сайтам. Закон вызвал многочисленные вопросы, в частности, со стороны иностранных компаний [1; 2. С. 164–166].

Закон запрещает владельцам специализированного программного обеспечения, информационных сетей, веб-сайта, а также соответствующего оборудования (совместно именуемые «VPN-технологии») от предоставления технологий, позволяющих обойти запрет на доступ к заблокированным в России сайтам.

Следовательно, VPN-технологии как таковые не запрещены: запрещено только использование этих технологий для предоставления доступа к заблокированным в России сайтам.

Технологии VPN могут пониматься, в частности, как:

- виртуальные частные сети (VPN);
- анонимные прокси-серверы;
- некоторые типы маршрутизаторов;
- другое программное или техническое оборудование, выполняющее аналогичные функции.

Закон нацелен на владельцев таких VPN-технологий, но не на их пользователей. Операторы поисковых систем, распространяющие через интернет-рекламу, ориентированную на российских потребителей, также подчиняются закону. Такие поисковые системы должны прекратить предоставлять ссылки на заблокированные сайты.

В связи с принятием этого закона Роскомнадзор установил всех собственников технологий VPN. При этом Роскомнадзор связывается с хостинг-провайдерами, направляет владельцам VPN Technologies на русском и английском языках уведомления о необходимости подключения к специальной информационной системе в сети Интернет, содержащей информацию о запрещенных в России сайтах. Владельцы VPN Technologies обязаны подключиться к этой системе и ограничить доступ к веб-сайтам, указанным в системе.

Закон предусматривает принятие целого ряда подзаконных актов, которые будут разяснять отдельные вопросы. В настоящее время такие подзаконные акты существуют только в виде проекта. Соответственно, главной тенденцией следующих лет в правовом регулировании VPN технологий будет принятие и вступление в силу подзаконных актов, которые будут подробнее регламентировать вопросы борьбы с подобными сервисами.

Список литературы

1. Российская Газета – Федеральный выпуск № 60 (8708) от 21.03.2022. URL: <https://rg.ru/2022/03/21/reg-cfo/sud-zapretil-v-rossii-instagram-i-facebook-za-ekstremistskuiu-deiatelnost.html> (дата обращения: 10.09.2022).
2. Синтез науки и общества в решении глобальных проблем современности: сборник статей Всероссийской научно-практической конференции (13 мая 2022 г., г. Екатеринбург). – Уфа: Аэтерна, 2022. – 240 с. (дата обращения: 10.09.2022)
3. Федеральный закон от 29.07.2017 № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru> (дата обращения: 10.09.2022).

Е. С. Корепанова,

студент,

Удмуртский государственный университет

МЕЖДУНАРОДНЫЕ РАСЧЕТЫ В КРИПТОВАЛЮТЕ И УКЛОНЕНИЕ ОТ ИСПОЛНЕНИЯ ОБЯЗАННОСТИ ПО РЕПАТРИАЦИИ ДЕНЕЖНЫХ СРЕДСТВ: ПРОБЛЕМЫ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ

Аннотация. Целью работы является изучение возможности применения криптовалюты при уклонении от исполнения обязанности по репатриации денежных средств. Анализируются действующее законодательство, регулирующее криптовалюту, судебная практика и доктринальные позиции о признании криптовалюты предметом преступлений, в том числе уклонение от исполнения обязанностей по репатриации денежных средств в иностранной валюте или валюте Российской Федерации. Также рассматриваются проблемы уголовно-правовой охраны валютного регулирования и валютного контроля над репатриацией валютной выручки от внешнеэкономических сделок. Оцениваются возможности привлечения к уголовной ответственности лиц, уклоняющихся от исполнения обязанности по репатриации денежных средств в криптовалюте и риски использования криптовалюты как способа вывода капиталов за рубеж. Делается вывод о необходимости разработки комплексного правового регулирования и внесения ряда изменений в УК РФ и КоАП РФ.

Ключевые слова: внешнеторговые сделки, цифровая валюта, криптовалюта, средства платежа, репатриация денежных средств, предмет преступления, идентификация субъекта

INTERNATIONAL SETTLEMENTS IN CRYPTOCURRENCY AND EVASION OF THE OBLIGATION TO REPATRIATE MONEY RESOURCE: PROBLEMS OF CRIMINAL LIABILITY

Abstract. The purpose of the work is to study the possibility of using cryptocurrencies when evading the obligation to repatriate funds. The current legislation regulating cryptocurrencies, judicial practice and doctrinal positions on recognizing cryptocurrencies as the subject of crimes, including evasion of obligations to repatriate funds in foreign currency or the currency of the Russian Federation, are analyzed. The problems of criminal law protection of currency regulation and currency control over the repatriation of foreign exchange earnings from foreign economic transactions are also considered. The possibilities of bringing to criminal responsibility persons who evade the obligation to repatriate funds in cryptocurrency and the risks of using cryptocurrency as a way to withdraw capital abroad are evaluated. It is concluded that it is necessary to develop a comprehensive legal regulation and make a number of changes to the Criminal Code of the Russian Federation and the Administrative Code of the Russian Federation.

Keywords: international trade transactions, cryptocurrency, digital currency, means of payment, repatriation of money resource, the object of the crime, the identification of the subject

В апреле 2022 г. Центральный банк РФ и Министерство финансов РФ имели противоположные позиции по поводу признания криптовалюты в качестве средства платежа [4]. Однако в условиях геополитической напряженности, санкционных мероприятий, проводимых Европейским Союзом и США, крупнейшие российские компании и импортеры остались без возможности расплачиваться по внешнеторговым сделкам. В связи с этим в конце мая 2022 г. Центральный банк России допустил возможность использования криптовалюты в международных сделках и международной финансовой инфраструктуре [3]. При этом директор Росфинмониторинга Юрий Чиханчин, поддерживая возможность осуществления таких сделок, заявил о необходимости запрета использования криптовалюты для осуществления платежей в России [8].

Несмотря на активное обсуждение возможности использования криптовалюты, ч. 5 ст. 14 ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» содержит прямой запрет на получение криптовалюты в качестве оплаты для «юридических лиц, личным законом которых является российское право, филиалов, представительств и иных обособленных подразделений международных организаций и иностранных юридических лиц, компаний и других корпоративных образований, обладающих гражданской правоспособностью, созданных на территории Российской Федерации, физических лиц, фактически находящихся в Российской Федерации не менее 183 дней в течение 12 следующих подряд месяцев» [17].

Реализация предложения об использовании криптовалюты в международных сделках предполагает необходимость внесения изменений не только в регулятивное законодательство, но и в административное и уголовное. Для формирования комплексного правового регулирования в Государственную Думу РФ Минфином России 18 февраля 2022 г. на рассмотрение внесен проект Федерального закона «О цифровой валюте», разработанный по поручению Правительства Российской Федерации [18]. В последней редакции проекта ФЗ криптовалюту предложено рассматривать в качестве инструмента для инвестиций, предмета совершения сделок купли-продажи [13], «использовать для оплаты внешнеторговой деятельности юридических лиц и индивидуальных предпринимателей» [3].

В сложившейся ситуации использование криптовалюты в качестве средства платежа по международным сделкам, возможно, будет реализовано в ближайшем будущем. На практике уже осуществляется разработка на острове Русский экспортно-импортных расчетов с использованием цифровых финансовых активов, о чем на конференции «Цифровые финансы: новые пути развития», проводимой в рамках Восточного экономического форума 2022, заявила Анна Шарипова, представитель Государственной корпорации «Ростех» [19]. В мировой практике первопроходцем применения криптовалюты в качестве средства платежа по международным сделкам является Иран. Так, представители бизнеса, применяя соглашение между Министерством промышленности и Центральным банком Ирана, могут импортировать автомобили, используя для оплаты криптовалюту вместо долларов США или евро [5].

Между тем использование криптовалюты в качестве средства платежа по международным сделкам может повлечь ряд проблем, связанных с уголовно-пра-

вой охраной валютного регулирования и валютного контроля над репатриацией валютной выручки от внешнеэкономических сделок, которые являются одним из способов противодействия выводу капитала за рубеж.

Диспозиции уголовно-правовых норм не предусматривают возможность их применения к случаям, когда расчеты по международным сделкам производятся с использованием криптовалюты. Предметом преступления, предусмотренного ст. 193 УК РФ, являются денежные средства в иностранной валюте или в валюте Российской Федерации. Ч. 1 ст. 1 ФЗ «О валютном регулировании и валютном контроле» [16], раскрывая основные понятия, не рассматривает цифровую валюту (криптовалюту) в качестве денежных средств ни в валюте Российской Федерации, ни в иностранной валюте. Таким образом, существующее нормативно-правовое регулирование, свидетельствует о том, что криптовалюта не является предметом уклонения от исполнения обязанностей по репатриации денежных средств.

В юридической литературе криптовалюта также не рассматривается в качестве предмета уклонения от исполнения обязанностей по репатриации. Особой позиции придерживается А. Ф. Волобуев. Признавая невозможность отнесения виртуальной валюты (криптовалюты) к предмету преступления, он, однако, моделирует ситуацию, при которой применение криптовалюты может быть квалифицировано по ст. 193 УК РФ, при наличии иных необходимых признаков. Такая ситуация характеризуется тем, что оплата по внешнеторговой сделке осуществляется с использованием криптовалюты, а эквивалентная ей сумма фиатных денежных средств оказывается незачисленной на счета резидента в уполномоченном банке или на счета резидента в банках, расположенных за пределами территории РФ [7. С. 41].

Анализ судебной практики позволяет говорить о том, что предметом уклонения от исполнения обязанностей по репатриации денежных средств за последние два года признаются денежные средства в иностранной валюте [9] и денежные средства в валюте Российской Федерации [2]. Аналогичным образом судебная практика формируется и по административным правонарушениям, предусмотренным ч. 5.2 ст. 15.25 КоАП РФ [14, 15].

Таким образом, в науке и судебной практике криптовалюта бесспорно признается в качестве средства совершения некоторых преступлений. Например, А. А. Коренная, Н. В. Тыдыкова указывают на то, что криптовалюта становится привлекательным средством для приобретения оружия, боеприпасов (ст. 222 УК РФ), наркотических и психотропных веществ (ст. 228 УК РФ), финансирования терроризма (ст. 205.1 УК РФ), отмывания «преступных доходов» (ст. ст. 174, 174¹ УК РФ), совершения налоговых правонарушений (ст. 199 УК РФ) [12. С. 411]. Суды в основном признают криптовалюту в качестве средства совершения таких преступлений, как сбыт, хранение наркотических средств и психотропных веществ [10], незаконного приобретения боевого пистолета с патронами [1]. С учетом особенностей конструкции состава преступления, предусмотренного действующей редакцией ст. 193 УК РФ, применение уголовного закона в отношении лиц, использующих криптовалюту как средство платежа, в отличие от вышеприведенных примеров, маловероятно, так как расширительное толкование предмета данного

преступления будет означать применение уголовного закона по аналогии. Следует согласиться с тем, что, исходя из действующей редакции ст. 193 УК РФ, криптовалюта в науке и судебной практике не признается в качестве предмета уклонения от исполнения обязанностей по репатриации денежных средств.

Проблемы уголовной ответственности за уклонение от исполнения обязанности по репатриации денежных средств, которые могут возникнуть в случае использования криптовалюты в международных сделках, обусловлены и другими обстоятельствами.

Большая часть негативных последствий применения криптовалюты связана с отсутствием возможности идентификации субъекта, использующего ее. Это условие применения криптовалюты оказывает влияние на невозможность отслеживания процесса осуществляемых с ней финансовых операций, а также осуществления получения информации для налогообложения сделок, совершаемых с использованием криптовалюты.

В руководстве 2019 г. ФАТФ указало на необходимость надзора и мониторинга в сфере виртуальных активов компетентными государственными органами [20]. При этом на надзорные органы должны быть возложены полномочия по применению финансовых санкций [11. С. 6].

В августе 2021 г. Федеральная служба по финансовому мониторингу заключила с компанией RCO контракт на выполнение «работ по созданию модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина» [6]. Данная система мониторинга позволит отслеживать процессы по перемещению цифровой валюты; выявлять криптовалютные кошельки, используемые для осуществления противоправной деятельности и финансирования терроризма, формировать базы данных таких криптовалютных кошельков; идентифицировать участников, применяющих для осуществления экономической деятельности цифровую валюту. Однако отсутствует информация о дальнейшей разработке, готовности и внедрении данного модуля. В связи с указанным можно предположить, что на сегодняшний день возможно отслеживать только цепочки операций, проводимых с Bitcoin или Ethereum, которые, однако, невозможно связать с конкретным субъектом.

Одним из конструктивных признаков состава преступления, предусмотренного ст. 193 УК РФ, является крупный размер. В случае с использованием криптовалюты определить его наличие или отсутствие практически невозможно, так как в отличие от официального курса валют, официального курса криптовалют не существует. Говоря о криптовалюте, необходимо отметить, что курс криптовалют в эквивалентном пересчете на фиатные деньги различен. При этом данный курс характеризуется невозможностью влияния на него государственных структур, нестабильностью и постоянным изменением.

Проблемы уголовно-правовой охраны экономической (внешнеэкономической) безопасности России при осуществлении международных расчетов в криптовалюте могут быть решены путем создания комплексного регулятивного законодательства и внесении изменений в УК РФ и КоАП РФ. Для этого необходимо признать криптовалюту в качестве средства платежа наравне с валютой РФ и иностранной валютой. Установление уголовной ответственности и применение уголовно-правовых норм

за нарушение регулятивного законодательства (нарушение установленных правил или уклонение от исполнения возложенных на участников регулятивных отношений обязанностей) возможно только в условиях его существования.

Предполагаем, что при введении расчетов в криптовалюте по международным сделкам риски использования их как способа вывода капиталов за рубеж будет минимальным по нескольким причинам. Во-первых, нестабильность курса криптовалюты делает ее непривлекательным средством платежа для представителей бизнеса, не готовых нести экономические риски, связанные с необеспеченностью криптовалюты каким-либо товаром. Эти обстоятельства позволяют рассматривать криптовалюту как «финансовый пузырь», способный лопнуть в любой момент в силу искусственных или естественных причин. Обрушение курса криптовалюты способно привести к финансовому кризису и негативно сказаться на субъектах предпринимательской деятельности, применяющих ее в качестве средства платежа. Во-вторых, думается, что в ближайшее время будет введен соответствующий государственный модуль мониторинга и анализа финансовых операций, совершаемых с криптовалютой, что позволит разрешить проблему анонимности таких платежей. Возможность идентификации субъекта, применяющего криптовалюту в целях совершения преступления, снизит привлекательность данной цифровой валюты. Тем не менее необходимо при установлении возможности использования криптовалюты в международных сделках ввести соответствующие изменения в ст. 193 УК РФ.

Список литературы

1. Апелляционное определение Липецкого областного суда от 24.11.2020 по делу № 22–1402/2020 // СПС «КонсультантПлюс». URL: <https://clck.ru/324nTq> (дата обращения: 11.09.2022).
2. Апелляционное определение Московского городского суда от 15.06.2020 по делу № 10–9701/2020 // СПС «КонсультантПлюс». URL: <https://clck.ru/324nKj> (дата обращения: 17.09.2022).
3. Банк России допустил возможность международных расчетов в криптовалюте. URL: <https://clck.ru/324s6C> (дата обращения: 11.09.2022).
4. Банк России заявил об угрозе замещения рубля криптовалютами. URL: <https://clck.ru/324s6c> (дата обращения: 11.09.2022).
5. В Иране разрешили оплачивать импорт автомобилей криптовалютой. URL: <https://clck.ru/324s74> (дата обращения: 14.09.2022).
6. В РФ начнут отслеживать криптовалютные транзакции. Что это значит. URL: <https://clck.ru/Wd59R> (дата обращения: 14.09.2022).
7. Волобуев А. Ф. Объект уклонения от исполнения обязанностей по репатриации денежных средств // Научный вестник Омской академии МВД России. 2018. № 4 (71). С. 39–43. URL: <https://clck.ru/324rxJ> (дата обращения: 17.09.2022).
8. Госкорпорация ростех проведет тестирование цифровых активов в международной торговле. URL: <https://clck.ru/325wof> (дата обращения: 11.09.2022).
9. Кассационное определение Четвертого кассационного суда общей юрисдикции от 21.04.2021 по делу № 77–1428/2021 // СПС «КонсультантПлюс». URL: <https://clck.ru/324nJW> (дата обращения: 17.09.2022).

10. Кассационное определение Четвертого кассационного суда общей юрисдикции от 21.06.2021 № 77-1787/2021 // СПС «КонсультантПлюс». URL: <https://clck.ru/324nSU> (дата обращения: 11.09.2022).

11. Кинсбургская В. А. Требования ФАТФ по регулированию криптовалют: проблемы имплементации в национальное законодательство // Национальная безопасность / nota bene. 2020. № 4. URL: <https://clck.ru/324rww> (дата обращения: 14.09.2022).

12. Коренная Анна Анатольевна, Тыдыкова Надежда Владимировна Криптовалюта как предмет и средство совершения преступлений // Всероссийский криминологический журнал. 2019. № 3. С. 408–415. URL: <https://clck.ru/324ruq> (дата обращения: 11.09.2022).

13. Минфин России направил в Правительство России проект федерального закона «О цифровой валюте» // <https://clck.ru/bmoVy> (дата обращения: 11.09.2022).

14. Постановление Пятнадцатого арбитражного апелляционного суда от 12.02.2021 № 15АП-22376/2020 по делу № А53-35608/2020 // СПС «КонсультантПлюс». URL: <https://clck.ru/324nP8> (дата обращения: 17.09.2022).

15. Постановление Тринадцатого арбитражного апелляционного суда от 27.07.2021 № 13АП-17117/2021 по делу № А56-3173/2021 // СПС «КонсультантПлюс». URL: <https://clck.ru/324nMY> (дата обращения: 17.09.2022).

16. Федеральный закон от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле» // СПС «КонсультантПлюс». URL: <https://clck.ru/324n85> (дата обращения: 11.09.2022).

17. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: <https://clck.ru/SUtu0> (дата обращения: 11.09.2022).

18. Федеральный портал проектов нормативно-правовых актов // <https://clck.ru/324rsS> (дата обращения: 11.09.2022).

19. Цифровые финансы: новые пути развития // <https://clck.ru/324rqD> (дата обращения: 14.09.2022).

20. VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS-2019. URL: <https://clck.ru/324rpc> (дата обращения: 12.09.2022).

К. С. Корчагина,

студент,

Московский государственный университет имени М. В. Ломоносова

ПРАВОВАЯ ОХРАНА ОБЪЕКТОВ АВТОРСКОГО ПРАВА, СОЗДАНЫХ ИСКУССТВЕННЫМИ ИНТЕЛЛЕКТОМ

Аннотация. В статье освещается проблема правовой охраны объектов, созданных искусственным интеллектом. Исследуется творческий аспект в деятельности ИИ, исследуются субъекты, которые могут быть наделены авторскими правами. Проблема определения режима, результата применения ИИ очень важна и актуальна, так как ИИ все активнее вторгается в нашу жизнь и становится способным создавать различные произведения.

Ключевые слова: право, искусственный интеллект, авторское право, разработчики искусственного интеллекта, правообладатели, творческий аспект деятельности, пользователь ИИ

LEGAL PROTECTION OF COPYRIGHT ITEMS CREATED BY ARTIFICIAL INTELLIGENCE

Abstract. The article deals with the problem of the occurrence of diseases caused by artificial intelligence. The author includes a creative aspect in the activity of AI, includes subjects that include copyright. The problem of determining the results of the application of AI is very important and relevant, as AI is increasingly invading our lives and has begun to create various works.

Keywords: Law, Artificial intelligence, Copyright, Creators of artificial intelligence, Copyright holders, Creative aspect of activity, AI user

Искусственный интеллект становится неотъемлемым элементом нашей жизни, он помогает решать многие проблемы, при этом затрачивая меньше усилий. В настоящее время искусственный интеллект уже имеет многое – он может создавать художественные, музыкальные произведения, писать новости и другое. Так, например, технология Next Rembrandt создает картины, которые достаточно сложно отличить от произведений Рембрандта. В связи с тем, что робот способен к созданию определенных объектов, возникают различные вопросы, которые не имеют однозначного ответа. Кто является правообладателем произведений, создаваемых ИИ? Каким образом охранять произведения, создаваемые ИИ или с его использованием? Эти и другие вопросы будут рассмотрены в данной работе.

Прежде всего, необходимо разделить слабый и сильный искусственный интеллект. Сильный ИИ будет способен имитировать процесса работы мозга человека. В настоящее время создан только «слабый» – такой ИИ не обладает сознанием, но даже слабый ИИ может создавать такие результаты, которые не охватывались замыслом разработчиков, связано это с тем, что ИИ способен к самообучению, именно поэтому при дальнейшей своей эксплуатации он способен создавать произведения, которые не были изначально в него заложено разработчиком. Таким образом, искусственный интеллект может быть как инструментом, который является помощником человека, и также как самостоятельным создателем, способным достигать каких-либо результатов интеллектуальной деятельности без участия человека.

В связи с тем, что произведения, создаваемые ИИ или с его помощью, представляют художественную и экономическую ценность, то возникает необходимость в обеспечении правовой охране таких результатов. Согласно ст. 1228 ГК РФ автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат. Данное определение включает в себя два критерия, во-первых, только человеком может стать автором произведения, во-вторых, необходим творческий вклад.

Можно ли говорить о наличии творческого аспекта в деятельности ИИ? Отвечая на этот вопрос, необходимо разделять две ситуации: 1) когда ИИ используется как

инструмент и 2) когда ИИ создает произведение при минимальном участии человека, либо же совершенно в его отсутствие. Если ИИ используется как помощник, то в такой ситуации вполне возможно обнаружить творческий вклад человека, потому что он прилагает определенные усилия, осуществляя свою сознательную деятельность. Во второй же ситуации дело обстоит по-другому. Достаточно проблематичным является признание авторства за человеком, потому что как такового он творческого вклада не привносит в создаваемый объект, зачастую достаточно механического нажатия на кнопку. Если же признать за таким действием творческий характер, то это может умалить творчество других людей, потому что получится, что простое нажатие на кнопку является творчеством, и долгая работа художника над картиной тоже будет творчеством. Можно ли применять понятие творчества к ИИ? О. С. Иоффе говорил о том, что творчество – сознательная и созидательная деятельность, на которую способен только человек. В творческой деятельности необходим именно осознанный контроль над процессом. Машина же воспроизводит категории и образы, которые были заложены в нее человеком. Внешней характеристикой объекты, создаваемые роботом, могут и напоминать произведения, однако они не будут ими являться, потому что произведения должны быть именно созидательной деятельностью, сам процесс создания объекта также должен быть творческим. Таким образом, в случае создания произведения при минимальном участии человека, творческого аспекта у человека может и не быть, тогда в судебном деле может оказаться невозможным доказать участие человека, и произведение не будет охраняться авторским правом. Так, материалы видеофиксации не охраняются авторским правом. Что касается ИИ, то он не может являться автором, так как, во-первых, автором по нашему законодательству может быть исключительно человек и, во-вторых, ИИ не обладает творческим характером деятельности, он только изучает множество объектов и создает похожее. Из этого вытекает проблема того, каким способом возможно будет исследовать степень участия человека в создании произведения совместно с ИИ.

Необходимо понимать, что степень участия человека в процессе создания произведения ИИ может быть различным, и от этого будет зависеть механизм охраны и наделяния. Выделяют следующие ситуации: а) произведения созданы по заданию пользователя, т. е. ИИ используется в качестве инструмента, б) произведения самостоятельно создаются ИИ без участия человека, в) совместное участие алгоритма и человека.

То есть степень участия робота в разработке объекта может быть различной: это может быть простое выполнение механических действия, а может доходить и до сложнейшей обработки исходного материала, когда компьютер выводит такой результат, который не охватывался замыслом разработчика.

Рассмотрим ситуации, где ИИ используется в качестве инструмента. Если ИИ используется в качестве инструмента и оказывает существенное влияние человека на результат, то в такой ситуации у человек поистине можно считать автором произведения, он привносит свой вклад.

В том случае, если результаты деятельности ИИ охраноспособны, то возникает вопрос, за кем закреплять права на эти результаты. В литературе сложились

различные точки зрения по поводу носителя прав на объекты, создаваемые ИИ: от машиноцентрической теории, которая предполагает надделение ИИ правами автора, до антропоцентрической, где автором является человек, также выделяются идеи отсутствия автора. Кроме того, права могут закрепляться за: а) автором-разработчиком или иным правообладателем программы, однако здесь лицо, однажды написавшее программу, станет автором всех последующих произведений, хотя непосредственного участия оно в них принимать не будет, б) программой, основанной на ИИ, однако стоит отметить, компьютер не нуждается в поощрении и вознаграждении, в) пользователем, но он просто может просто нажимать на кнопку, не являясь, на самом деле, автором произведения, г) не охранять такие результаты. Последний вариант также критикуется, так как правовая охрана объектов играет важную роль, помогая не допустить несанкционированного использования и заимствования, а также она позволяет поощрять авторов, давая возможность получать им вознаграждение путем коммерциализации. Получается, что возникает проблема определения режима результата применения ИИ, и очень важно определить режим регулирования, потому что от ответа на этот вопрос будет зависеть то, кто будет получать вознаграждение за использование объектов, созданных ИИ.

Рассматривая вопрос о способе охране результатов, созданных ИИ без вмешательства человека, тоже возникают несколько вариантов: а) общественное достояние – это препятствует инновационному развитию, в рыночной экономике существует цель коммерциализации, б) охрана в качестве информации, в) охрана авторским правом – но в нашем законодательстве для признания автора необходимо не только творческий вклад, но и произведение должно быть создано человеком, однако здесь опять возникает вопрос о способности ИИ заниматься творчеством, г) охрана смежными правами, однако при таком подходе создаваемые объекты не становятся полноценными произведениями.

Таким образом, если произведение создано творческим трудом человека с использованием ИИ, то правовая охрана должна осуществляться по сложившимся правилам авторского права, однако если произведения создаются без творческого труда человека, уже защищая произведения средствами защиты в авторском праве, следует выбрать другую модель защиты. Возможно, стоит выбрать модель смежного права по примеру охраны прав изготовителей баз данных, которая направлена на обеспечение экономических прав и интересов разработчиков ИИ в течение ограниченного времени. Кроме того, принимая во внимание то, что искусственный интеллект в результате своего обучения создает произведения на основе большой базы данных, возможен и другой вариант регулирования через рассмотрение ИИ в качестве производного произведения от базы данных, в таком случае разработчику необходимо будет получать лицензию на базу данных, допускающую создание производных произведений.

Список литературы

1. Войниканис Е. А., Семенова Е. В., Тюляев Г. С. Искусственный интеллект и право: вызовы и возможности самообучающихся алгоритмов // Вестник ВГУ. Серия: Право. 2018. № 4 (35). URL: [https://cyberleninka.ru/article/n/iskusstvennyy-](https://cyberleninka.ru/article/n/iskusstvennyy)

intellekt-i-pravo-vyzovy-i-vozmozhnosti-samoobuchayuschih-sya-algoritmov (дата обращения: 10.09.2022).

2. Морхарт П. М. «Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы»: дисс. ... д-ра юрид. наук. Москва, 2018.

3. Калятин В. О. Объекты авторского права, созданные с использованием компьютера // Патенты и лицензии. Интеллектуальные права. 2011. № 5. С. 22–25.

4. Иоффе О. С. Основы авторского права. Авторское, изобретательское право, право на открытие: учебное пособие. Москва: Знание, 1969. С. 46.

5. Харитонов Ю. С. К вопросу об охраноспособности результата деятельности искусственного интеллекта // Право будущего: Интеллектуальная собственность, инновации, Интернет: Ежегодник. Вып. 1 / РАН. ИНИОН. Центр. социал. науч.-информ. исслед. Отд. правоведения; Каф. предпринимательского права МГУ им. М. В. Ломоносова; Отв. ред. Афанасьева Е. Г, место издания Москва, тезисы. С. 52–64.

6. Наумов В. Б., Тытюк Е. В. К вопросу о правовом статусе «творчества» искусственного интеллекта // Правоведение. 2018. Т. 62, № 3. С. 531–540. <https://doi.org/10.21638/11701/spbu25.2018.307>

У. В. Костылева,

Российский университет дружбы народов

ОСНОВНЫЕ ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ПРАВОСУБЪЕКТНОСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. Целью исследования является изучение основных подходов к определению правосубъектности искусственного интеллекта. Представлены основные подходы к определению понятия искусственного интеллекта, проанализированы взгляды о вероятности наделения искусственного интеллекта статусом физического, юридического или электронного лица, также уделено внимание правовому режиму вещи в контексте правового статуса искусственного интеллекта.

Ключевые слова: цифровое право, цифровые технологии, искусственный интеллект, ИИ, электронное лицо, правосубъектность искусственного интеллекта, ответственность искусственного интеллекта

THE MAIN APPROACHES TO DETERMINING THE LEGAL PERSONALITY OF ARTIFICIAL INTELLIGENCE

Abstract. The purpose of this research is to review the main approaches to determining the legal personality of artificial intelligence. The main approaches to the definition of the concept of artificial intelligence are presented, the possibilities of granting artificial intelligence the status of an individual, legal or electronic person are considered, attention is paid to the legal regime of a thing in the context of the legal status of artificial intelligence.

Keywords: Digital law, Digital technologies, Artificial intelligence, AI, Electronic person, Legal personality of artificial intelligence, Responsibility of artificial intelligence

Введение. Сегодня информационные технологии стали неотъемлемой частью общества, с каждым днем появляется все больше и больше систем, упрощающих нашу жизнь. Стремительно возрастающее значение приобретает и такой феномен современности, как искусственный интеллект (далее также – ИИ).

ИИ представляется одной из самых перспективных и потенциально применимой во всех сферах общественных отношений и вместе с тем наиболее противоречивой и несущей немало угроз технологической системой. Стремительное развитие таких универсальных, многофункциональных и способных оказывать значительное влияние технологий, принципиальная новизна общественных отношений, складывающихся в данной сфере и различные угрозы, связанные с применением технологий ИИ, обуславливают необходимость законодательного регулирования процесса разработки и применения искусственного интеллекта.

При этом ошибки машины или отсутствие регулирования ее действий в тех или иных областях представляют собой разной степени и разного рода угрозы. Так, например, использование беспилотных летательных аппаратов с фото- и видеофиксацией (квадрокоптеры и проч.) способно привести к обнаружению посторонними лицами засекреченных объектов, что может быть совершенно как ненамеренно, так и с корыстным и иным нехорошим умыслом. Это может создать угрозу национальной безопасности целой страны. С другой стороны, неверный машинный перевод всегда может быть исправлен специалистом в данной сфере. В одних случаях, требуется тщательный контроль над результатами деятельности ИИ, в других – законодательное регулирование их разработки и использования.

Такая необходимость также обосновывается и самой природой технологий искусственного интеллекта. Известно, что технологии ИИ неоднородны и неодинаковы, они все имеют определенную степень развития. Если считать, что слабый и средний ИИ всегда будут подчинены человеку и не смогут выйти за рамки заданной программы, а сильный ИИ в идеале будет способен к принятию самостоятельных решений и выполнению самостоятельных действий, то возникает вопрос об ответственности за его действия [10]. Исходя из этого, стоит сразу подчеркнуть, что в данной работе под ИИ будет пониматься система сложного искусственного интеллекта (super-AI), так как именно его решения и действия могут быть не подконтрольны человеку.

Под правосубъектностью мы понимаем способность кого-либо быть субъектом правоотношений, т. е. иметь определенные права и обязанности. Какими же правами и обязанностями, каким юридическим статусом можно наделить системы искусственного интеллекта? Близок ли он по своей природе к физическому лицу, или к юридическому лицу, или стоит вообще разработать отдельное понятие для такого специфического субъекта правоотношений и назвать его, скажем, электронным лицом? Таковы основные вопросы данной работы.

1. Определение понятия «искусственный интеллект». Не так давно в России появилось легальное определение термина «искусственный интеллект». В соответствии с Указом Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») (далее также Указ Президента РФ № 490), «искусственный интеллект – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений» [11].

Помимо легального определения данного понятия, в науке сформировались и иные точки зрения по данному вопросу. Так, известна позиция института статистических исследований и экономики знаний НИУ ВШЭ, где под искусственным интеллектом понимается система программных и/или аппаратных средств, способная воспринимать информацию с определенной степенью автономности, обучаться и принимать решения на основе анализа больших массивов данных, в том числе имитируя человеческое поведение [12].

Г. С. Осипов отмечал, что искусственный интеллект является предметом многих компьютерных наук, а создаваемые на его основе технологии представляют собой не что иное, как информационные технологии, позволяющие совершать не только разумные рассуждения, но и действия с помощью вычислительных систем и иных искусственных устройств [7].

Разумеется, это далеко не единственные подходы к определению данного понятия, но все они позволяют выделить общие существенные признаки искусственного интеллекта:

1. Искусственно созданная технология или система;
2. Способная к самообучению;
3. Созданная для принятия решений и осуществления определенных действий.

Дискуссия об определении правового статуса искусственного интеллекта ведется уже очень давно, однако однозначного ответа в доктрине так и не было представлено. Наиболее популярными с точки зрения относительно определения правового статуса ИИ являются:

- Наделение ИИ статусом физического лица.
- Наделение ИИ статусом юридического лица.
- Наделение ИИ статусом электронного лица.
- ИИ как техническое средство с правовым режимом вещи.

Разумеется, наделение ИИ статусом уже существующих субъектов (физического или юридического лица) не означает, что не должна приниматься во внимание специфика правовой природы искусственного интеллекта, а также

специфика ИИ как явления современности. Рассмотрим же подробно каждый из вариантов.

2. Искусственный интеллект как физическое лицо. Большинство исследователей сходятся во мнении, что ИИ не должен обладать правосубъектностью, схожей с правосубъектностью физического лица ввиду отсутствия у «мыслящей машины» таких существенных характеристик, как автономия, сознание и самосознание, а также сложное мышление и способность к коммуникации [3]. Невозможно говорить об ИИ как о личностях (в рамках правовых категорий – как о физических лицах) по той причине, что роботы (на сегодняшний момент их развития) не обладают таким существенным элементом жизнедеятельности, как воля, которая является обязательной для субъектов правоотношений.

Более того, наделение ИИ правосубъектностью физического лица будет предполагать наличие у него не только обязанностей, но и определенных прав. Интересен опыт некоторых зарубежных стран, в которых в отношении ИИ введен институт гражданства (подданства), – в 2017 г. робот София, разработанная гонконгской компанией Hanson Robotics, стала подданой Саудовской Аравии [9]. Данный случай является первым в своем роде. Здесь возникает некая «бомба замедленного действия», так как при наделении роботов такими (личными) гражданскими правами, как, например, право на самоопределение, право на личное достоинство и прочие, права роботов, созданных искусственно, неизбежно будут противопоставляться естественным правам человека, что сделает их равными юридически при фактическом неравенстве.

Таким образом, несмотря на все более возрастающее сходство между машинами и людьми, наделение юнита ИИ правосубъектностью человека (физического лица) представляется не только маловероятным, но даже, на наш взгляд, невозможным.

3. Искусственный интеллект как юридическое лицо. В своем исследовании П. М. Морхат упомянул, что можно допустить признание за юнитом ИИ правосубъектности юридического лица. Данный подход представляется более корректным ввиду основания его на условном принятии юридической фикции. Подобный метод позволит минимизировать какие-либо социальные потрясения и значительно упростит правовое регулирование некоторых взаимоотношений и видов деятельности. Тем не менее данный вариант имеет и существенные недостатки, в частности, в том, что сама суть юридического лица как организации и искусственного интеллекта различны – у юридического лица всегда есть люди, которые стоят за ним, есть органы управления, которые действуют от имени данного юридического лица, чего нельзя сказать о роботах, которые способны осуществлять самостоятельно лишь некоторые действия, не могут обладать деликтоспособностью и нести (пока что) какую-то ответственность [3].

4. Искусственный интеллект как электронное лицо. Данный вариант является наиболее вероятным и обсуждаемым, так как, во-первых, является гибридной формой субъекта права, которая сочетает в себе признаки юридического и физического лица (наиболее подходящие для ИИ их характеристики), а во-вторых,

соответствовал бы природе искусственного интеллекта как совершенно нового, не существовавшего ранее субъекта права, в связи с чем представляется целесообразным разработать для него новое понятие и статуса, который можно было бы гармонично и без ущерба вписать в существующую систему права.

В своей монографии П. М. Морхат предлагает ввести в оборот понятие «электронное лицо». Автор предлагает для него следующее определение: «обладающий некоторыми признаками юридической фикции (по аналогии с юридическим лицом) технико-юридический образ (в значении воспринимаемой и создаваемой третьими лицами целостной информационной проекции), отражающий, воплощающий и детерминирующий в юридическом пространстве конвенциально специфическую правосубъектность персонифицированного юнита искусственного интеллекта, обособленную от человеческого субстрата и гетерогенную (в части комплексов «прав» и обязанностей юнита) в зависимости от функционально-целевого назначения и возможностей такого юнита, и в силу этого аппроксимированный к конкретному целеполаганию производства и задействования такого юнита, т. е. его функционально-целевому назначению» [4].

Схожей точки зрения придерживается О. А. Ястребов – в своем исследовании он упоминает о доказанной возможности существования «принципиально нового механизма бытия» [13], что обосновывает создание нового юридического понятия, описывающего статус такого «механизма бытия». Автор предлагает ввести такую категорию лиц, как электронное лицо, и, прислушиваясь к идеям Г. Кельзена, трактует электронное лицо как «персонифицированное единство норм права, которые обязывают и уполномочивают искусственный интеллект (электронный индивид), обладающий критериями «разумности» [13. С. 15].

Однако помимо достаточно твердой и имеющей право на существование концепции электронного лица, существуют и такие подходы, которые не рассматривают ИИ не только как субъекта правоотношений, но и как их участника. Большинство современных исследователей убеждены в том, что искусственный интеллект – сложное техническое устройство с правовым режимом вещи. И такой подход имеет место быть.

5. Искусственный интеллект как техническое средство с правовым режимом вещи. Данный подход наиболее распространен в сфере цивилистики при определении автора результатов интеллектуальной деятельности. Вопросы о правосубъектности искусственного интеллекта в качестве электронного лица представлены на обсуждениях во Всемирной организации интеллектуальной собственности в качестве дискуссионных [2]. Р. О. Оморов проанализировал результаты данных обсуждений и сформулировал некоторые конкретные позиции по данному вопросу. Так, если мы говорим об ИИ как об инструменте, способствующем созданию объектов авторского права, то данные технологии приравниваются к электронно-вычислительным машинам. Если же мы говорим об ИИ как о системе, создающей определенные объекты ИС в автономном режиме, то авторское право должно отходить одушевленному субъекту – человеку или коллективу, разработавшему данную систему, при чем данный одушевленный субъект будет иметь статус субсубъекта с ограничением определенных авторских прав. К результатам

деятельности таких машин стоит применять особый режим авторско-правовой охраны (к примеру, сокращение срока правовой охраны) [6].

ВОИС также утвердила основные принципы регулирования в сфере искусственного интеллекта: во-первых, правовое обеспечение деятельности по созданию и развитию систем ИИ должно поощрять и стимулировать развитие современных технологий в данной области с введениями мер определенной ответственности. Во-вторых, подчеркивается роль ИИ как средства, усиливающего человеческий творческий потенциал и свобода человеческого творчества ставится прежде всего. Развитие инновационных технологий должно проходить для усилия человеческих возможностей [2].

Говоря об авторских правах искусственного интеллекта (или о потенциальном наделении ИИ авторскими правами), уместно упомянуть исследования В. Б. Нагродской, в которых она обозначает, что при определении автора результатов интеллектуальной деятельности сложились две абсолютно противоположные практики: немецкая, исключающая возможность правовой охраны интеллектуальной собственности, которая создана не человеком, и английская, тяготеющая к признанию автором лицо, которое со своей стороны предприняло все необходимые действия, достаточные для создания объекта авторского права [5].

Также подход к наделению ИИ статусом вещи можно найти на сайте проекта Робоправо, где находится проект федерального закона «О внесении изменений в Гражданский кодекс» Российской Федерации в части совершенствования правового регулирования отношений в области робототехники», подготовленный основателем инвестиционного фонда Grishin Robotics и сооснователем Mail.ru Group Дмитрием Гришиным [8].

Согласно данному документу предлагается ввести такие категории, как робот-агент и робот, причем оба из них рассматриваются как имущество, а их собственники и владельцы несут ответственность за их деятельность. Однако по некоторым причинам данный законопроект не был принят.

Помимо представленных выше подходов существует и еще один, имеющий не меньшее право на существование. Некоторые исследователи говорят об определении такого правового статуса систем ИИ, который содержал бы определенные запреты и ограничения, характерные и для ныне существующих лиц (к примеру, реализация избирательных прав). То есть речь идет о постепенном установлении отдельных элементов юридического статуса искусственного интеллекта. Так, по мнению Г. А. Гаджиева и Е. А. Войниканис, правосубъектность ИИ будет развиваться выборочно, постепенно добавляя в его статус отдельные права и возлагая отдельные обязанности, которых нет у некоторых граждан (например, неостребованные или опасные для жизни и здоровья населения должности или службы могут быть замещены только электронным лицом). Авторы считают, что в будущем возможно существование правового положения ИИ с ситуативным и смешанным статусом субъекта права [1].

Заключение. Таким образом, на сегодняшний день имеется огромное количество мнений относительно правосубъектности искусственного интеллекта – представленные выше подходы представляют собой далеко не исчерпывающий

их перечень. Разумно было бы отметить, что на сегодняшний день вопрос определения правового статуса искусственного интеллекта с тщательной проработкой всех аспектов такого статуса представляется невозможным, ввиду неустоявшейся практики по данным вопросам (в России и за рубежом), динамичному изменению отношений в данной сфере, еще не изученного влияния ИИ на науку и общество в целом и прочих факторов. Тем не менее необходимость такого регулирования превалирует над всеми этими тонкостями, которые важно принимать во внимание. В данной ситуации «что-то» лучше, чем «ничего», поэтому постоянное изучение и анализ имеющихся и вновь возникающих данных, умение верно их интерпретировать и преобразовывать в подходящие обществу правовые нормы – ключ к успешному формированию комплексной системы законодательства об искусственном интеллекте и роботехнике.

Список литературы

1. Гаджиев Г. А., Войниканис Е. А. Может ли робот быть субъектом права (Поиск правовых форм для регулирования цифровой экономики)? // Право. Журнал Высшей школы экономики. 2018. № 4. С. 24–48.
2. Дискуссия ВОИС на тему «Интеллектуальная собственность (ИС) и искусственный интеллект (ИИ)»: второй раунд (2019) // WIPO/IP/AI/2/GE/20/1, 13 декабря. URL: https://www.wipo.int/meetings/ru/details.jsp?meeting_id=55309 (дата обращения: 12.08.2022).
3. Морхат П. М. Правосубъектность юнита искусственного интеллекта: некоторые гражданско-правовые подходы // Вестник КГУ. 2018. № 3.
4. Морхат П. М. Правосубъектность юнитов искусственного интеллекта. Гражданско-правовое исследование. Москва: ЮНИТИ-ДАНА, 2018. 113 с.
5. Нагродская В. Б. Новые технологии (блокчейн / искусственный интеллект) на службе права: научно-методическое пособие / под ред. Л. А. Новоселовой. – Москва: Проспект, 2019.
6. Оморов Р. О. «Интеллектуальная собственность и искусственный интеллект» // E-Management, vol. 3, no. 1, 2020. С. 43–49.
7. Осипов Г. С. Искусственный интеллект: состояние исследований и взгляд в будущее // Новости искусственного интеллекта. 2001. № 1. С. 3–13.
8. Официальный сайт Исследовательского центра проблем регулирования роботехники и искусственного интеллекта, проект «РОБОПРАВО». URL: <https://robopravo.ru/> (дата обращения: 12.08.2022).
9. Российское информационное агентство ТАСС. URL: https://tass.ru/ekonomika/4680400?utm_source=ru.wikipedia.org&utm_medium=referral&utm_campaign=ru.wikipedia.org&utm_referrer=ru.wikipedia.org (дата обращения: 12.08.2022).
10. Рязанов, С. И. Искусственный интеллект как множество – классификация искусственных интеллектов / С. И. Рязанов // Вузовская наука в современных условиях: сборник материалов 54-й научно-технической конференции: в 3 ч., Ульяновск, 27 января 2020 года. Ульяновск: Ульяновский государственный технический университет, 2020. С. 72–75.

11. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собрание законодательства Российской Федерации № 41 от 14.10.2019, ст. 5700.

12. Что такое цифровая экономика? Тренды, компетенции, измерение: докл. к XX Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 9–12 апр. 2019 г. / Г. И. Абдрахманова, К. О. Вишневский, Л. М. Гохберг и др.; науч. ред. Л. М. Гохберг; Нац. исслед. ун-т «Высшая школа экономики». – Москва: Изд. дом Высшей школы экономики, 2019.

13. Ястребов О. А. Правосубъектность электронного лица: теоретико-методологические подходы // Труды Института государства и права РАН. – 2018. – № 2. – С. 6.

А. О. Кочетова,
студент,

Самарский государственный университет путей сообщения

С. А. Сарычева,
студент,

Самарский государственный университет путей сообщения

ПАТЕНТНОЕ ПРАВО В ЦИФРОВОЙ СРЕДЕ

Аннотация. В статье рассмотрено понятие цифровых технологий, перечислены основные их виды и типы, обозначены сферы применения цифровых разработок. Проанализированы преимущества и недостатки цифровых технологий в аспекте правового регулирования интеллектуальных прав в России. Выделены требования, которые необходимо выполнить для получения патента. Изложены особенности получения патента на изобретение.

Ключевые слова: технология, цифровизация, искусственный интеллект, разработка, патент, авторское право

PATENT LAW IN THE DIGITAL ENVIRONMENT

Abstract. The article considers the concept of digital technology, lists the main types of digital technologies. The areas of application of digital developments are also given. An analysis of the advantages and disadvantages of digital technologies has been carried out. In addition, the legal regulation of intellectual property rights in Russia is considered. The requirements that must be met to obtain a patent are highlighted. The features of obtaining a patent for an invention are also described.

Keywords: Technology, Digitalization, Artificial intelligence, Development, patent, Copyright

Введение. Развитие цифровых технологий непосредственно связано с прогрессом во всех областях жизнедеятельности человека. Ведь развитие технологий не имеет границ. На сегодняшний день жизнь человека трудно представить

без использования цифровых разработок, так как у каждого имеются различные цифровые приборы: компьютеры, смартфоны, планшеты. Тем самым общество использует технику для реализации конкретных заданий. Развитие цифровых технологий позволит упростить решение различных задач во всех сферах жизни общества.

Цифровые технологии – разработки, которые сформированы благодаря использованию технических средств, имеющих собственное программное обеспечение [3].

Основные виды цифровых технологий (рис. 1):

1. Искусственный интеллект. Искусственный интеллект использует в своей системе те способы, которые позволяют имитировать поведение человека.

Оперируя информацией о способностях интеллекта и понимании процесса обучения, машина имеет способность запоминать эти данные, а также может воспроизводить их [4].

Существуют следующие группы искусственного интеллекта:

- 1) искусственный интеллект с ограничениями – предназначен для решения определенной цели или задачи;
- 2) общий искусственный интеллект с ограничениями – предназначен для выполнения многих целей или задач, по работоспособности похож на человеческий мозг;
- 3) сверхразумный искусственный интеллект – вычислительная сила машины превосходит интеллект человека.

Для искусственного интеллекта существует машинное обучение, которое обучает машину и предоставляет данные для обучения и запоминания. Во время обучения машина, например, может научиться распознавать образы (нейросеть).

Также используют вид «Глубоко машинного обучения», позволяющий использовать нейронные сети, чтобы решать определенные реальные задачи. Этот вид характеризуется тем, что машина начинает имитировать поведение человека в процессе принятия им решений.

2. Компьютерное зрение – это отрасль искусственного интеллекта, отвечающая за обработку информации с видео или фотографий, компьютер находит и извлекает информацию из представленных материалов, учится отслеживать необходимые объекты, классифицировать информацию.

3. Нейросеть – программа, которая построена на математической модели, функционирующая как нейронные сети. Данная программа позволяет создавать прогнозы, распознавать и производить поиск различной информации [1].

4. Блокчейн и криптовалюты. Блокчейн – это совокупность блоков с информацией, связанных друг с другом и выстроенных в определенном порядке. Каждый из блоков содержит свою собственную хеш-сумму, а также хеш-сумму предыдущего блока, но если изменить информацию в блоке, то его хеш-сумма тоже изменится.

Криптовалюта – валюта, находящаяся в цифровой среде, количество которой можно определить, если рассмотреть объем расчетных единиц, находящихся в информационном пакете протоколов для передачи данных.

5. Интернет вещей – совокупность устройств, подключенных к сети интернет, которые могут взаимодействовать с внешним миром и друг с другом. Состоят из датчиков, которые следят за определенными параметрами, и разветвленной сети устройств для хранения и передачи данных [6].

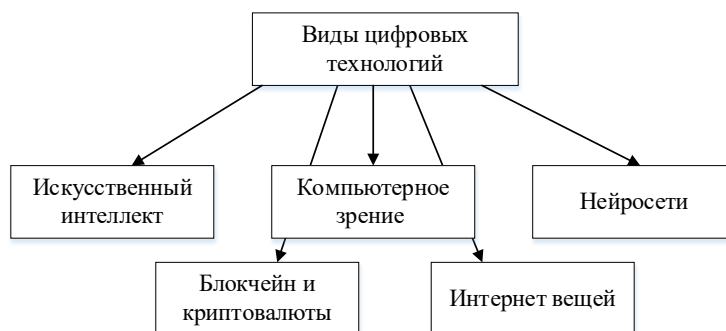


Рис. 1. Виды цифровых технологий

Области применения цифровых технологий:

- Онлайн-сервисы – используются для удаленной работы, хранения данных и управления ими. Данные сервисы можно использовать без скачивания, что является их преимуществом.

- В образовательной среде применяют технику и приложения для того, чтобы учащиеся могли обучаться дистанционно, а также для решения творческих задач, создания презентаций. Данный метод позволяет ученикам быстрее осваивать изученную информацию.

- В медицинской сфере технологии позволяют оперативно находить необходимые лекарства, формировать заказ медикаментов, следить за базой, также позволяет определять диагноз на раннем сроке, заниматься сбором информации с последующим прогнозом болезней, проводить онлайн-консультацию у специалиста, а также использовать роботов во время операции.

- В ритейле поиск и покупка товара становится значительно проще с использованием искусственного интеллекта, также можно управлять и отслеживать доставку. Позволяет оптимизировать пространство внутри магазина с помощью проведения анализа на предмет выявления поведения и перемещения клиента. Магазины, которые работают без касс и консультантов, благодаря технологиям функционируют с системой распознавания лиц, а голосовые помощники помогают обрабатывать запросы с минимальным временем для удобства и экономии времени покупателя.

- На производстве технологии без участия человека могут управлять целыми заводами, создавать новые материалы, обеспечивать охрану за окружающей средой и безопасностью предприятия, оптимизировать рабочее время, следить за состоянием оборудования, предотвращать брак.

- В сфере быстрого питания технологии помогают в выборе товаров, формировании заказа, распределении приоритетов приготовления блюд, также ведут контроль над состоянием продуктов, помогают в поиске точек с высокой проходимостью.

Положительные стороны применения цифровых технологий:

- в двоичной системе минимизируется риск потери информации или ее изменения;
- данные можно сохранять на длительное время, а также данные сохраняются без помех;
- специально созданные программы позволяют сделать процесс управления устройствами более упрощенным;
- цифровые технологии могут применять сложные алгоритмы, которые обладают высокой точностью реализации;
- полученные данные можно оцифровывать, тем самым данные занимают небольшое пространство.

Отрицательные стороны:

- некоторые элементы процессов являются энергозатратными, это приводит к усложнению устройства;
- если при передаче информации будет утерян смысл одного элемента, то смысл сообщения изменится.

В нашей стране цифровыми технологиями пользуются активно, но цифровые стандарты практически не используются, по этой причине возникают проблемы в области патентного права. Важным направлением развития государства является урегулирование проблем в сфере защиты объектов интеллектуальной собственности [2].

В кодексе Российской Федерации представлена совокупность способов защиты патентных прав. Регулирование интеллектуальной собственности (ИС) на правовой основе имеет отношение к комплексному законодательству, состоящие из нескольких норм права, таких как гражданское, административное, уголовное. Существует два способа защиты интеллектуальных прав – с помощью государственных органов (палата по патентным спорам, суд, федеральная антимонопольная служба) и самозащита. Самозащита реализуется путем передачи извещения о нарушении прав человеку, который совершил правонарушение.

Предприятия или частные лица имеют возможность приобрести исключительные права на изобретения или творческие результаты только благодаря праву на интеллектуальную собственность. Если владелец фирмы владеет несколькими интеллектуальными активами, то это позволяет ему быть в более преимущественном положении перед конкурентами. Патентное ведомство занимается деятельностью, которая направлена на поощрение изобретательской активности. Также ведомство стимулирует людей, занимающихся разработками, на открытие собственных технических решений в обмен на обеспечение исключительными правами на патент [5].

Для того чтобы получить патент на интеллектуальную собственность необходимо выполнить следующие требования: разработка должна иметь новизну и изобретательский статус. Однако процедура регистрации является продолжительной – минимальное время подтверждения изобретения один год. Но для некоторых изобретений устанавливаются индивидуальные условия регистрации, что обуславливается важностью разработки.

Патентная система в данный момент имеет совокупность ограничений, которые мешают изобретательской деятельности предприятий. Для того чтобы получить патент, необходимо объяснить суть разработки и область применения. Данный этап является рискованным, так как конкуренты могут скопировать идею и модернизировать разработку.

Также разработка может попасть под влияние патентных организаций, которые имеют портфель патентов и не обладают собственным производством. Такие предприятия имеют в своем составе команду юристов, которые специализируются на патентном праве. Данная организация владеет большим объемом патентов и подает иски на тех людей или предприятия, которые пользуются попытками применения похожих разработок на практике [7].

Особенность патентования цифровых технологий заключается в том, что программное обеспечение имеет статус авторского права при реализации современных технологий – это является причиной исключения таких технологий из объектов, которые можно запатентовать. Охране авторского права принадлежит исходный код, а не само его содержание, вследствие чего предприятия конкуренты имеют возможность переделать защищенный код с целью обхода защиты авторских прав. Именно по этой причине предприятия заинтересованы в охране созданного программного обеспечения в статусе изобретения, так как это позволит защитить содержание разработки. Для этого предприятию необходимо объяснить новую научно-техническую идею разработки с использованием технических средств для решения конкретизированной технической задачи.

Заключение. Для развития государства и сферы жизнедеятельности человека необходимо постоянно разрабатывать новейшие научно-технические решения, которые будут продвигать технологии на высокий уровень. Цифровые технологии в наше время позволяют человеку решать многочисленные задачи за минимальное количество времени. Развитие цифровых технологий приводит к созданию новых устройств и технологий, поэтому необходимо также модернизировать правовую охрану объектов интеллектуальной собственности.

Список литературы

1. Гохберг Г. С., Короткин А. А., Зафиевский А. В. Информационные технологии // Учебное пособие. – 9-е изд., перераб. и доп. – Москва: Издательский центр «Академия». – 2014. – 240 с.
2. Даниленков А. В. Интернет-право: научная литература. – Москва: Юстицинформ. – 2014. – 232 с.
3. Машевская О. В. Цифровые технологии как основа цифровой трансформации современного общества // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. – 2020. – № 1. URL: <https://cyberleninka.ru/article/n/tsifrovye-tehnologii-kak-osnova-tsifrovoy-transformatsii-sovremennogo-obschestva/viewer> (дата обращения: 25.07.2021).
4. Потапов А. С. Технологии искусственного интеллекта // Учебное пособие. – Санкт-Петербург: СПбГУ. – 2010. – 218 с.

5. Рожкова М. А. Интеллектуальная собственность: основные аспекты охраны и защиты: учебное пособие. – Москва: Проспект. – 2014. – 248 с.

6. Сарычева С. А., Кочетова А. О. Разработка комплекса лабораторных работ по технологиям компьютерных сетей для изучения передачи пакетной информации // Дни студенческой науки: Сборник материалов 49-й научной конференции обучающихся СамГУПС, Самара, 05–16 апреля 2022 года. – Самара: Самарский государственный университет путей сообщения. – 2022. – С. 141–145.

7. Савельев А. И. Правовая природа «облачных» сервисов: свобода договора, авторское право и высокие технологии // Вестник гражданского права. – 2015. – № 5. – С. 99.

Ю. А. Кошлыкова,
магистрант,

Южный федеральный университет

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ 3D-ТЕХНОЛОГИЙ ДЛЯ РЕШЕНИЯ КРИМИНАЛИСТИЧЕСКИХ ЗАДАЧ

Аннотация. В статье рассматриваются некоторые направления использования 3D-технологий в процессе раскрытия и расследования преступлений. С практической точки зрения оценивается эффективность 3D-сканирования и 3D-моделирования для фиксации обстановки места происшествия и обнаруженных в ходе ее осмотра следов, при проведении баллистических исследований, для совершенствования современных систем идентификации личности. Оцениваются проблемы их применения и определяются перспективы развития.

Ключевые слова: криминалистика, криминалистическая техника, 3D-технологии, 3D-моделирование, трасология, след, фиксация, изъятие, баллистика, идентификация

POSSIBILITIES OF USING 3D TECHNOLOGIES TO SOLVE FORENSIC PROBLEMS

Abstract. The article discusses some areas of the use of 3D technologies in the process of detection and investigation of crimes. From a practical point of view, the effectiveness of 3D scanning and 3D modeling is evaluated for fixing the situation of the scene of the accident and traces found during its inspection, during ballistic studies, for improving modern identification systems. The problems of their application are evaluated and the prospects for development are determined.

Keywords: Criminalistics, Forensic technology, 3D technologies, 3D modeling, tracology, Trace, Fixation, Seizure, Ballistics, Identification

3D-технологии в настоящее время прочно вошли в повседневную жизнь человечества. Трехмерное моделирование широко применимо как в бытовой сфере (3D-визуализация интерьеров, развлекательная индустрия), так и в промышленности (проектировка зданий, автомобилей), и в большом количестве научных ис-

следований (медицина, археология, биология, экология и т. д.). Одной из сфер, в которых задействование 3D-технологий представляется достаточно результативным, является и криминалистика.

Преимущества включения устройств 3D-сканирования в оснащение криминалистов очевидны. Современные технологии позволяют создать наиболее точную и максимально приближенную к оригиналу модель любого о вещественного объекта. Для задач криминалистики это имеет первостепенное значение, так как объективное отражение следов крайне важно для их дальнейшего исследования и, как следствие, сыграет значительную роль для расследования и разрешения конкретного уголовного дела [6. С. 90–93]. Если раньше построение 3D-моделей требовало особых знаний и навыков, то в настоящее время данные процессы значительно упрощены: 3D-сканеры портативны и довольно просты в использовании, виртуальные 3D-модели создаются в специальных программах, адаптированных для использования лицами, не имеющими профессионального IT-образования.

Наиболее продуктивным представляется использование 3D-технологий в процессе работы со следами на месте происшествия. Нами было проведено исследование (обнаруженный на условном месте происшествия след обуви был отсканирован, виртуально воспроизведен в программном обеспечении и напечатан на 3D-оборудовании), в рамках которого мы на практике подтвердили преимущества 3D-технологий над традиционными методами работы со следами [7. С. 28–31].

Преимущества применения данного метода были очевидны: быстрота, экономия материалов, наглядность и точность [5. С. 929–934]. Данное исследование было направлено на изучение возможностей изъятия объемных следов, но использованная техника, на наш взгляд, актуальна для любого их вида. Любой объемный след можно с легкостью отсканировать 3D-сканером и преобразовать в специальной программе в набор точек, лежащих на трехгранной координатной плоскости по примеру нашего исследования (рис. 1).

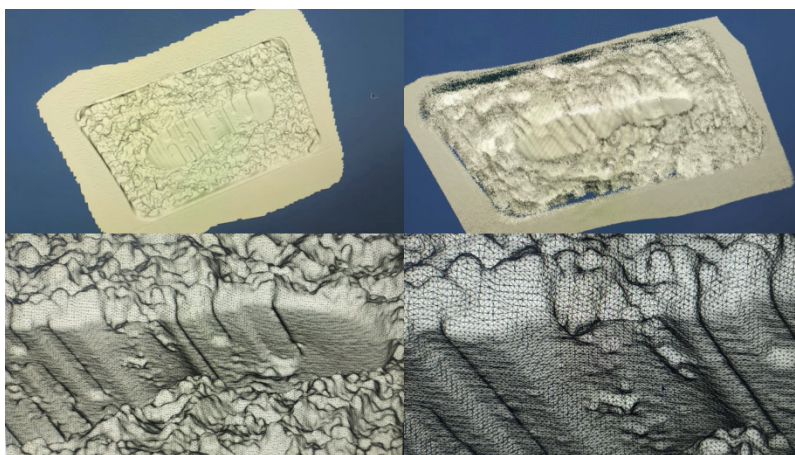


Рис. 1. Отсканированная и перенесенная в программу модель отпечатка подошвы

Сканирование осуществляется с очень высокой степенью точности – на экран выводится огромное количество пространственных точек считанной сканером поверхности. По каждой из полученных точек с математической точностью можно отследить координаты и иные пространственные характеристики, но для решения криминалистических задач достаточно точной фиксации изображения объекта для дальнейшего исследования. При работе с поверхностными следами сканирование происходит по аналогичному алгоритму, за исключением одного нюанса: уместнее будет преобразовывать считанную 3D-сканером информацию в двухмерное изображение. Несмотря на то, что сканер может зафиксировать даже высоту микроскопической полости, образовавшейся при оставлении отпечатка пальца на пыльной поверхности, для целей криминалистики в большей степени здесь будет иметь значение обычное качественное изображение отпечатка пальца, а 3D-модель, безусловно, в силу бесконтактного сканирования, будет представлять гораздо более точный результат фиксации, чем если бы отпечаток пальца был изъят традиционным методом с помощью специального порошка и дактилоскопической пленки. Таким образом, на наш взгляд, процесс следокопирования можно значительно облегчить задействованием технологий 3D-моделирования вне зависимости от вида изымаемых следов.

3D-технологии также могут быть результативно использованы в процессе проведения баллистических исследований [2. С. 34–41]. В данном случае применяется немного иная технология, чем при фиксации следов портативным сканером: пуля либо гильза фиксируется в стационарном состоянии, через микроскоп на объект пропускаются световые лучи стационарного 3D-сканера, работающего на основе модулированного света, и по интенсивности отражаемого света фиксируется глубина отметин на объекте [4]. Далее в программном обеспечении генерируется 3D-модель боеприпаса, позволяющая изучить все существенные детали. Данная методика в сравнении с изъятием следов представляет собой средство технологической экономии. Если для достоверной идентификации по отпечатку пальца нам необходимо зафиксировать его в мельчайших деталях, то в баллистике изучаемые объекты в виде пуль и гильз идентифицируются принадлежностью к конкретному виду оружия, и в рамках исследования ценность представляет именно изучение деформаций, образовавшихся в результате выстрела. Таким образом, в программе должны фиксироваться конкретные данные об объекте, а сведения о повреждениях будут транслироваться по итогам указанного упрощенного процесса сканирования. Достоверность расположения считываемых точек в данном случае также довольно высока, соотношение координат варьируется от десятков до сотен микрометров, что также делает данный способ фиксации наиболее передовым и результативным.

Перспективной представляется и возможность создания на основе одной фотографии трехмерного изображения внешности человека, которая позволяет сделать более эффективным поиск лиц, уже находящихся в различных базах данных (как правило, это 2D-изображения) по их трехмерным изображениям, имеющимся в системах распознавания лиц, являющихся частью современных

систем безопасности. Исследование крупномасштабной 3D-реконструкции лица по одному изображению с помощью прямой объемной регрессии было представлено на Международной конференции по компьютерному зрению (ICCV) 2017 в Венеции. Исследовательская группа «обучила» Convolutional Neural Network (CNN – в адаптированном переводе «сверточная нейронная сеть») огромному набору данных из 2D-изображений и 3D-моделей лица. Обладая всей этой информацией, CNN может реконструировать 3D-геометрию лица по одному 2D-изображению. В рамках этой же технологии возможно воссоздать 3D-модель лица даже в том случае, если какая-то его часть не видна на снимке (солнцезащитные очки, медицинская маска). Единственное препятствие – данное лицо уже должно содержаться в какой-либо базе данных, с которыми будет сравниваться считанное изображение и, как следствие, реконструироваться новое. Пока практические результаты исследования не имеют обширного применения, но 3D-реконструкция и сегментация, применяемые к человеческому лицу и телу, могут быть успешно внедрены в современные идентификационные системы.

Но наиболее значимым прорывом в криминалистике, на наш взгляд, будет возможность воссоздания с помощью технологий 3D-моделирования полноценной картины места происшествия. Запротолировать все детали зачастую сложно, во-первых, потому, что вербализованная информация не всегда может объективно и точно передать сложившуюся ситуацию, а, во-вторых, если место происшествия имеет довольно обширную площадь, достоверно описать все в протоколе будет крайне затруднительно. Правоохранительные органы некоторых стран еще в конце прошлого века делали вещественные модели мест происшествий. Например, в Гонконге с 1988 г. существует подразделение полиции, осуществляющее, при необходимости, изготовление макетов вручную. Так, в 2011 г. специалистам этого подразделения пришлось воссоздать в миниатюре целый жилой квартал после пожара, унесшего девять жизней. Следователи потребовали исключительной точности вплоть до детализации телефонных будок с тем, чтобы свидетели легко ориентировались и давали точные показания. Естественно, как только современные технологии позволили воссоздавать 3D-модели объектов, полиция Гонконга незамедлительно внедрила данные методы в свою деятельность [3. С. 305–310]. К 2017 г. практика воссоздания детализированных 3D-макетов мест происшествий уже активно использовалась в качестве наглядных пособий в рамках рассматриваемых дел.

На наш взгляд, в Российской Федерации сканирование обширного пространства для целей правоохранительных органов пока не получило масштабного развития в силу ряда обстоятельств: высокой стоимости оборудования для комплексного 3D-моделирования, отсутствия необходимого количества специалистов, несовершенства необходимого функционала 3D-сканеров. И если возможности решения технических задач имеются (например, совершенствование диапазона считывания стационарного 3D-сканера: увеличения подлежащего достоверному сканированию расстояния и расширения угла фиксации), то для разрешения

других указанных выше проблем требуется гораздо больше времени и ресурсов [1. С. 287–291]. Внедрение таких устройств в техническое оснащение криминалистов позволило бы в разы более быстро и точно фиксировать информацию обо всех необходимых деталях места происшествия и значительно облегчило бы процесс раскрытия и расследования преступлений.

На основании всего вышесказанного можно сделать вывод, что использование современных 3D-технологий действительно имеет значительную ценность для решения криминалистических задач.

Список литературы

1. Золотова Ю. А. Использование 3D-технологий и технологий виртуальной реальности при осмотре места происшествия // Следственная деятельность: проблемы, их решение, перспективы развития: материалы IV Всероссийской молодежной научно-практической конференции, Москва, 30 ноября 2020 года. – Москва: Московская академия Следственного комитета Российской Федерации, 2020. – С. 287–291.

2. Кокин А. В. 3D-оружие и перспективы его криминалистического исследования // Теория и практика судебной экспертизы. – 2017. – Т. 12, № 2. – С. 34–41.

3. Кочкина О. В., Тябина Ю. А. Опыт Гонконга в области кибербезопасности и технологических преступлений // Научные труды ФКУ НИИ ФСИН России: Научно-практическое ежеквартальное издание. – Москва: Федеральное казенное учреждение «Научно-исследовательский институт информационных технологий Федеральной службы исполнения наказаний», 2021. – С. 305–310.

4. Курбанаева Э., Степанова И., Чепрасов М. Значение 3D-технологий в науке «Криминалистика» // Вестник казахско-русского международного университета. – 2015.

5. Маннова А. А., Рожкова В. Р. 3D-сканер: инновации в области криминалистики // Вопросы российской юстиции. – 2019. – № 3. – С. 929–934.

6. Мордюк А. В., Скороходова А. А. 3D-технологии в криминалистике // Защита прав человека в периоды внешнеполитической напряженности: материалы международной научно-практической конференции, Саранск, 19 апреля 2019 года / Средне-Волжский институт (филиал) ВГУЮ (РПА Минюста России). – Саранск: Б. и., 2019. – С. 90–93.

7. Фролова Е. Ю., Кошлыкова Ю. А. Перспективы применения 3D-технологий для фиксации и изъятия следов на месте происшествия // Эксперт-криминалист. – 2021. – № 4. – С. 28–31.

А. В. Кулагина,

студент,

Московский государственный университет имени М. В. Ломоносова

ПОНЯТИЕ АЛГОРИТМИЗАЦИИ И ЕЕ ВЛИЯНИЕ НА СФЕРУ ТРУДА

Аннотация. В статье рассматривается понятие алгоритмизации и ее проявления в трудовом праве. Анализируются возникновение и распространение алгоритмических процессов в сфере труда, их влияние на современных работников и работодателей в условиях постоянной трансформации экономики. Делается вывод об упрощении выполняемых задач и повышении эффективности производства при наличии значительных нарушений законных интересов обеих сторон трудовых правоотношений и необходимости правового регулирования новых технологий.

Ключевые слова: трудовое право, автоматизация, алгоритмизация, цифровые навыки, гиг-экономика, безработица, персональные данные

THE CONCEPT OF ALGORITHMIZATION AND ITS IMPACT ON THE SPHERE OF WORK

Abstract. The article considers the concept of algorithmization and its manifestation in labor law. The author analyzes the emergence and spread of algorithmic processes in the field of labor, their impact on modern workers and employers in the constant transformation of the economy. The conclusion is made about the simplification of performed tasks and increasing of production efficiency in the presence of significant violations of the legitimate interests of both parties of labor legal relations and the need for legal regulation of new technologies.

Keywords: Labor law, Automation, Algorithmization, Digital skills, Gig economy, unemployment, Personal data

Важной и значимой чертой текущей цифровой трансформации экономики и общества, безусловно, является алгоритмизация, обеспечивающая быструю и корректную обработку большого объема данных. Именно она меняет условия труда работников и производственные процессы в целом, взывая к неизбежности обновления норм трудового права. Исполняя работу с применением особых приложений для компьютера и находясь под управлением систем с элементами искусственного интеллекта, работники и работодатели тем самым включаются в «цифровую среду». Под алгоритмом следует понимать «совокупность инструкций, позволяющих решить проблему и достичь определенного заданного результата, отвечающих концепции надлежащего, качественного государственного управления» [8. С. 25].

Что же касается алгоритмизации в сфере труда, то ее можно определить, как «описание очередности выполнения различных операций через создание блок-схем, пошагово описывающих процедуры, процессы трудоустройства, привлечения к дисциплинарной и материальной ответственности, расследования несчастных случаев на производстве, разрешения коллективных трудовых споров, создания локальных нормативных актов» [13. С. 12–14].

Если обратиться к предыстории и мнениям ученых, то американский экономист Дж. Рифкин в своих трудах опирается на статистику сокращений рабочих мест и снижение реальных доходов населения с 1980-х гг. из-за влияния автоматизации [23. Р. 176]. Можно также добавить, что эксперты выделяют три промышленные революции, радикально преобразившие облик и сущность трудовой деятельности. Их основными этапами представляются индустриализация (иными словами, переход от ручного труда к машинному), электрификация и автоматизация (внедрение вычислительной техники в производство, отрасли обслуживания населения и процессы управления). Нынешнее состояние мировой экономики символизирует начало четвертой промышленной революции, характеризующейся повышением гибкости и результативности производства, уменьшением издержек, вызванных человеческим фактором, передачей принятия однотипных решений нейросетям.

Более того, согласно докладу ЮНКТАД (Конференция ООН по торговле и развитию), ключевыми изменениями в сфере труда во время четвертой промышленной революции станут: появление новых профессий одновременно с исчезновением отдельных видов деятельности, радикальное изменение условий труда (удаленная работа, работа посредством платформ), требования к знанию и улучшению цифровых навыков (*digital skills*) [14. С. 31–35].

Углубляясь в детали введения в жизнь алгоритмизации, стоит отметить, что она подразделяется на несколько этапов, среди которых: предварительный анализ задач, теоретическое и экспериментальное определение статических и динамических характеристик процесса, моделирование, анализ полученной математической модели и выработка рекомендаций [15. С. 28]. Развивая мысль о совершенствовании алгоритмов и извлечении максимальной выгоды из их использования, имеет смысл говорить о двух типах алгоритмов машинного обучения: контролируемых и неконтролируемых. Первый тип формирует обучающий набор данных с ответами, направленных на создание модели, которая сможет правильно распознавать ранее незнакомые данные. Неконтролируемые же алгоритмы модернизируются без вмешательства человека с помощью беспрестанной корректировки параметров своих моделей на базе предшествующих операций.

Описываемая способность быстро и эффективно использовать цифровые ресурсы станет значимым условием конкурентоспособности и трансформации рынка труда. Техническая инфраструктура платформ упрощает сделки между многими производителями по низкой цене и приводит к появлению «гиг-экономики» с рабочей силой по требованию [17]. Что же понимается под этим понятием? Его ввела журналистка Тина Браун и определила, как «нетипичную работу, которая состоит из свободно плавающих проектов, консультаций и частичной занятости» [22]. Применение алгоритмического управления в такой экономике для приложений и платформ может влиять на поведение и самостоятельность и степень контроля, оказываемого на поведение работников [20. Р. 5]. По сравнению с «традиционной» экономикой «гиг-экономика» представляет собой очень гибкий механизм и для работников, и для работодателей. Но в то же самое время в новом типе экономики причудливо соединяются умеренная степень свободы и точный контроль алгоритмов.

Об активном внедрении процессов алгоритмизации можно говорить уже сейчас. Например, в России в начале 2020 г. в Трудовой кодекс были внесены положения, предусматривающие электронный формат трудовых книжек, а с мая 2020 г. был разрешен перевод всей документации, касающейся трудовых отношений, в электронный вид пока что в качестве правового эксперимента для отдельных работодателей [9]. Помимо этого, было положено начало созданию информационно-аналитической системы – Общероссийской базы вакансий «Работа в России». Данная система на основе алгоритмов предоставляет информацию о вакансиях в электронной форме как соискателям, так и работодателям, желающих найти новых работников [1. С. 16–18]. За рубежом цифровизация также динамично влияет на структуру рынка труда. К примеру, компания Boeing стала использовать на треть меньше работников, чем 30 лет назад, при этом производство самолетов увеличилось на 20 %. Повышение эффективности стало возможным благодаря использованию роботов, снизивших затраты предприятия и процент брака и ошибок на две трети [15. С. 43]. Те, работодатели, которые уже начали применять алгоритмизационный менеджмент, т. е. передачу управленческих решений алгоритмам, освободились от постоянного мониторинга за деятельностью и эффективностью сотрудников, а также получают больше данных.

Несмотря на кажущуюся радужность и высокие показатели эффективности упомянутых средств, они несут серьезную угрозу для работников и структуры рынка труда. Это обусловлено тем, что новые революционные методы, внедряемые в производство, освобождают работников от монотонного и рутинного умственного труда, тем самым заменяя их на определенной должности и способствуя увеличению количества безработных. Согласно исследованию компании McKinsey, к 2030 г. около 14 % рабочей силы лишится своей работы, а их функции будут выполняться с помощью цифровых технологий, а примерно 50 % рабочих мест могут быть автоматизированы [21]. Данное явление описывается термином «технологическая безработица». Если обратиться непосредственно к представителям юридических профессий, то согласно анализу профессоров Оксфордского университета [19. Рр. 254–280], статистика весьма неутешительна: практически 98 % ассистентов и помощников юристов, а также около половины судебных репортеров потеряют рабочие места. Их трудовые обязанности будут выполнять алгоритмами, приложениями и искусственным интеллектом.

Тем не менее есть и иная точка зрения, отстаивающая утверждение о том, что введение новых технологий не только вытесняет работников, но в то же время создает большой резерв рабочей силы. Так, компания Amazon заявила о намерении создать почти 100 000 новых рабочих мест в США, в основном это будут разработчики ПО, так и сотрудники склада [2]. Кроме того, специалисты McKinsey утверждают, что пока в профессиях, основывающихся на креативности, умении оценивать эмоциональные реакции и построения социального взаимодействия новые технологии не в состоянии заменить человека.

Самой главной проблемой сопутствующей алгоритмизации труда в трансформирующейся экономике является недостаточность или вовсе полное отсут-

ствии так называемых цифровых навыков (digital skills) у работников. Чаще всего под этим понятием рассматривается уверенное пользование техникой и цифровыми устройствами, знание современных методологий и принципов управления проектами, аналитические способности, позволяющие обрабатывать большие объемы информации, общение с помощью цифровых каналов и, наконец, умение быстро и оперативно реагировать на изменения обстоятельств и адаптироваться к ним без ущерба производству. Согласно исследованию компании Deloitte, почти 60 % работодателей считают, что работники не обладают достаточными для цифровой экономики навыками даже после получения профессионального образования. В этой ситуации главам компаний придется решать самостоятельно, нанимать ли новых сотрудников или обучать существующий персонал [12].

Учитывая довольно небольшой промежуток времени, в течение которого алгоритмы возникли и активно проникли во все сферы жизни, логично предположить, что на данный момент отсутствует единый международно-правовой документ, унифицирующий и стандартизирующий законодательные положения о цифровизации общества.

Одним из важных вопросов является соотношение принципов трудового права с последними тенденциями распространения цифровых технологий. Эти принципы закреплены в Декларации Международной организации труда «Об основополагающих принципах и правах в сфере труда» от 18.06.1998. Так, уже сейчас ставится вопрос о необходимости всеобщих трудовых гарантий (universal labour guarantee), другими словами, социальной защиты с рождения и до старости, а также права на непрерывное образование из-за возможных ограничений и нарушений, вызванных цифровизацией и алгоритмизацией [26]. А также обсуждается обязанность работодателей уведомлять работников о введении систем искусственного интеллекта в рабочий процесс, что указывается в решениях федеральных окружных судов США и Национального управления по трудовым отношениям.

Что касается российской нормативной базы, то единый кодекс или федеральный закон, регулирующий цифровую трансформацию экономики и права, на настоящий момент отсутствует. Однако в России в течение нескольких лет усматривается поэтапное принятие актов, предполагающих и продвигающих системные изменения, связанных с цифровизацией. Среди них можно отметить: постановление Правительства Российской Федерации от 18.04.2016 № 317 «О реализации Национальной технологической инициативы» [4]; Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в России на 2017–2030 годы» [10]; распоряжение Правительства Российской Федерации от 28.07.2017 № 1632-р «Об утверждении Программы «Цифровая экономика Российской Федерации» [5], Указ Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» и иные акты [11]. В них прослеживается твердая решимость по внесению определенных предложений для устранения всяческих препятствий для развития высокотехнологичного бизнеса. Наиболее интересными представляются положения Программы «Цифровая эко-

номика» и ее влиянии на изменения нормативной базы. В частности, в документе указывается, что для комплексного правового регулирования трудовых отношений в цифровой экономике неизбежно потребуются изменения в области нового способа оформления трудовых отношений, безбумажного взаимодействия участвующих лиц и иные нововведения.

В зарубежных странах ведется активная разработка нормативных актов, регулирующих процессы алгоритмизации и использования новых технологий. Так, уже в 2000 г. восемь мировых держав, в том числе и Российская Федерация, подписали особое соглашение – Окинавскую хартию глобального информационного общества – направленное на формирование специализированной нормативной базы, сопутствующей началу тесного сотрудничества и содействию распространению глобальных сетей и ликвидации технологического и цифрового разрыва между странами [3]. Наиболее продуктивными в области издания актов, посвященных новым технологиям, оказались страны Евросоюза. Так, специальной комиссией были подготовлены несколько документов, относящихся к регулированию систем искусственного интеллекта. Довольно примечательным еще представляется акт, опубликованный в марте 2018 г. Европейской группой по этике в науке и новых технологиях «Об искусственном интеллекте, робототехнике и «автономных» системах» [24]. В нем подчеркивается недопустимость настраивание общества под определенные нужды работодателей или агрегаторов из-за «улучшения» управления посредством искусственного интеллекта с неоправданным господствующим положением тех, кто имеет доступ к новым технологиям.

Таким образом, законодатели и работодатели, использующие впоследствии изданные акты должны ориентироваться на такую модель поведения, которая, с одной стороны, будет максимизировать преимущества и достоинства применения алгоритмов, а с другой стороны, наиболее полно защищает и гарантирует права и свободы работников.

Серьезную обеспокоенность вызывает вопрос о сохранности и безопасности персональных данных работодателей и работников. Несмотря на то, что алгоритмы оперативно управляют огромной базой данных, абсолютной гарантии надежного хранения личных данных нет. В случае сбоя системы или намеренной атаки на хранилище информация может оказаться в открытом доступе для любого пользователя Интернета. Более того, эксперт по защите данных и трудовому праву Питер Ведде критикует то, что эта информация может быть использована для создания «точного профиля производительности и поведения, что приводит к тотальной фиксации каждого поведенческого шага [18. Рр. 15–31]. Еще в 2013 г. была составлена Резолюция Генеральной Ассамблеи ООН № 68/167 «Право на неприкосновенность личной жизни в цифровой век» [25], а позднее в 2016 г. во избежание подобных ситуаций в Европейском союзе был принят Общий регламент по защите данных, унифицировавший защиту персональных данных [7]. Предполагается, что принятые меры помогут стандартизировать порядок сохранения и защиты персональных данных в новых условиях и не допустить вероятные нарушения и споры.

Обобщая вышесказанное, следует отметить, что грядущие перемены, вызванные цифровизацией экономики, несомненно, коснутся норм трудового права. Наиболее вероятными проявлениями данных процессов будут изменение технологического уклада рынка труда и условий занятости, исчезновение одних видов профессий и появление новых и повышение гибкости и эффективности производства в целом. Для успешного использования новых технологий, и в том числе алгоритмизации, законодателю следует урегулировать следующие вопросы: пределы использования новых технологий, обеспечить комфортный для всех участников экономики переходный период от старого уклада к новому, закрепить права и гарантии сторон [16. С. 49].

Список литературы

1. Аббасова Е. В., Васильев В. А. Трудовое право в цифровой реальности: проблемы интеграции // Российская юстиция. – 2019. – № 4. – С. 16–18.
2. Amazon создаст в США более 100 000 рабочих мест. URL: <https://www.vedomosti.ru/technology/articles/2017/01/16/673060-amazon-rabochih-mest/> (дата обращения: 11.09.2022).
3. Окинавская хартия Глобального информационного общества от 22.07.2000. URL: <http://www.kremlin.ru/supplement/3170/> (дата обращения: 11.09.2022).
4. О реализации Национальной технологической инициативы: постановление Правительства Российской Федерации от 18.04.2016 № 317 // СЗ РФ. 2016. № 17. Ст. 2413.
5. Об утверждении программы «Цифровая экономика Российской Федерации»: распоряжение Правительства Российской Федерации от 28.07.2017 № 1632-р // СЗ РФ. 2017. № 32. Ст. 5138.
6. Роботы в промышленности – тренд или необходимость? URL: <https://ritm-magazine.com/en/node/10252/> (дата обращения: 11.09.2022).
7. Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27.04.2016 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) (General Data Protection Regulation) (GDPR). URL: http://www.eurasiancommission.org/ru/act/techreg/depsanmer/consumer_rights/Documents/Регламент%20Европейского%20Парламента%20и%20Совета%20Европейского%20Союза%202016%20679%20от%2027%20апр.pdf/ (дата обращения: 11.09.2022).
8. Талапина Э. В. Алгоритмы и искусственный интеллект сквозь призму прав человека // Журнал российского права. 2020. № 10. С. 25.
9. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // СЗ РФ. 2002. № 1. Ст. 3.
10. О Стратегии развития информационного общества в России на 2017–2030 годы: Указ Президента РФ от 09.05.2017 № 203 // СЗ РФ. 2017. № 20. Ст. 2901.
11. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: Указ Президента РФ от 07.05.2018 № 204 // СЗ РФ. 14.05.2018. № 20. Ст. 2817.

12. Факультет нужных вещей: какие кадры требуются цифровой экономике. URL: <https://trends.rbc.ru/trends/education/5edf4af49a79477dc7ebd5a2/> (дата обращения: 11.09.2022).

13. Филипова И. А. Алгоритмизация: воздействие на сферу труда и ее регулирование // Российская юстиция. 2020. № 11. С. 12–14.

14. Филипова И. А. Правовое регулирование труда – 2020: смена парадигмы как следствие цифровизации экономики // Юрист. 2018. № 11. С. 31–35.

15. Филипова И. А. Трансформация правового регулирования труда в цифровом обществе. Искусственный интеллект и трудовое право. Н. Новгород, 2019. С. 89.

16. ЦСР. Новая технологическая революция: вызовы и возможности для России. Экспертно-аналитический доклад под научным руководством В. Н. Княгинина. Москва, 2017. С. 83.

17. De Stefano Valerio and Aloisi Antonio. Fundamental Labour Rights, Platform Work and Human-Rights Protection of Non-Standard Workers (February 18, 2018). // Forthcoming, Labour, Business and Human Rights Law, Edited by Janice R. Bellace and Beryl ter Haar, Edward Elgar Publishing Ltd., Bocconi Legal Studies Research Paper. – № 3125866. URL: <http://dx.doi.org/10.2139/ssrn.3125866/> (дата обращения: 11.09.2022).

18. Federico Chicchi. Beyond the ‘salary institution’: on the ‘society of performance’ and the platformisation of the employment relationship // «WORK ORGANISATION, LABOUR & GLOBALISATION». 2020. № 14. Pp. 15–31.

19. Frey Carl Benedikt and Michael A. Osborne. “The future of employment: How susceptible are jobs to computerisation?” // Technological Forecasting and Social Change. 2017. № 114. Pp. 254–280.

20. Griesbach K., Reich A. D., Elliott-Negri L., & Milkman R. Algorithmic Control in Platform Food Delivery Work // Socius. 2019. P. 5.

21. Jobs lost, jobs gained: workforce transitions in a time of automation. URL: <https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages/> (дата обращения: 11.09.2022).

22. Nilsen Marie, Kongsvik Trond, Antonsen Stian. Working Conditions and Safety in the Gig Economy // A Media Coverage Analysis. e-proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15). 2020.

23. Rifkin J. The end of work: the decline of the global work-force and the dawn of the post-market era // G. P. Putnam’s Sons. 1995. P. 176.

24. Statement on Artificial Intelligence, Robotics and “Autonomous” Systems. European Group on Ethics in Science and New Technologies. 2018. URL: http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf/ (дата обращения: 11.09.2022).

25. The Right to Privacy in the Digital Age. Resolution Adopted by the General Assembly. 18 December 2013. URL: <https://undocs.org/ru/A/RES/68/167/> (дата обращения: 11.09.2022).

26. Work for a brighter future – Global Commission on the Future of Work International Labour Office // Geneva: ILO. 2019. P. 18.

А. Н. Куликова,

студент,

Санкт-Петербургский институт (филиал) Всероссийского
государственного университета юстиции

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ПРАВОВЫХ ОТНОШЕНИЙ

Аннотация. В статье рассматривается процесс цифровизации правовых отношений, внедрения информационных технологий в правовую сферу общества. Исследуется влияние цифровизации на правотворчество, осуществление правосудия, а также на осуществление юридической помощи гражданам. Целью статьи является анализ системы правовых отношений в период активной информатизации общества. Сделаны выводы о важности использования цифровых технологий в системе правоотношений, а также о последствиях для правовой сферы, которые могут возникнуть в процессе цифровизации.

Ключевые слова: право, цифровизация, цифровые технологии, правовые отношения, правотворчество, правосудие, Legal Tech, Law Tech

DIGITAL TECHNOLOGIES IN THE SYSTEM OF LEGAL RELATIONS

Abstract. The article discusses the process of digitalization of legal relations, the introduction of information technologies in the legal sphere of society. The impact of digitalization on law-making, the administration of justice, as well as on the provision of legal assistance to citizens is being studied. The purpose of the article is to analyze the system of legal relations during the period of active informatization of society. The author draws conclusions about the importance of using digital technologies in legal relations, as well as about the consequences for the legal sphere that may arise in the process of digitalization.

Keywords: Law, Digitalization, Digital technologies, Legal relations, Lawmaking, justice, Legal Tech, Law Tech

В современном мире активно происходит процесс информатизации всех сфер общественной жизни. Право является главным регулятором отношений в обществе, что ставит необходимость внедрять цифровые технологии в данную сферу. Конечно, информатизация несет в себе и положительные, и негативные последствия. Процессы цифровизации играют значительную роль в правотворческой деятельности, вершении правосудия и оказании юридической помощи гражданам.

Процесс цифровизации может быть применен не только для сбора и анализа общественного мнения, но и для обеспечения всех этапов разработки законопроектов. Можно выделить несколько стадий законотворчества, на которых возможно использование цифровых технологий: учет мнения населения, разработка законопроектов и голосование по ним. Во многих странах уже применяются различные системы для голосования.

В России также существуют подобные проекты, например, «Российская общественная инициатива». Суть данной программы заключается в том, что граж-

дане могут разместить на сайте инициативу, по которой в дальнейшем будет проходить голосование. При получении необходимого количества голосов инициатива будет обязательной к рассмотрению органами государственной власти [2]. Также следует выделить автоматизированную систему обеспечения законодательной деятельности. Система позволяет гражданам получать необходимую информацию о законодательном процессе (его ход, тексты законов и иных документов).

Д. А. Пашенцев в монографии верно отметил, что внедрение цифровых технологий в правовые отношения, а точнее в правотворчество поможет обеспечить более высокий уровень информированности граждан, а вследствие и повышение правовой культуры людей. Кроме того, цифровизация делает возможным быстрое и удобное использование нормативно-правовых актов в электронной версии [1]. Хорошими примерами данного влияния цифровых технологий на правотворчество являются справочно-правовые системы «КонсультантПлюс» и «Гарант». Благодаря этим системам любой гражданин имеет возможность ознакомиться с нормативно-правовыми актами в актуальной редакции. Именно это позволит повысить правосознание населения.

Внедрение цифровых технологий может улучшить и систему правосудия. Многие авторы выделяют такое понятие, как «электронное правосудие». Так, Е. В. Бурдиной отмечается, что под электронным правосудием понимается форма и способ процесса судопроизводства с использованием информационных технологий [4 с. 43].

Использование цифровых технологий в осуществлении правосудия позволит значительно облегчить действия сторон на всех этапах. Как точно отметила А. Н. Приженникова, цифровизация системы правосудия обеспечит ускорение и оптимизацию процессов судопроизводства [9]. Для повышения эффективности работы судов возможно создание систем для электронной подачи различных документов (исковых заявлений, жалоб и т. д.); получения электронных извещений; аудио- и видеофиксации судебных заседаний; проведения видеоконференций в зале суда для того, чтобы обеспечить публичность. К тому же значительный вклад в цифровизацию деятельности судов может внести система для ведения электронного дела.

Подача документов в суд в электронном виде возможна уже и сейчас. Согласно Приказу Судебного департамента при Верховном Суде РФ от 28.12.2016 № 252 (ред. от 20.02.2018) подача производится в соответствии с установленными требованиями через личный кабинет в информационной системе «Мой арбитр». Данная система позволяет повысить доступность правосудия для граждан.

Однако не стоит забывать о том, что внедрение цифровых технологий в правосудие имеет и свои риски. Так, например, встает вопрос об обеспечении информационной безопасности и конфиденциальности различных данных. Существует возможность подмены электронных документов, что может повлечь за собой вынесение неверного решения на судебном процессе.

Цифровизация также влияет и на профессиональную деятельность юристов. Благодаря такому понятию, как Legal Tech существует возможность ознакомления

с судебными практиками, научными статьями и составлением различных договоров [6]. Использование информационных технологий снижают издержки юридической деятельности и повышают эффективность работы специалистов данной сферы. Legal Tech позволяет находить альтернативные способы разрешения споров, например, с помощью примирительных процедур.

А. В. Лошкарев и Е. А. Канунникова отметили, что освоение информационных технологий и искусственного интеллекта позволяют автоматизировать юридическую работу. Авторы привели в пример проникновение цифровых технологий в правовые отделы «Сбербанка». Такая оптимизация позволит повысить уровень юридических услуг, однако появится риск утечки персональных данных и иной важной информации, так как сфера информационных технологий может иметь «слабые места».

В оказании юридической помощи гражданам цифровизация также играет немаловажную роль. Как уже упоминалось выше, существуют справочно-правовые системы, которые помогают населению повысить правовую культуру. Кроме того, существует термин Law Tech, который дает возможность гражданам получить юридическую консультацию дистанционно, что значительно упрощает взаимодействие пользователя услуг и юриста.

В период внедрения цифровых технологий во все сферы общественных отношений, в том числе и в правоотношения, следует осуществлять государственную поддержку проектов, которые могут внести большой вклад в цифровизацию правовой системы. Информационные технологии позволяют соблюдать принцип гласности, а также повышать уровень образованности и осведомленности населения. Цифровизация делает возможным упрощение и ускорение работы многих элементов правовых отношений. Важно использовать информационные технологии в сфере права, так как это поможет достаточно оперативно собирать и анализировать информацию и искать наиболее верные решения.

Безусловно, не стоит забывать и о негативных аспектах процесса цифровизации. Право является основным регулятором общественных отношений и влияет на другие сферы жизни. Поэтому необходимо постоянно обеспечивать безопасность правотворчества, осуществления правосудия и других видов правовых отношений. Нельзя допускать какой-либо утечки конфиденциальной информации, которая может привести к необратимым последствиям.

Подводя итог можно сказать, что главной задачей для специалистов является определение направления вектора развития цифровых технологий в системе правовых отношений. Цифровизация, несмотря на всевозможные риски, позволит решить многие важные вопросы в сфере права и повысить уровень юридической грамотности среди населения.

Список литературы

1. Алферова Е. В., Пашенцев Д. А., Залоило М. В., Иванюк О. В., Головина А. А. 2000.02.002. Цифровизация правотворчества: поиск новых решений: монография // Государство и право: Реферативный журнал. 2020. № 2. URL:

<https://cyberleninka.ru/article/n/2000-02-002-tsifrovizatsiya-pravotvorchestva-poisk-novyh-resheniy-monografiya-d-a-pashentsev-m-v-zaloilo-o-v-ivanyuk-a-a-golovina-pod-obsch-red> (дата обращения: 17.09.2022).

2. Арнаутова А. А. Цифровизация правотворческой деятельности // Век качества. 2019. № 2. URL: <https://cyberleninka.ru/article/n/tsifrovizatsiya-pravotvorcheskoj-deyatelnosti> (дата обращения: 17.09.2022).

3. Булгакова Е. В. Применение искусственного интеллекта при проведении экспертизы законопроектов // Вестник Волгоградской академии МВД России. 2012. № 3 (22). URL: <https://cyberleninka.ru/article/n/primenenie-iskusstvennogo-intellekta-pri-provedenii-ekspertizy-zakonoproektov> (дата обращения: 17.09.2022).

4. Бурдина Е. В. Электронное правосудие: Монография / – Москва: РГУП, 2021. – 344 с. (дата обращения: 17.09.2022).

5. Джикия М. Д., Шкаленко А. В., Джикия А. А. Роль «LegalTech» в модернизации профессиональной юридической деятельности // Вестник Московского университета МВД России. 2021. № 6. URL: <https://cyberleninka.ru/article/n/rol-legaltech-v-modernizatsii-professionalnoj-yuridicheskoy-deyatelnosti> (дата обращения: 17.09.2022).

6. Канунникова Е. А., Лошкарев А. В. Цифровизация юридической профессии: угрозы и возможности // Международный журнал гуманитарных и естественных наук. 2020. № 10–3. URL: <https://cyberleninka.ru/article/n/tsifrovizatsiya-yuridicheskoy-professii-ugrozy-i-vozmozhnosti> (дата обращения: 17.09.2022).

7. Липень С. В. Информационные технологии в правотворческой деятельности // Lex Russica. 2019. № 8 (153). URL: <https://cyberleninka.ru/article/n/informatsionnye-tehnologii-v-pravotvorcheskoj-deyatelnosti> (дата обращения: 17.09.2022).

8. Новикова К. С. Цифровые новации и элементы электронного правосудия в арбитражном судопроизводстве в период распространения коронавирусной инфекции // Образование и право. 2020. № 4. URL: <https://cyberleninka.ru/article/n/tsifrovye-novatsii-i-elementy-elektronnogo-pravosudiya-v-arbitrazhnom-sudoproizvodstve-v-period-rasprostraneniya-koronavirusnoy-infekcii> (дата обращения: 17.09.2022).

9. Приженникова А. Н. Осуществление правосудия в условиях информатизации и цифровизации // Образование и право. 2020. № 9. URL: <https://cyberleninka.ru/article/n/osuschestvlenie-pravosudiya-v-usloviyah-informatizatsii-i-tsifrovizatsii> (дата обращения: 17.09.2022).

10. Приказ Судебного департамента при Верховном Суде РФ от 28.12.2016 № 252 «Об утверждении Порядка подачи в арбитражные суды Российской Федерации документов в электронном виде, в том числе в форме электронного документа» (дата обращения: 17.09.2022).

11. Рожкова М. А. Онлайн-конференция «развитие legal tech» (Санкт-Петербург, 20 апреля 2020 г.) // Теоретическая и прикладная юриспруденция. Москва, 2020. – 104 с.

12. Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1 (253). URL: <https://cyberleninka.ru/article/n/pravo-v-usloviyah-tsifrovoy-realnosti> (дата обращения: 17.09.2022).

13. Ягофарова И. Д. Цифровые технологии в правотворческой деятельности: теоретико-правовой аспект // Пролог: журнал о праве. 2021. № 2. С. 4–13. DOI: 10.21639/2313–6715.2021.2.1. URL: <https://cyberleninka.ru/article/n/tsifrovyye-tehnologii-v-pravotvorcheskoy-deyatelnosti-teoretiko-pravovoy-aspekt> (дата обращения: 17.09.2022).

Н. С. Купцов,
студент,

Российский государственный университет правосудия

ПРОБЛЕМА ОПРЕДЕЛЕНИЯ ТЕОРЕТИКО-ПРАВОВОЙ СУЩНОСТИ НЕКОТОРЫХ ЭЛЕМЕНТОВ ВИРТУАЛЬНОГО МИРА В КОНТЕКСТЕ ОТНЕСЕНИЯ ИХ К ОБЪЕКТАМ ГРАЖДАНСКИХ ПРАВ

Аннотация. На сегодняшний день очевидно наличие серьезных вызовов для устоявшихся подходов к пониманию основ правового регулирования отдельных групп правоотношений, что не в последнюю очередь связано со стремительным развитием современных технологий и тотальной цифровизацией профессиональной и обыденной жизни населения. В частности, отсутствует единое мнение о правовой природе элементов виртуального мира, их способности выступать в качестве объектов гражданских прав и, следовательно, гражданско-правового оборота. Целью исследования в настоящей статье является последовательный поиск ответа на вопрос о целесообразности отнесения подобных элементов к одной из категорий объектов гражданских прав, законодательно закрепленных в Российской Федерации. Для этого проводится выявление сходных и различных признаков между ними, делается вывод о возможности отождествления или его нежелательности.

Ключевые слова: развитие цифровых технологий, виртуальный мир, элементы виртуального мира, многопользовательские онлайн-игры, социальные сети, объекты гражданских прав, гражданско-правовые отношения

THE PROBLEM OF DETERMINING THE THEORETICAL AND LEGAL ESSENCE OF SOME VIRTUAL WORLD OBJECTS IN THE CONTEXT OF THEIR ATTRIBUTION TO OBJECTS OF CIVIL RIGHTS

Abstract. Today, it is obvious that there are serious challenges for established approaches to understanding the basics of legal regulation of certain groups of legal relations, which is not least due to the rapid development of modern technologies and the total digitalization of professional and everyday life of the population. In particular, there is no consensus on the legal nature of virtual world elements, their ability to act as objects of civil rights and, consequently, civil law turnover. The purpose of the author in this article is a consistent search for an answer to the question of the expediency of assigning such elements to one of the categories of objects of civil rights legally enshrined in the Russian Federation. To do this, the identification of similar and different signs between

them is carried out, the conclusion is made about the possibility of identification or its undesirability.

Keywords: Development of digital technologies, Virtual world, Elements of the virtual world, Online multiplayer games, Social network, Objects of civil rights, Civil law relations

В начале третьего десятилетия XXI в. с уверенностью можно констатировать окончательное оформление постиндустриального общества в ряде развитых государств мира и утверждение тенденции на его построение в подавляющем большинстве стран развивающихся. Появление и повсеместное распространение интернет-технологий, разработка принципиально новых способов передачи информации (и, как следствие, многократное ускорение и удешевление этого процесса), всестороннее совершенствование технологического потенциала, инновации в производстве всего спектра товаров и услуг – это и многое другое сегодня уже не фантастическая далекая перспектива, а почти «осязаемая» действительность. Безусловно, технологический прогресс такого масштаба направлен, прежде всего, на совершенствование жизнедеятельности как отдельных граждан, так и всего общества в целом, исправление существующих в этой связи недостатков, а также развитие человеческого и техногенного потенциала. Вместе с тем трудно не обратить внимание на то, что по мере нарастания темпов технологического развития все более очевидными становятся возникающие противоречия между новыми, инновационными явлениями и процессами, неизбежно порождаемыми прогрессом, и уже существующими (порой не одно столетие) политическими, экономическими, социальными, культурными моделями. Сказанное выше в полной мере справедливо и для права: формирование, по сути, принципиально новой картины реальности, неизбежно сопровождающее сегодняшние технологические прорывы, выступает серьезным вызовом для проверки жизнеспособности многих правовых концепций и теоретических положений, до недавнего времени считавшихся едва ли не абсолютными истинами. При этом такая ситуация наблюдается буквально повсеместно в правовой теории и практике: одинаково дискуссионными выглядят, например, и проблемы регулирования правоотношений субъектов посредством использования обширных возможностей сети Интернет, и изыскание способов для защиты авторских прав в условиях тотальной открытости цифровых платформ и неограниченного количества их пользователей, и разработка эффективных методов борьбы с цифровой преступностью и усиления кибербезопасности – а потому нет оснований не согласиться с мнением Г. А. Гаджиева, назвавшего технологические изменения конца XX в. (в частности, создание виртуальной реальности) «самым серьезным вызовом праву за всю его историю» [5. С. 14].

Справедливо вести речь о том, что одним из основополагающих, корневых вызовов цифровой современности праву является именно «виртуальность», переходу которой от абстрактно-философской концепции к вполне реально существующему пространству, своего рода, «параллельной реальности» немало поспособствовал научно-технический прогресс, в том числе – стремительное

развитие цифровых и интернет-технологий. По весьма меткому выражению Н. В. Алексеева «с появлением сети Интернет виртуальность стала воплощаться в реальность» [1. С. 83], а вместе с ней совершенно реальными оказались и проблемы правового регулирования огромного числа разнородных отношений между пользователями возникающих цифровых технологий. Одной из наиболее острых автору представляется вопрос о правовой природе так называемых виртуальных (цифровых) объектов (элементов), сфера возникновения которых отличается значительной широтой: от предметов игрового мира в однопользовательских и многопользовательских онлайн-играх до учетных записей пользователей на всевозможных интернет-ресурсах; от созданных пользователями на конкретных платформах цифровых аватаров, обладающих специфическими, если не уникальными, признаками до обыкновенных сайтов, созданных конкретными лицами для обеспечения доступа к предоставляемым ими услугам. Все вышеуказанные объекты объединены принадлежностью к пространствам «виртуальных миров», подход к пониманию которых до сих пор не устоялся. К ставшей уже классической концепции виртуального мира как многопользовательского игрового пространства добавляются довольно неожиданные новые: так, В. В. Архипов указывает на то, что виртуальным миром может считаться любое цифровое пространство, обладающее определенной организованностью, возможностью одновременного нахождения в нем нескольких пользователей, взаимодействующих друг с другом, а значит, таковым может считаться любая социальная сеть [2. С. 97–98]. Разнородные объекты таких виртуальных миров сегодня выступают полноценными объектами гражданских правоотношений: покупаются и продаются, являются предметами дарения и даже платежа, т. е. оформляются в качестве объектов гражданских прав. Прямое нормативно-правовое закрепление статуса виртуальных объектов уже состоялось в ряде развитых постиндустриальных государств (на Тайване, в Южной Корее и США и пр.) [11. С. 382–385]. В Российской Федерации, однако, такое оформление пока происходит исключительно на уровне практического правоприменения: с точки зрения цивилистической доктрины однозначного отнесения объектов виртуального мира к той или иной категории объектов гражданских прав, поименованных в ст. 128 Гражданского кодекса РФ [6], не произошло. Естественно, это приводит к значительному расхождению и отсутствию единообразия в материалах судебной практики (если вовсе не к тотальному игнорированию судами соответствующих исковых заявлений с абсолютно неприемлемой в данном случае ссылкой на гл. 58 ГК РФ [2. С. 95]) и, как следствие, отсутствию достаточного уровня правовой защищенности интересов граждан и организаций в отношении принадлежащих им объектов виртуального мира. Вместе с тем, стремительный рост числа пользователей интернет-ресурсов и онлайн-игр, а также распространение практики приобретения объектов виртуального мира и распоряжения ими делает дальнейшее игнорирование рассматриваемой проблемы бесперспективным и вызывающим опасения. Возможно ли отнесение виртуальных объектов к какой-либо из законодательно закрепленных в России категорий объектов гражд-

данских прав? И есть ли необходимость модернизации в этой связи гражданского законодательства страны?

На сегодняшний день наиболее устоявшимся подходом к определению правовой сущности объектов виртуального мира является подход, определяющий их в качестве охраняемых результатов интеллектуальной деятельности или объектов интеллектуальной собственности. Такая точка зрения небесспорна, поскольку в указанном качестве пп. 2 п. 1 ст. 1225 ГК РФ [6] устанавливает программы для ЭВМ (электронных вычислительных машин, в число которых по определению входит и компьютер). Сторонники указанного подхода апеллируют к фактической сущности любого виртуального объекта: он, как и вся программа в целом, выступает лишь элементом программного кода, написанного разработчиками соответствующего цифрового продукта, а значит, все права (в том числе, имущественные) на получившийся результат принадлежат им. Все действия с такими объектами рядовых пользователей продукта осуществляются на основании строго установленного пользовательским соглашением порядка, исключающего свободное владение, пользование или распоряжение объектами вне пределов виртуального мира [8. С. 37–38]. Следует признать, что до момента возникновения многопользовательских онлайн-ресурсов и широкого распространения социальных сетей вышеизложенный подход оставался едва ли не единственно верным: так, безусловным объектом интеллектуальной собственности выступает дизайн конкретного сайта в пространстве сети Интернет; любые объекты и предметы в однопользовательских игровых продуктах также являются лишь визуальным отображением программного кода – охраняемого результата интеллектуальной деятельности разработчика (стоит, однако, уточнить, что игровой продукт с возможностью пользования им лишь каждым игроком в отдельности без способности взаимодействия друг с другом вряд ли может выступать виртуальным миром в том смысле, в котором его понятийные признаки были раскрыты выше). Вместе с тем возникновение широкого спектра пространств виртуальных миров как досугового, так и коммуникативного характера стало для рассматриваемой точки зрения серьезным ударом и вызвало достаточное количество противоречий. Так, отсутствует единое мнение о том, что конкретно в виртуальном многопользовательском пространстве может выступать объектом интеллектуальной собственности его создателя: если программный код, графические модели и звуковое сопровождение могут считаться таковыми, то товарные знаки или отдельные элементы, созданные или используемые самими пользователями (аватары, фотоматериалы и пр.) – с большой долей условности [7. С. 121]. Сказанное выше равным образом справедливо и по отношению к многопользовательским онлайн-играм, где у игрока как правило существует возможность индивидуализировать своего аватара (персонажа), в том числе путем оформления внешнего облика или создания «имени» с использованием фото или графических изображений, и по отношению к личным страницам в социальных сетях, которые по сути представляют собой целостный образ конкретного реального пользователя в цифровом пространстве. Кроме того, признание объектов виртуального мира как результатов интеллектуальной деятельности

вступает в резкое противоречие с устоявшейся практикой гражданско-правового оборота: все чаще с целью извлечения прибыли разработчик цифрового виртуального мира прибегает к продаже пользователям отдельных «уникальных» или «лимитированных» виртуальных предметов или доступа к более широким возможностям в границах виртуального мира за реальные денежные средства. В этих условиях у пользователей возникает законный интерес к беспрепятственному владению, пользованию и распоряжению приобретенным, однако с позиции определения виртуальных предметов как объектов интеллектуальной собственности разработчика это является весьма проблематичным, так как любые действия с приобретенными объектами в силу абз. 2 п. 1 ст. 1229 ГК РФ [6] ставятся в прямую зависимость от воли создателя виртуального мира, который, в сущности, несмотря на факт совершения сделки купли-продажи, остается их собственником и владельцем. В этой связи небезосновательными выглядят замечания исследователей о зыбкости соблюдения баланса прав и законных интересов пользователей и разработчиков виртуальных ресурсов и тенденции на превалирование интересов последних [8. С. 38]. О. Н. Горохова и вовсе указывает на то, что зачастую юридические правообладатели (разработчики) виртуального цифрового продукта в одностороннем порядке закрепляют в правовых актах (в том числе, пользовательских соглашениях) положения об отсутствии у пользователей каких-либо имущественных прав на виртуальные объекты вне зависимости от затраченных ими средств и / или усилий; по мнению исследователя, отрицать наличие у пользователей имущественных прав на приобретенные ими объекты виртуального мира «в корне неверно» [11. С. 381]. Очевидно, что оформления элементов виртуального мира как объектов гражданских прав исключительно с позиции интеллектуальной собственности уже недостаточно для установления эффективного правового регулирования в данной области.

Поиск новых путей определения правовой природы элементов виртуального мира с опорой на предложенные ст. 128 ГК РФ варианты неизбежно способствовал появлению точки зрения, согласно которой виртуальные объекты могут считаться вещами, а регулирование возникающих гражданско-правовых отношений – осуществляться путем применения уже существующих норм вещного права. Так, Д. А. Черноусов и Ж. Ю. Юзефович не исключают возможности применения соответствующих положений гражданского законодательства РФ к регулированию правоотношений по поводу и в связи с принадлежностью и оборотом виртуальных объектов, указывая на соответствующий позитивный опыт ряда государств (Республики Кореи, Тайваня и Гонконга) [9. С. 40–41]. Несмотря на то, что отдельные элементы виртуального мира действительно могут выражаться в качестве своего рода «виртуальных вещей» (автомобили, дома, участки земли и т. д.), такой упрощенный подход представляется неверным и контрпродуктивным. Прежде всего, вещью, как известно, может выступать лишь конкретная «ограниченная часть материального мира» [10. С. 159], существующая и доступная для прямого взаимодействия с ней в реальности. Разумеется, любой цифровой объект таким признаком не обладает: владение,

пользование и распоряжение им если и возможно, то исключительно в границах соответствующего виртуального мира без возможности воплощения в физической реальности. Кроме того, рассматриваемый подход не универсален: если приобретенные оружие, элементы обмундирования или транспортные средства персонажа в многопользовательской онлайн-игре можно представить в качестве вещей хотя бы условно, то платное усиление его возможностей, а также различные аккаунты пользователя в социальных сетях или цифровых сервисах вещами не выступают даже с точки зрения логики. Наконец, в современных условиях говорить о полной принадлежности того или иного виртуального объекта конкретному пользователю не приходится: в конечном итоге само существование любого элемента виртуального мира зависит от существования самого этого мира, которое в сущности может быть прекращено по желанию его разработчика. Иными словами, осуществление любых действий с подобным объектом не является исключительной прерогативой пользователя, он не обладает принципиально важным для вещного права господством над принадлежащим ему имуществом [11. С. 380]. В этой связи, говорить об эффективности применения к регулированию гражданско-правовых отношений, возникающих по поводу обладания и распоряжения виртуальными объектами, существующих норм вещного права по аналогии не приходится. Следует, однако, отдать должное указанной точке зрения: ее раскрытие в значительной степени приближает отечественную цивилистическую доктрину к необходимости широкого научного и профессионального признания проблемы неопределенности статуса виртуальных объектов как объектов гражданских прав, поиску путей ее преодоления. В том числе это выражается во все чаще оглашаемых предложениях признания за пользователями виртуальных миров «имущественных прав использования тех или иных виртуальных объектов» [3. С. 41].

Трудность нахождения наиболее оптимального и однозначного подхода к определению правового статуса виртуальных объектов как объектов гражданских прав вынуждает обращать внимание и на нейтральные, своего рода, «неконфликтные» варианты. К примеру, нельзя не обратить внимания на то, что ст. 128 ГК РФ содержит открытый перечень объектов гражданских прав: в качестве таковых закон готов признавать любое «иное имущество», среди которого, при желании, можно найти место и элементам виртуальных миров. Так, И. З. Аюшеева отмечает, что «несмотря на отсутствие в ГК РФ определения многих цифровых объектов ... нельзя делать вывод о том, что иные непоименованные объекты не могут быть признаны объектами гражданских прав» [3. С. 36]; О. Н. Горохова указывает, что «игровое имущество» может рассматриваться в качестве объекта гражданских прав, так как по существу является «благом, которое служит удовлетворению потребностей» [11. С. 382]. Автору представляется, что рассматриваемый подход, хотя и имеет право на жизнь, все же не может и не должен восприниматься исследовательским сообществом в качестве основополагающего. Устранив ряд теоретических разногласий в среде цивилистической науки, он, тем не менее способен привести к еще большей неопределенности в плоскости юридической (в том числе – судебной) практики, а значит – подвергнуть дополнительному ри-

ску защиту прав и законных интересов фактических владельцев разнообразных объектов виртуального мира. Кроме того, данная точка зрения, в сущности, не дает ответа и на главный вопрос, поднятый автором в настоящем исследовании: «Какую именно теоретико-правовую природу имеют объекты виртуального мира, выступая в качестве объектов гражданских прав»? В этой связи, рассмотрение указанного подхода в качестве наиболее эффективного представляется резким логическим противоречием.

Думается, что анализ приведенных выше теоретических подходов к определению гражданско-правовой сущности элементов виртуальных миров в полной мере иллюстрирует всю сложность рассматриваемой проблемы для современной отечественной цивилистики. Удовлетворяя отдельным признакам каждой из поименованных в ст. 128 ГК РФ категорий объектов гражданских прав (будь то вещи, интеллектуальная собственность или цифровые права), элементы виртуальных миров, тем не менее не могут быть однозначно отнесены к какой-либо из них. Путь наименьшего сопротивления, предполагающий попытки определения объектов виртуального мира через потенциально бесконечную категорию «иного имущества» на деле выступает едва ли не самым опасным для правовой теории и правоприменения, многочисленно повышая риски размывания и без того весьма неопределенных понятий «виртуальных объектов» и «виртуального имущества». Поэтому наиболее адекватным, эффективным и жизнеспособным подходом к определению сущности виртуальных объектов в контексте отнесения их к объектам гражданских прав автору представляется, пожалуй, наиболее радикальный и сложный: реформирование существующего гражданского законодательства и введение в научно-практический юридический оборот принципиально новой категории «виртуального имущества», а также ее дальнейшая разработка и детализация. С этой позиции, в частности, первостепенным шагом, имеющим принципиальное значение для развития отечественного гражданского законодательства, является изменение редакции ст. 128 ГК РФ, а именно: введение в ее состав конструкции «виртуальное имущество» в качестве одной из категорий объектов гражданских прав.

Наряду с качественным увеличением уровня правовой определенности и совершенствованием степени правового регулирования гражданских правоотношений, возникающих по поводу обладания и распоряжения объектами виртуальных миров, а также уровня защищенности прав и законных интересов владельцев подобного виртуального имущества, поддерживаемый автором подход, как представляется, обладает еще одним важным преимуществом. Он позволит отечественным исследователям и правоприменителям не заикливаться на существующих правовых категориях, разработать и усовершенствовать и подготовить крепкую основу для последующего развития российского законодательства и права в условиях сохранения тенденции на дальнейшую цифровизацию жизнедеятельности человека и общества. Очевидно, что на данный момент потенциал развития цифровых и информационных технологий далеко не исчерпан; это справедливо и для широкого спектра технологий

виртуальных миров, виртуальной реальности. Такое наблюдение становится еще более обоснованным, если учесть обширную сферу возможного применения инноваций в сфере виртуальной реальности: от развлечения и досуга до медицины [4. С. 811–812]. Ясно, что искусственное промедление в вопросе реформирования законодательства и права с целью достижения более эффективного уровня правового регулирования в рассматриваемой сфере со временем способно привести к еще большим проблемам правоприменения и издержкам по их преодолению. В этой связи предлагаемое автором решение нуждается в как можно более незамедлительном осмыслении и оценке возможности его осуществления на практике.

Список литературы

1. Алексеев Н. В. Виртуальные пространства и вопросы права // Цифровизация как новая парадигма развития: сборник статей II Международной научно-практической конференции, Петрозаводск, 11 января 2022 года. – Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская И. И.), 2022. С. 82–89.
2. Архипов В. В. Виртуальное право: основные проблемы нового направления юридических исследований // Известия высших учебных заведений. Правоведение. 2013. № 2 (307). С. 93–114.
3. Аюшеева И. З. Цифровые объекты гражданских прав // Lex russica (Русский закон). 2021. № 74 (7). С. 32–43.
4. Волынов, М. М. Виртуальная реальность: виды, структура, особенности, перспективы развития / М. М. Волынов, А. А. Китов, Б. С. Горячкин // E-Scio. 2020. № 5 (44). С. 795–812.
5. Гаджиев Г. А. Онтология права (критическое исследование юридического концепта действительности): монография. Москва: Норма: ИНФРА-М, 2021. 320 с. URL: <https://znanium.com/catalog/product/1240961> (дата обращения: 26.08.2022).
6. Гражданский Кодекс Российской Федерации (часть первая): Федеральный закон от 30.11.1994 № 51-ФЗ // Собрание законодательства РФ. 1994. № 32. Ст. 3301.
7. Демкович Д. А. Виртуальный мир как объект права интеллектуальной собственности // Суверенное государство и его право: актуальные проблемы юридической науки и правоприменительной практики в современной России» (к 370-летию со времени принятия Соборного Уложения (1649 года): сборник трудов XVI Всероссийских декабрьских юридических чтений в Костроме. Всероссийская научно-практическая конференция, Кострома, 12–13 декабря 2019 года. Кострома: Костромской государственный университет, 2020. С. 118–122.
8. Милашова, И. Б. Виртуальная собственность или инновационная интеллектуальная собственность: проблемы теории и практики в контексте развития индустрии компьютерных игр / И. Б. Милашова, Р. Л. Наумова // Актуальные проблемы права и экономики: Сборник научных трудов / под общей редакцией А. В. Трофименко и А. М. Петрова. Саратов: Саратовский социально-экономический институт (филиал) федерального государственного бюджетного образова-

тельного учреждения высшего образования «Российский экономический университет им. Г. В. Плеханова», 2016. С. 31–39.

9. Черноусов, Д. А. Применение вещного права к регулированию виртуального имущества / Д. А. Черноусов, Ж. Ю. Юзефович // Право и законность: вопросы теории и практики: сборник материалов XII Всероссийской научно-практической конференции, Абакан, 22–23 апреля 2022 года. Абакан: Издательство ФГБОУ ВО «Хакасский государственный университет им. Н. Ф. Катанова», 2022. С. 40–43.

10. Шершеневич Г. Ф. Учебник русского гражданского права (по изданиям 1912 и 1914–1915 гг.): в 2 томах. Том 1: учебник. Москва: Статут, 2021. 838 с.

11. E-commerce и взаимосвязанные области (правовое регулирование): сборник научных трудов / А. А. Богустов, О. Н. Горохова, Д. А. Доротенко [и др.]; под ред. М. А. Рожковой. – Москва: Статут, 2019. – 448 с.

СОДЕРЖАНИЕ | CONTENTS

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ПРАВОВЫХ ОТНОШЕНИЙ
(МОЛОДЕЖНОЕ ПРОСТРАНСТВО НАУКИ)» | DIGITAL TECHNOLOGIES
IN THE SYSTEM OF LEGAL RELATIONS (YOUTH SPACE OF SCIENCE)

<i>Абабкова А. Ю.</i> МЕСТО ЦИФРОВОЙ ВАЛЮТЫ В СИСТЕМЕ ОБЪЕКТОВ ГРАЖДАНСКИХ ПРАВ <i>Ababkova A.</i> THE PLACE OF DIGITAL CURRENCY IN THE SYSTEM OF OBJECTS OF CIVIL LAW RIGHTS.....	6
<i>Авдеева Е. В., Мелик-Оганджян А. Ф.</i> ЦИФРОВИЗАЦИЯ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ПРАВ СУБЪЕКТОВ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ <i>Avdeeva E., Melik-Ogandzhanyan A.</i> DIGITALIZATION TO IMPROVE THE EFFICIENCY OF THE PROTECTION OF THE RIGHTS OF BUSINESS ENTITIES.....	11
<i>АвтомONOва М. В., Блинкова А. Е.</i> ПРАВОВАЯ ДЕЙСТВИТЕЛЬНОСТЬ ВОСПИТАНИЯ МОЛОДЕЖИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ <i>Avtomonova M., Blinkova A.</i> LEGAL VALIDITY OF YOUTH EDUCATION IN CONDITIONS OF DIGITALIZATION.....	21
<i>Акифьева В. С., Рау А. И., Сметанина А. И.</i> ПРЕИМУЩЕСТВА И НЕДОСТАТКИ ЦИФРОВИЗАЦИИ В ПРАВОВОЙ СИСТЕМЕ <i>Akifeva V., Rau A., Smetanina A.</i> BENEFITS AND DISADVANTAGES OF DIGITALIZATION IN THE LEGAL SYSTEM.....	23
<i>Александров Д. О.</i> ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ СУДОСТРОЕНИЯ <i>Aleksandrov D.</i> PROBLEMS OF LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE IN SHIPBUILDING.....	30
<i>Антонова Л. И., Корнева К. А.</i> К ВОПРОСУ О «МЯГКОМ ПРАВЕ» И САМОРЕГУЛИРОВАНИИ В КОДЕКСАХ ЭТИКИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА <i>Antonova L., Korneva K.</i> ON SOFT LAW AND SELF-REGULATION IN CODES OF ETHICS FOR ARTIFICIAL INTELLIGENCE.....	34
<i>Артамонова Д. А., Киселев А. М.</i> О ВОПРОСЕ ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ТРУДОВОМ ПРАВЕ <i>Artamonova D., Kiselev A.</i> ON THE ISSUE OF THE USE OF DIGITAL TECHNOLOGIES IN LABOR LAW.....	38

<i>Астрыкова Е. С., Шевцова А. В.</i> К ПРОБЛЕМЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОТДЕЛЬНЫХ ОБЪЕКТОВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ <i>Astryakova E., Shevcova A.</i> ON THE PROBLEM OF LEGAL REGULATION OF THE SEPARATION OF INTELLECTUAL PROPERTY OBJECTS	41
<i>Ахатова А. М.</i> ОБОСНОВАННЫЙ РИСК И КРАЙНЯЯ НЕОБХОДИМОСТЬ КАК ИНСТИТУТЫ УГОЛОВНОГО ПРАВА В СФЕРЕ ДЕЙСТВИЯ «РЕГУЛЯТОРНЫХ ПЕСОЧНИЦ» (ЭКСПЕРИМЕНТАЛЬНЫХ ПРАВОВЫХ РЕЖИМОВ В ОБЛАСТИ ЦИФРОВЫХ ИННОВАЦИЙ) <i>Ahatova A.</i> JUSTIFIED RISK AND EXTREME NEED AS INSTITUTIONS OF CRIMINAL LAW IN THE SPHERE OF “REGULATORY SANDBOXES” (EXPERIMENTAL LEGAL REGIMES IN THE FIELD OF DIGITAL INNOVATION)	43
<i>Базака В. В., Ковалев И. П.</i> К ВОПРОСУ О ЦИФРОВИЗАЦИИ ГРАЖДАНСКОГО ПРОЦЕССА В ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКЕ <i>Bazaka V., Kovalev I.</i> ON THE ISSUE OF DIGITALIZATION OF THE CIVIL PROCESS IN THE DONETSK PEOPLE’S REPUBLIC	51
<i>Баучкина М. Ю.</i> ЭЛЕКТРОННЫЙ ФОРМАТ КАК ПЕРСПЕКТИВНОЕ НАПРАВЛЕНИЕ РАЗВИТИЯ ГОСУДАРСТВЕННЫХ ЗАКУПОК <i>Vauchkina M.</i> ELECTRONIC FORMAT AS A PROMISING DIRECTION FOR THE DEVELOPMENT OF PUBLIC PROCUREMENT.....	55
<i>Баяндурян А. К.</i> ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ ПОЛУЧЕНИИ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ ИЗ IoT-УСТРОЙСТВ <i>Bayanduryan A.</i> THE USE OF SPECIAL KNOWLEDGE IN OBTAINING EVIDENTIARY INFORMATION FROM IOT DEVICES	59
<i>Белов Н. С.</i> ПРАВОВЫЕ И ТЕХНИЧЕСКИЕ АСПЕКТЫ ВНЕДРЕНИЯ СТЕЙБЛКОИНОВ В РОССИЙСКОЙ ФЕДЕРАЦИИ <i>Belov N.</i> LEGAL AND TECHNICAL ASPECTS OF THE INTRODUCTION OF STABLECOINS IN THE RUSSIAN FEDERATION	62
<i>Белозерова Д. Д.</i> УЧАСТИЕ ГРАЖДАН В ЗАКОНОДАТЕЛЬНОМ ПРОЦЕССЕ ПРИ ПОМОЩИ ЦИФРОВЫХ ТЕХНОЛОГИЙ <i>Belozerova D.</i> CITIZENS’ PARTICIPATION IN THE LEGISLATIVE PROCESS WITH THE HELP OF DIGITAL TECHNOLOGIES	66
<i>Блохина А. А.</i> ПРИМЕНЕНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ФАРМАЦЕВТИЧЕСКОМ БИЗНЕСЕ: ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРОДАЖИ РЕЦЕПТУРНЫХ ПРЕПАРАТОВ ЧЕРЕЗ ПЛОЩАДКИ ЭЛЕКТРОННОЙ КОММЕРЦИИ <i>Blohina A.</i> APPLICATION OF DIGITAL TECHNOLOGIES IN THE PHARMACEUTICAL BUSINESS: LEGAL REGULATION OF THE SALE PRESCRIPTION DRUGS THROUGH E-COMMTRCE PLATFORM	74

<i>Богославская К. Э.</i> ЦИФРОВЫЕ ТЕХНОЛОГИИ В НАЛОГОВЫХ И ГРАЖДАНСКИХ ПРАВООТНОШЕНИЯХ В РОССИЙСКОЙ ФЕДЕРАЦИИ <i>Bogoslavskaya K.</i> DIGITAL TECHNOLOGIES IN TAX AND CIVIL LEGAL RELATIONS.....	80
<i>Бойкова П. В.</i> НЕОБХОДИМОСТЬ СИСТЕМАТИЗАЦИИ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ <i>Bojkova P.</i> THE NEED TO SYSTEMATIZE LEGISLATION IN THE FIELD OF DIGITAL TECHNOLOGIES	91
<i>Бордакова А. Г., Калягин А. В.</i> МОНИТОРИНГ И МЕРЫ ПО ПРОФИЛАКТИКЕ КАК ФОРМЫ ГОСУДАРСТВЕННОГО КОНТРОЛЯ (НАДЗОРА) <i>Bordakova A., Kalyagin A.</i> MONITORING AND PREVENTIVE MEASURES AS A FORM OF STATE CONTROL (SUPERVISION).....	97
<i>Буравцова Е. Г.</i> ТРАНСФОРМАЦИЯ ПРАВ ЧЕЛОВЕКА В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ: ОПЫТ ЗАРУБЕЖНЫХ СТРАН <i>Buravcova E.</i> TRANSFORMING HUMAN RIGHTS IN THE DIGITAL AGE: EXPERIENCES FROM ABROAD.....	102
<i>Булатова З. А.</i> РАЗВИТИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В УСЛОВИЯХ СОВЕРШЕНСТВОВАНИЯ КОНСТИТУЦИОННО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРОСТРАНСТВЕННОГО РАЗВИТИЯ <i>Bulatova Z.</i> THE DEVELOPMENT OF DIGITAL TECHNOLOGIES IN THE CONTEXT OF IMPROVING THE CONSTITUTIONAL AND LEGAL REGULATION OF SPATIAL DEVELOPMENT	105
<i>Бурак Н. И.</i> О ВЛИЯНИИ РАЗВИТИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА СУЩНОСТЬ ПРАВООТНОШЕНИЙ <i>Burak N.</i> THE IMPACT OF THE DEVELOPMENT OF DIGITAL TECHNOLOGIES ON THE ESSENCE OF LEGAL RELATIONS	109
<i>Валиуллин Т. Р., Мустафина С. Д.</i> ПРАВОВЫЕ ОГРАНИЧЕНИЯ ИСПОЛЬЗОВАНИЯ КРИПТОВАЛЮТЫ В СОВРЕМЕННУЮ ЭПОХУ <i>Valiullin T., Mustafina S.</i> LEGAL RESTRICTIONS ON THE USE OF CRYPTOCURRENCIES IN THE DIGITAL AGE	122
<i>Великохатко Ю. И.</i> ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ УГОЛОВНО-ПРАВОВЫХ ОТНОШЕНИЙ <i>Velikohatko Yu.</i> DIGITAL TECHNOLOGIES IN THE SYSTEM OF CRIMINAL LAW RELATIONS	124

<i>Викторов И. Д.</i> ЦИФРОВЫЕ ПЛАТФОРМЫ: ПРОБЛЕМЫ АНТИМОНОПОЛЬНОГО РЕГУЛИРОВАНИЯ И МЕРЫ ПО ИХ УСТРАНЕНИЮ <i>Viktorov I.</i> DIGITAL PLATFORMS: ANTITRUST PROBLEMS AND MEASURES TO ADDRESS THEM	127
<i>Виноградова А. А., Хайрутдинова Л. Р.</i> КИБЕРВИКТИМНОСТЬ ЖЕРТВ КИБЕРСТАЛКИНГА <i>Vinogradova A., Hajrutdinova L.</i> CYBERVICTIMITY OF CYBERSTALKING PEOPLE	133
<i>Виноградова А. Ю.</i> АКТУАЛЬНЫЕ ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЦИФРОВОГО ПРОФИЛЯ <i>Vinogradova A.</i> CURRENT FEATURES OF THE LEGAL REGULATION OF THE DIGITAL PROFILE	136
<i>Вишняков И. С.</i> ЗАКОНОДАТЕЛЬНЫЕ ПРЕДЛОЖЕНИЯ США В СФЕРЕ РЕГУЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ЦИФРОВЫХ ПЛАТФОРМ <i>Vishnyakov I.</i> US LEGISLATIVE PROPOSALS IN THE FIELD OF REGULATION OF DIGITAL PLATFORMS	140
<i>Гаврилова В. Д.</i> ВНЕДРЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМУ ПРАВОВОГО РЕГУЛИРОВАНИЯ: АНАЛИЗ ОТЕЧЕСТВЕННОГО И ЗАРУБЕЖНОГО ОПЫТА <i>Gavrilova V.</i> IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE INTO THE SYSTEM OF LEGAL REGULATION: ANALYSIS OF DOMESTIC AND FOREIGN EXPERIENCE.....	146
<i>Гашимов Т. А.</i> ВЛИЯНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА ВЗАИМОДЕЙСТВИЕ ГОСУДАРСТВА И ГРАЖДАНСКОГО ОБЩЕСТВА <i>Gashimov T.</i> THE IMPACT OF DIGITAL TECHNOLOGIES ON THE INTERACTION BETWEEN THE STATE AND CIVIL SOCIETY.....	153
<i>Гладкова Т. С.</i> ОБ УЧАСТИИ ГРАЖДАН В УПРАВЛЕНИИ ВЫЗОВАМИ ЦИФРОВОЙ ЭКОНОМИКИ КОНСТИТУЦИОННЫМ ПРАВООТНОШЕНИЯМ <i>Gladkova T.</i> ABOUT THE IMPORTANCE OF CITIZENS' PARTICIPATION IN MANAGING THE CHALLENGES OF THE DIGITAL ECONOMY TO CONSTITUTIONAL RELATIONSHIPS	156
<i>Глотов Н. В.</i> ОСОБЕННОСТИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ <i>Glotov N.</i> FEATURES OF THE USE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL PROCEEDINGS	157

<i>Горина Т. В.</i> ЦИФРОВЫЕ ТЕХНОЛОГИИ В ИНДУСТРИИ ТУРИЗМА В СИСТЕМЕ ПРАВОВЫХ ОТНОШЕНИЙ <i>Gorinova T.</i> DIGITAL TECHNOLOGIES IN THE TOURISM INDUSTRY IN THE SYSTEM OF LEGAL RELATIONS	163
<i>Горшкова М. А., Драгун Д. С.</i> ЭЛЕКТРОННОЕ ПРАВОСУДИЕ В РЕСПУБЛИКЕ БЕЛАРУСЬ <i>Gorshkova M., Dragun D.</i> E-JUSTICE IN THE REPUBLIC OF BELARUS	168
<i>Гришин К. И.</i> РАЗВИТИЕ СЕМЕЙНОГО ПРАВА В РОССИЙСКОЙ ФЕДЕРАЦИИ В КОНТЕКСТЕ ЗАКЛЮЧЕНИЯ И РАСТОРЖЕНИЯ БРАКА В ОНЛАЙН-ФОРМАТЕ <i>Grishin K.</i> DEVELOPMENT OF FAMILY LAW IN THE RUSSIAN FEDERATION IN THE CONTEXT OF CONCLUSION AND DIVORCE OF MARRIAGE IN ON-LINE FORMAT	171
<i>Губаева Е. А.</i> ЭКСПЕРИМЕНТАЛЬНЫЕ ПРАВОВЫЕ РЕЖИМЫ ОСУЩЕСТВЛЕНИЯ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ЦИФРОВЫХ ИННОВАЦИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ <i>Gubaeva E.</i> EXPERIMENTAL LEGAL REGIMES OF ENTREPRENEURIAL ACTIVITY IN THE FIELD OF DIGITAL INNOVATIONS IN THE RUSSIAN FEDERATION	173
<i>Гуляев Т. Р., Решетников И. А., Скрылев И. Д.</i> О ПРИНАДЛЕЖНОСТИ ИСКЛЮЧИТЕЛЬНЫХ ПРАВ НА РЕЗУЛЬТАТЫ, СОЗДАННЫЕ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ <i>Gulyaev T., Reshetnikov I., Skrylev I.</i> ON THE OWNERSHIP OF EXCLUSIVE RIGHTS TO RESULTS CREATED BY ARTIFICIAL INTELLIGENCE	181
<i>Дамдинова Э. Б., Тимошенко Ю. В.</i> РАСПРОСТРАНЕННОЕ КИБЕРПРЕСТУПЛЕНИЕ СОВРЕМЕННОСТИ – ФИШИНГ <i>Damdinova E., Timoshenko Yu.</i> A COMMON CYBERCRIME OF OUR TIME IS PHISHING	185
<i>Данакари Л. Р., Ермоченко К. П., Ивентьев С. И.</i> ДУХОВНО-ПРАВСТВЕННЫЙ И ПРАВОВОЙ АСПЕКТЫ СВОБОДЫ ЛИЧНОСТИ В ЦИФРОВУЮ ЭПОХУ <i>Danakari L., Ermochenko K., Iventev S.</i> SPIRITUAL, MORAL AND LEGAL ASPECTS OF INDIVIDUAL FREEDOM IN THE DIGITAL AGE	191
<i>Дементьева М. В.</i> К ВОПРОСУ О ПРИВЛЕЧЕНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ <i>Dementeva M.</i> TO THE QUESTION OF ATTRACTION OF ARTIFICIAL INTELLIGENCE TO CRIMINAL RESPONSIBILITY	199

Демиденко Д. В. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ РЕШАЕТ СУДЬБУ ЧЕЛОВЕКА: НАШЕ БУДУЩЕЕ ИЛИ ФАНТАЗИЯ? <i>Demidenko D. ARTIFICIAL INTELLIGENCE DECIDES PERSON'S FATE: OUR FUTURE OR FANTASY?</i>	203
Дружинина Е. И., Шабалина Д. А. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ЖИЗНИ СОВРЕМЕННОГО ОБЩЕСТВА <i>Druzhinina E., Shabalina D. ARTIFICIAL INTELLIGENCE IN THE LIFE OF MODERN SOCIETY</i>	213
Дудкин Д. А. ПУБЛИЧНО-ПРАВОВЫЕ И ЧАСТНОПРАВОВЫЕ СВОЙСТВА ЦИФРОВЫХ ТЕХНОЛОГИЙ, ПРИМЕНЯЮЩИХСЯ В РАМКАХ ОКАЗАНИЯ ДЕТЕКТИВНЫХ УСЛУГ <i>Dudkin D. PROBLEMS OF THE COMPETITIVE ENVIRONMENT IN THE PROVISION OF DETECTIVE SERVICES IN THE RUSSIAN FEDERATION.....</i>	221
Дюмина В. Э. ПАРАДИГМА ЧАСТНОГО ПРАВА В ИННОВАЦИОННУЮ ЭПОХУ: ЦИФРОВОЙ ОБРАЗ ПРОИЗВЕДЕНИЯ КАК НОВЫЙ ОБЪЕКТ ГРАЖДАНСКИХ ПРАВ <i>Dyutina V. PARADIGM OF PRIVATE LAW IN THE INNOVATIVE AGE: DIGITAL IMAGE OF A WORKS AS A NEW OBJECT OF CIVIL RIGHTS.....</i>	226
Евстефеева М. С. ВИРТУАЛЬНАЯ СОБСТВЕННОСТЬ В МЕТАВСЕЛЕННОЙ <i>Evstefeeva M. VIRTUAL PROPERTY IN THE METAVERSE.....</i>	236
Ермоченко К. П. СМАРТ-КОНТРАКТ СЕГОДНЯ: «УМНЫЙ ДОГОВОР» В СИСТЕМЕ ПРАВОВЫХ ОТНОШЕНИЙ ИЛИ МАЛОЭФФЕКТИВНЫЙ «ЦИФРОВОЙ ЗАРОДЫШ» НЕСАМОСТОЯТЕЛЬНОЙ ДОГОВОРНОЙ КОНСТРУКЦИИ <i>Ermochenko K. SMART CONTRACT TODAY: A "SMART CONTRACT" IN THE SYSTEM OF LEGAL RELATIONS, OR AN INEFFECTIVE "DIGITAL GERM" OF AN INDEPENDENT CONTRACTUAL STRUCTURE</i>	240
Журавлева А. Л. ЛИЦЕНЗИРОВАНИЕ ОНЛАЙН-ОБРАЗОВАНИЯ КАК ЭЛЕМЕНТА ЦИФРОВЫХ ТЕХНОЛОГИЙ <i>Zhuravleva A. LICENSING ONLINE EDUCATION, AS AN ELEMENT OF DIGITAL TECHNOLOGY.....</i>	244
Захаров И. В. ОРГАНЫ И УЧРЕЖДЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: РЕГИОНАЛЬНЫЙ АСПЕКТ <i>Zaharov I. BODIES AND INSTITUTIONS IN THE FIELD OF INFORMATION TECHNOLOGY: REGIONAL ASPECT.....</i>	248

<i>Зубкова В. В.</i> ОСНОВНЫЕ ТЕНДЕНЦИИ ПРАВОВОГО РЕГУЛИРОВАНИЯ РЫНКА БАНКОВСКИХ УСЛУГ В ЕАЭС В УСЛОВИЯХ ЦИФРОВИЗАЦИИ <i>Zubkova V.</i> THE MAIN TRENDS IN THE LEGAL REGULATION OF THE BANKING SERVICES MARKET IN THE EURASIAN ECONOMIC UNION (EAEU) IN THE CONTEXT OF DIGITALIZATION	256
<i>Ивардава Л. И.</i> СУБЪЕКТ ПРАВА В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ В РОССИИ <i>Ivardava L.</i> THE SUBJECT OF LAW IN THE CONTEXT OF THE DEVELOPMENT OF THE DIGITAL ECONOMY IN RUSSIA	262
<i>Иллюк П. А.</i> ПРАВОВОЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: ОПЫТ ИНДИИ <i>Ilyuk P.</i> LEGAL REGULATION IN THE FIELD OF INFORMATION TECHNOLOGY: THE EXPERIENCE OF INDIA	265
<i>Иманалиева М. А.</i> ОСОБЕННОСТИ РЕГУЛИРОВАНИЯ ОНЛАЙН-ИГР ЧЕРЕЗ ПРИЗМУ ЗАЩИТЫ ПРАВ И ИНТЕРЕСОВ НЕСОВЕРШЕННОЛЕТНИХ <i>Imanalieva M.</i> FEATURES OF REGULATION OF ONLINE GAMES THROUGH THE PRISM OF PROTECTION OF THE RIGHTS AND INTERESTS OF MINORS	269
<i>Иртегова А. Е.</i> О ПРИДАНИИ ОФИЦИАЛЬНОГО СТАТУСА МАЙНИНГУ В РОССИИ <i>Irtegova A.</i> ON GIVING AN OFFICIAL STATUS TO MINING IN RUSSIA	276
<i>Калашников Н. А., Козлова О. Е.</i> АНАЛИЗ И ВЫЯВЛЕНИЕ ЭКСТРЕМИСТСКИХ РИСКОВ В РАБОТЕ НЕЙРОСЕТЕЙ <i>Kalashnikov N., Kozlova O.</i> ANALYSIS AND IDENTIFICATION OF EXTREMIST RISKS IN THE WORK OF NEURAL NETWORKS	280
<i>Калинюк Е. В.</i> ЦИФРОВЫЕ ТЕХНОЛОГИИ В НОТАРИАЛЬНОЙ ЗАЩИТЕ ПРАВ ПРЕДПРИНИМАТЕЛЕЙ <i>Kalinyuk E.</i> DIGITAL TECHNOLOGIES IN THE NOTARIAL PROTECTION OF THE RIGHTS OF ENTREPRENEURS	285
<i>Калмыкова М. А.</i> ОТСУТСТВИЕ ЕДИНЫХ СТАНДАРТОВ РАБОТЫ МАРКЕТПЛЕЙСОВ КАК ПРАВОВАЯ ПРОБЛЕМА <i>Kalmykova M.</i> THE LACK OF UNIFORM STANDARDS FOR THE OPERATION OF MARKETPLACES AS A LEGAL PROBLEM	289

<i>Кантаев М. А.</i> ДЕПОНИРОВАНИЕ ОБЪЕКТОВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ С ПРИМИНЕНИЕМ ТЕХНОЛОГИИ-БЛОКЧЕЙН <i>Kantaev M.</i> DEPOSITING OF OBJECTS OF INTELLECTUAL PROPERTY USING BLOCKCHAIN TECHNOLOGY.....	291
<i>Каргин М. Н., Хижняков Д. В., Щенин Н. Н.</i> ПРОБЛЕМЫ ВНЕДРЕНИЯ ДИСТАНЦИОННОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ В ПРАВОВУЮ СИСТЕМУ ИЗБИРАТЕЛЬНОГО ЗАКОНОДАТЕЛЬСТВА И ЕГО ПРИМЕНЕНИЯ НА ПРАКТИКЕ <i>Kargin M., Hizhnyakov D., Shchenin N.</i> PROBLEMS OF INTRODUCING THE ONLINE VOTING IN THE LEGAL SYSTEM OF THE ELECTORAL LEGISLATION AND ITS APPLICATION IN PRACTICE.....	299
<i>Каримова Г. Ю., Лежнев С. В.</i> ЦИФРОВАЯ ИДЕНТИФИКАЦИЯ НАЛОГОПЛАТЕЛЬЩИКА <i>Karimova G. Yu., Lezhnev S.</i> DIGITAL TAXPAYER IDENTIFICATION.....	309
<i>Карпов А. Н.</i> ПРОБЛЕМЫ ЦИФРОВИЗАЦИИ ПРАВА В РОССИИ <i>Karpov A.</i> PROBLEMS OF DIGITALIZATION OF LAW IN RUSSIA	315
<i>Каюмова Ф. Х.</i> ЗАЩИТА ЛИЧНОЙ ИНФОРМАЦИИ В ЦИФРОВУЮ ЭПОХУ <i>Kayumova F.</i> PROTECTING PERSONAL INFORMATION IN THE DIGITAL AGE.....	318
<i>Киракосов В. Б.</i> КРИПТОВАЛЮТА: ОПЫТ ПРАВОВОГО РЕГУЛИРОВАНИЯ В РОССИИ И ЗАРУБЕЖНЫХ ГОСУДАРСТВАХ <i>Kirakosov V.</i> CRYPTOCURRENCY: EXPERIENCE OF LEGAL REGULATION IN RUSSIA AND FOREIGN STATES.....	322
<i>Кирей С. С.</i> ЦИФРОВЫЕ ТЕХНОЛОГИИ В ПРОЦЕДУРЕ ЗАКЛЮЧЕНИЯ СДЕЛОК И РЕГИСТРАЦИИ ПРАВ НА НЕДВИЖИМОСТЬ <i>Kirei S.</i> DIGITAL TECHNOLOGIES IN THE PROCEDURE OF TRANSACTIONS AND REGISTRATION OF RIGHTS TO REAL ESTATE.....	335
<i>Кирилова А. Д.</i> АНАЛИЗ НАЛОГОВОГО СТИМУЛИРОВАНИЯ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ <i>Kirilova A.</i> ANALYSIS OF TAX INCENTIVES FOR INNOVATION.....	341
<i>Киселева Н. Н., Афонин А. Н.</i> ЦИФРОВИЗАЦИЯ ЧАСТНЫХ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ С ТОЧКИ ЗРЕНИЯ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ <i>Kiseleva N., Afonin A.</i> DIGITALISATION OF PRIVATE HEALTHCARE FACILITIES FROM THE PERSPECTIVE OF PERSONAL DATA PROTECTION LEGISLATION.....	349

<i>Комова М. Ю.</i> ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ VPN-ТЕХНОЛОГИЙ В РОССИИ <i>Kotova M.</i> LEGAL REGULATION OF THE USE OF VPN TECHNOLOGIES IN RUSSIA.....	354
<i>Корепанова Е. С.</i> МЕЖДУНАРОДНЫЕ РАСЧЕТЫ В КРИПТОВАЛЮТЕ И УКЛОНЕНИЕ ОТ ИСПОЛНЕНИЯ ОБЯЗАННОСТИ ПО РЕПАТРИАЦИИ ДЕНЕЖНЫХ СРЕДСТВ: ПРОБЛЕМЫ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ <i>Korepanova E.</i> INTERNATIONAL SETTLEMENTS IN CRYPTOCURRENCY AND EVASION OF THE OBLIGATION TO REPATRIATE MONEY RESOURCE: PROBLEMS OF CRIMINAL LIABILITY	356
<i>Корчагина К. С.</i> ПРАВОВАЯ ОХРАНА ОБЪЕКТОВ АВТОРСКОГО ПРАВА, СОЗДАНЫХ ИСКУССТВЕННЫХ ИНТЕЛЛЕКТОМ <i>Korchagina K.</i> LEGAL PROTECTION OF COPYRIGHT ITEMS CREATED BY ARTIFICIAL INTELLIGENCE.....	361
<i>Костылева У. В.</i> ОСНОВНЫЕ ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ПРАВОСУБЪЕКТНОСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА <i>Kostyleva U.</i> THE MAIN APPROACHES TO DETERMINING THE LEGAL PERSONALITY OF ARTIFICIAL INTELLIGENCE	365
<i>Кочетова А. О., Сарычева С. А.</i> ПАТЕНТНОЕ ПРАВО В ЦИФРОВОЙ СРЕДЕ <i>Kochetova A., Sarycheva S.</i> PATENT LAW IN THE DIGITAL ENVIRONMENT.....	372
<i>Кошлыкова Ю. А.</i> ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ 3D-ТЕХНОЛОГИЙ ДЛЯ РЕШЕНИЯ КРИМИНАЛИСТИЧЕСКИХ ЗАДАЧ <i>Koshlykova Yu.</i> POSSIBILITIES OF USING 3D TECHNOLOGIES TO SOLVE FORENSIC PROBLEMS	377
<i>Кулагина А. В.</i> ПОНЯТИЕ АЛГОРИТМИЗАЦИИ И ЕЕ ВЛИЯНИЕ НА СФЕРУ ТРУДА <i>Kulagina A.</i> THE CONCEPT OF ALGORITHMIZATION AND ITS IMPACT ON THE SPHERE OF WORK.....	382
<i>Куликова А. Н.</i> ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ПРАВОВЫХ ОТНОШЕНИЙ <i>Kulikova A.</i> DIGITAL TECHNOLOGIES IN THE SYSTEM OF LEGAL RELATIONS.....	389

Кунцов Н. С. ПРОБЛЕМА ОПРЕДЕЛЕНИЯ
ТЕОРЕТИКО-ПРАВОВОЙ СУЩНОСТИ НЕКОТОРЫХ ЭЛЕМЕНТОВ
ВИРТУАЛЬНОГО МИРА В КОНТЕКСТЕ ОТНЕСЕНИЯ
ИХ К ОБЪЕКТАМ ГРАЖДАНСКИХ ПРАВ |
Kircov N. THE PROBLEM OF DETERMINING
THE THEORETICAL AND LEGAL ESSENCE OF SOME VIRTUAL
WORLD OBJECTS IN THE CONTEXT OF THEIR ATTRIBUTION
TO OBJECTS OF CIVIL RIGHTS 393

Научное издание

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
I Международной научно-практической конференции

23 сентября 2022 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*

Главный редактор *Г. Я. Дарчинова*
Редакторы: *Г. А. Тарасова, Е. А. Маннапова*
Технический редактор *О. А. Аймурзаева*
Дизайн обложки: *Г. И. Загретдинова*

ISBN 978-5-8399-0770-6



Подписано в печать 27.10.2022. Формат 60×84/16.
Гарнитура PT Astra Serif, 9. Усл. печ. л. 23,94. Уч.-изд. л. 19.
Тираж 2000 экз. Заказ № 109.



Издательство «Познание» Казанского инновационного университета им. В. Г. Тимирязова
420111, г. Казань, ул. Московская, 42; тел. (843) 231-92-90; e-mail: zaharova@ieml.ru

Отпечатано с готового оригинал-макета в типографии ООО «ТЦО «Таглимат»
420108, г. Казань, ул. Зайцева, 17



НАУРР

Национальная Ассоциация
Участников Рынка Робототехники

ICTONLINE

ICT2GO

УВЕРЕННОСТЬ В КАЖДОМ РЕШЕНИИ



ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ



JOURNAL OF DIGITAL
TECHNOLOGIES AND LAW

ХАЙТЕК

it.world

technoverity

International Journal of
Law in Changing World

РАПСИ Российское агентство
правовой и судебной информации

