Как цитировать: Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции (г. Казань, 22 сентября 2023 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 6. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – 476 с. EDN: IDLEUI. DOI: http://dx.doi.org/10.21202/978-5-8399-978-5-8399-0819-2_476

For citation: Digital Technologies and Law: collection of scientific articles of the II International Scientific and Practical Conference (Kazan, 2023, September 22) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 6. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2023. – 476 p. EDN: IDLEUI. DOI: http://dx.doi.org/10.21202/978-5-8399-978-5-8399-0819-2_476

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
II Международной научно-практической конференции

22 сентября 2023 г.
г. Казань

В шести томах
Том 6

Казань ■ КИУ ИЗДАТЕЛЬСТВО «ПОЗНАНИЕ» ■ 2023

DIGITAL TECHNOLOGIES AND LAW

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

2023, September 22
Kazan

In 6 volumes
Volume 6

Kazan ■ KIU "POZNANIYE" PUBLISHERS ■ 2023

УДК 004:34(063)
ББК 67с51я43
Ц75

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

Ц75 **Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции** (г. Казань, 22 сентября 2023 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 6. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – 476 с. EDN: IDLEUI. DOI: http://dx.doi.org/10.21202/978-5-8399-0819-2_476.
ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0819-2 (Том 6)

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

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

Научные труды представленного тома охватывают тематику специальных вопросов по регулированию и охране общественных отношений, возникающих или связанных с развитием цифровых технологий.

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

УДК 004:34(063)
ББК 67с51я43

ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0819-2 (Том 6)

UDC 004:34(063)
LBC 67c51я43

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

Digital Technologies and Law: collection of scientific papers of the II International Scientific and Practical Conference (Kazan, 2023, September 22) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 6. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2023. – 476 p. EDN: IDLEUI. DOI: http://dx.doi.org/10.21202/978-5-8399-0819-2_476
ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0819-2 (Vol. 6)

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

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

The scientific works of the presented volume cover the subject of special issues on the regulation and protection of social relations arising or related to the development of digital technologies.

The ideas and proposals reflected in the multi-volume publication in their entirety are the key to understanding the intellectual map of meanings that will be of interest to legal scholars and experts in the field of digital technologies, practicing lawyers, representatives of law-making and law enforcement bodies, government officials and participants in the real sector of the economy, including developers and manufacturers of products of digital technology achievements, young student researchers, undergraduates and graduate students, everyone interested in the mutual influence of digital technologies and law.

UDC 004:34(063)
LBC 67c51я43

ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0819-2 (Vol. 6)

СПЕЦИАЛЬНЫЕ ВОПРОСЫ РЕГУЛИРОВАНИЯ И ОХРАНЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ

SPECIAL ISSUES OF REGULATION AND PROTECTION OF DIGITAL TECHNOLOGIES

С. А. Агамагомедова,
кандидат юридических наук, доцент,
Институт государства и права
Российской академии наук

ЦИФРОВИЗАЦИЯ ТАМОЖЕННОГО КОНТРОЛЯ ТОВАРОВ, СОДЕРЖАЩИХ ОБЪЕКТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Аннотация. Целью исследования является выделение особенностей цифрвизации таможенного контроля товаров, содержащих объекты интеллектуальной собственности. На основе анализа данного направления таможенного контроля сделаны выводы о его специфике, связанной с электронным таможенным декларированием, цифровыми государственными услугами, сервисом «Правообладатели» в личном кабинете участника внешнеэкономической деятельности и другими факторами. Цифровизация процедур как самого таможенного контроля, так и предшествующих и последующих процедур направлена на повышение эффективности трансграничной защиты интеллектуальных прав.

Ключевые слова: таможенный контроль, объекты интеллектуальной собственности, параллельный импорт, правообладатель, цифровые сервисы, таможенное декларирование, управление рисками

DIGITALIZATION OF CUSTOMS CONTROL OF GOODS CONTAINING INTELLECTUAL PROPERTY OBJECTS

Abstract. The purpose of the study is to highlight the features of the digitalization of customs control of goods containing intellectual property. Based on the analysis of this area of customs control, conclusions were drawn about its specifics related to electronic customs declaration, digital public services, the “Copyright Holders” service in the personal account of a participant in foreign economic activity, and other factors. The digitalization of the procedures of both the customs control itself and the previous and subsequent procedures is aimed at increasing the efficiency of cross-border protection of intellectual property rights.

Keywords: customs control, intellectual property objects, parallel import, copyright holder, digital services, customs declaration, risk management

Введение. Цифровизация активно проникает в сферу государственного управления. Данная сфера стремительно трансформируется и генерирует качественно новые формы взаимодействия государства с гражданами и организациями. Ученые справедливо констатируют тот факт, что под воздействием информационно-коммуникационных технологий государственное управление становится качественно иным, открытость и участие общества меняют саму его концепцию [9]. Особенно явственно мы наблюдаем изменение присутствия государства в экономике, которая сегодня является цифровой экономикой, экономикой знаний, цифровой интеллектуальной экономикой [4]. При этом меняются базовые управленческие функции государственного управления, в частности контроль и надзор. Трансформация государственного контроля и надзора в условиях цифровизации экономики свидетельствует о приобретении государственным управлением свойств управления сетевого, доминировании не двустороннего, а многостороннего взаимодействия, причем взаимодействия исключительно в цифровом формате [1]. Рассмотрим процессы цифровизации применительно к таможенному контролю товаров, содержащих объекты интеллектуальной собственности, который выступает одновременно частью государственного контроля в области создания, использования и защиты прав на объекты интеллектуальной собственности, с другой стороны, является структурным элементом, самостоятельным направлением таможенного контроля как вида государственного контроля.

Основная часть. Эффективная защита прав на объекты интеллектуальной собственности определенным образом обслуживает, обеспечивает экономические отношения. Прежде всего это касается объектов промышленной собственности. Механизмы таможенной (или трансграничной) защиты интеллектуальных прав прошли в нашей стране достаточно показательный путь развития на протяжении последних трех десятилетий [3]. Поэтапно формируется нормативно-правовая база подобной защиты, основанная на международных стандартах трансграничных аспектов защиты интеллектуальных прав (прежде всего, Соглашения ТРИПС [8]); обособляется в качестве самостоятельной функции компетенция таможенных органов по защите таких прав; детализируется регламентация процедур таможенного контроля товаров, содержащих объекты интеллектуальной собственности, уточняется перечень последних. Последние годы подобной эволюции неразрывно связаны с цифровизацией процедур рассматриваемого вида таможенного контроля. В связи с этим следует обратить внимание на несколько особенностей подобной цифровизации.

Во-первых, оцифровывается не только сам таможенный контроль рассматриваемой категории товаров, но и обслуживающая его, неразрывно связанная с ним функция по предоставлению соответствующих услуг правообладателям для эффективной защиты своих исключительных прав при трансграничном перемещении товаров. Речь идет, прежде всего, о предоставлении государственной услуги по ведению таможенного реестра объектов интеллектуальной собственности (ТРОИС) [7]. Фактически ТРОИС (его аналог в виде списка правообладателей) ведется с 1999 года, на нормативном уровне его ведение впервые закреплено в Таможенном кодексе РФ 2003 года. Несмотря на то, что таможенные органы РФ

принимают меры по защите прав на объекты интеллектуальной собственности и в отношении объектов, не включенных в ТРОИС (процедура «ex officio»), именно ТРОИС на протяжении последних десятилетий выступает основой таможенного контроля рассматриваемой категории товаров. Неоднозначным является вопрос об отнесении ведения ТРОИС к государственным услугам (в административном регламенте предшествующего периода ведение ТРОИС позиционировалось ФТС России в качестве государственной функции). В настоящее время ведение ТРОИС позиционируется в качестве услуги и данная услуга предоставляется в электронном виде. Более того, само пользование ТРОИС максимально упрощено, позволяет в режиме реального режима поиска работать с более чем шестью тысячами объектов интеллектуальной собственности [11].

Во-вторых, цифровизация рассматриваемого направления таможенного контроля отражена в создании и функционировании специализированного сервиса для правообладателей – личного кабинета правообладателя. Сервис «Правообладатели» личного кабинета участника ВЭД функционирует на официальном сайте ФТС России [5]. Работа в данном сервисе предусматривает всего два предварительных шага: получение усиленной электронной подписи и регистрацию в Личном кабинете участника ВЭД. Данный сервис предназначен для российских правообладателей, их представителей и доверенных лиц, а также для их лицензиатов и (или) уполномоченных импортеров. Он позволяет заинтересованным правообладателям оперативно взаимодействовать с таможенными органами в рамках, к примеру, приостановления срока выпуска товаров, обладающих признаками контрафактных.

В-третьих, цифровизации подвергаются операции как до контрольно-надзорного взаимодействия в рамках защиты интеллектуальных прав, так и после него. При выявлении в рамках такого таможенного контроля признаков нарушений прав на объекты интеллектуальной собственности таможенные органы возбуждают дела об административных правонарушениях и расследуют их. В настоящее время взаимодействие участников административного производства также происходит в личном кабинете участника ВЭД, с помощью которого многие процессуальные действия в рамках расследования дела об административном правонарушении также возможны в цифровом формате.

Важнейшим условием цифровизации таможенного контроля товаров, содержащих объекты интеллектуальной собственности и одновременно стадией цифровизации в таможенной сфере в целом выступает институт электронного таможенного декларирования. Электронное декларирование – базовое условие цифровизации документального текущего таможенного контроля. В настоящее время, когда более 99 % всех таможенных деклараций на товары составляют электронный декларации, таможенный контроль на этапе до выпуска товаров практически полностью оцифрован.

Отдельно следует остановиться на системе управления рисками (СУР) при таможенном контроле товаров, содержащих объекты интеллектуальной собственности. СУР практически изначально внедрена, фактически «прошита» в процедуры текущего таможенного контроля. Критерии отнесения товаров и иных

объектов таможенного контроля к объектам высокого уровня риска нарушения таможенного законодательства инкорпорированы в информационную систему СУР и позволяют оперативно применять меры по минимизации таких рисков, в том числе и применительно к правам на объекты интеллектуальной собственности.

Упомянутая выше процедура «ex officio» в деятельности таможенных органов РФ также основана на информационно-коммуникационных технологиях. Основой данной процедуры выступает наличие у таможенного органа информации о зарегистрированном в РФ объекте интеллектуальной собственности (речь идет о товарных знаках, знаках обслуживания, наименованиях мест происхождения товаров и географических указаниях). Наличие данной информации у таможенного органа основано на системе межведомственного взаимодействия между ФТС России и Роспатентом. Должностные лица таможенных органов имеют доступ к информационным базам Роспатента, что позволяет им оперативно реагировать на потенциальные нарушения исключительных прав.

Особенностью цифровизации рассматриваемого направления таможенного контроля в последние годы стало решение проблемы параллельного импорта. Вопросы исчерпания прав в рамках экономической интеграции и вне ее нами рассматривались в период, предшествующий созданию ЕАЭС [2]. Мировая практика свидетельствует о том, что современные государства по-разному решают для себя вопрос исчерпания исключительных прав с учетом того, что Соглашение ТРИПС оставляет этот аспект защиты интеллектуальных прав на усмотрение национального законодателя [12]. Усиление санкционного давления на Россию повысил внимание к данным механизмам, позволив рассматривать их в качестве меры поддержки отечественной экономики. Как известно, Правительство Российской Федерации в марте 2022 года частично легализовало параллельный импорт в отношении ряда правообладателей из недружественных государств. Данный список регулярно пересматривается и актуализируется с учетом текущей экономической ситуации [6]. Представляется, что таможенный контроль товаров, содержащих объекты интеллектуальной собственности, традиционно направленный на выявление контрафактной продукции, в условиях частичного введения международного принципа исчерпания прав требует цифровой поддержки и в части обеспечения беспрепятственного трансграничного перемещения так называемых «оригинальных» товаров в целях удовлетворения потребительского спроса на них. Представляется, что и в механизмах ведения ТРОИС, и в инструментах по контролю товаров, перемещаемых в рамках параллельного импорта, целесообразно использование технологии распределенного реестра. Ученые справедливо отмечают, что технология распределенного реестра, в том числе блокчейн, имеет явные преимущества, которые могут повлиять на качество государственного управления. Они обращают внимание на оперативность взаимодействия и отсутствие в нем субъективного фактора, на его открытость и прозрачность [10].

Заключение. Цифровизация трансформирует все направления таможенного контроля товаров, в том числе и товаров, содержащих объекты интеллектуальной собственности. Нами были выделены особенности подобного направления таможенного контроля, которые связаны с цифровизацией сопутствующих

государственных услуг, созданием и функционированием цифрового сервиса «Правообладатели» в личном кабинете участника ВЭД, межведомственным взаимодействием с иными федеральными органами исполнительной власти, задействованными в механизме защиты исключительных прав на объекты интеллектуальной собственности. Можно констатировать цифровую трансформации взаимодействия между участниками данного механизма как на этапе, предшествующем рассматриваемому направлению таможенного контроля (процедуры ведения ТРОИС), так и на этапе после контроля, связанном с выявлением признаков административного правонарушения и административным расследованием. Цифровизация таможенного контроля товаров, содержащих объекты интеллектуальной собственности, позволяет повысить эффективность данного направления контроля и обеспечить полноценную защиту частных и публичных интересов при трансграничном перемещении товаров.

Список литературы

1. Агамагомедова С. А. Государственный контроль и надзор в условиях цифровизации экономики // Вестник Нижегородского университета им. Н. И. Лобачевского. 2020. № 3. С. 79–85.

2. Агамагомедова С. А. Проблемы «параллельного импорта» в правоприменительной практике таможенных органов Таможенного союза России, Белоруссии и Казахстана // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2013. № 3(27). С. 25–35.

3. Агамагомедова С. А. Трансграничная защита интеллектуальных прав: эволюция регулирования и проблемы правоприменения // Труды по интеллектуальной собственности. 2023. Т. 45, № 2. С. 32–43.

4. Беликова К. М. Цифровая интеллектуальная экономика: понятие и особенности правового регулирования (теоретический аспект) // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2018. № 8(99). С. 82–85.

5. Личный кабинет участника ВЭД. Официальный сайт ФТС России. URL: https://customs.gov.ru/storage/document/document_image/2022-07/11/info_11_07.jpg

6. Приказ Минпромторга России от 19.04.2022 № 1532 (ред. от 02.03.2023) «Об утверждении перечня товаров (групп товаров), в отношении которых не применяются положения подпункта 6 статьи 1359 и статьи 1487 Гражданского кодекса Российской Федерации при условии введения указанных товаров (групп товаров) в оборот за пределами территории Российской Федерации правообладателями (патентообладателями), а также с их согласия» // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

7. Приказ ФТС России от 28.01.2019 № 131 «Об утверждении Административного регламента Федеральной таможенной службы по предоставлению государственной услуги по ведению таможенного реестра объектов интеллектуальной собственности» // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru

8. Соглашение по торговым аспектам прав интеллектуальной собственности» (ТРИПС/TRIPS) (Заключено в г. Марракеше 15.04.1994) // Собрание законодательства РФ. 10 сентября 2012 г. № 37 (приложение, ч. VI). С. 2818–2849.

9. Талапина Э. В. Государственное управление в информационном обществе (правовой аспект): монография. М.: Юриспруденция, 2015. 192 с.

10. Талапина Э. В., Ефремов А. А., Черешнева И. А. Перспективы применения технологии распределенного реестра для осуществления отдельных государственных функций // Административное право и процесс. 2019. № 11. С. 41–44.

11. Таможенный реестр объектов интеллектуальной собственности. Официальный сайт ФТС России. URL: https://customs.gov.ru/registers/objects-intellectual-property

12. Grigoriadis, L. G. (2014). Exhaustion of Trademark Rights and Legality of Parallel Imports in the Ten Most Important Trading Partners of the EU. URL: https://doi.org/10.1007/978-3-319-04795-9

Ф. Г. Аминев,
доктор юридических наук, профессор,
Уфимский университет науки и технологий
А. И. Янгиров,
преподаватель,
Уфимский университет науки и технологий

ПРОБЛЕМЫ ВНЕДРЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В СУДЕБНО-ЭКСПЕРТНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Проанализированы ключевые проблемы процесса цифровизации в производстве судебных экспертиз в России. Показано, что для повышения качества судопроизводства на современном этапе необходимо повысить эффективность судебно-экспертной деятельности путем внедрения инновационных цифровых технологий в производство судебных экспертиз. Рассмотрены разновидности экспертных исследований, в которых используются и разрабатываются высокотехнологичные средства и методы исследования. Предложены рекомендации по внедрению самых передовых экспертных технологий в молекулярно-генетическую, компьютерно-техническую и иные классификационные группы судебных экспертиз.

Ключевые слова: цифровизация, инновационные технологии, программно-компьютерный комплекс, судебно-экспертная деятельность, искусственный интеллект

PROBLEMS OF INTRODUCTION OF DIGITAL TECHNOLOGIES IN FORENSIC EXPERTISE

Abstract. The key problems of the digitalization process in the production of forensic examinations in Russia are analyzed. It is shown that in order to improve the

quality of legal proceedings at the present stage, it is necessary to increase the efficiency of forensic expert activity by introducing innovative digital technologies into the production of forensic examinations. The types of expert research in which high-tech research tools and methods are used and developed are considered. Recommendations on the introduction of the most advanced expert technologies in molecular genetic, computer-technical and other classification groups of forensic examinations are proposed.

Keywords: digitalization, innovative technologies, software and computer complex, forensic activity, artificial intelligence

Введение. Из 1 966 795 преступлений, зарегистрированных на территории Российской Федерации в течение 12 месяцев 2022 г., 522 065 преступлений совершено с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 0,8 % больше, чем за аналогичный период прошлого года [1] (еще больше правонарушений остались латентными).

Поэтому в условиях продолжающегося реформирования судопроизводства в условиях цифровизации и ускорения научно-технического прогресса, актуальным является вопрос использования в расследовании преступлений инновационных цифровых технологий судебно-экспертной деятельности.

Основная часть. Многочисленные инновационные процессы, происходящие в сфере судопроизводства в настоящее время, в, основном, сводятся к внедрению новейших технологий, связанных с цифровизацией. И имеющие место в практической судебно-экспертной деятельности прогрессивные изменения также в большей степени являются результатом использования цифровых технологий.

Инновационными разработками и внедрением цифровых технологий в методическое обеспечение судебно-экспертных исследований занимались: Н. П. Майлис – в трасологической экспертизе [2, 3], В. Ю. Владимиров – в судебно-баллистической экспертизе [4], Н. Н. Ильин – в судебной портретной экспертизе [5], Д. В. Бахтеев – в судебной почерковедческой экспертизе [6] и другие.

Научные исследования, проведенные Е. Р. Россинской, позволили сформировать учение о цифровизации судебно-экспертной деятельности, основой которой послужили современные принципы и закономерности функционирования инновационных методов и средств исследования объектов материального мира [7. С. 109–117].

В этом контексте полагаем, что организацию проведения геномной регистрации всего населения Российской Федерации следует проводить в соответствии с разработанной Е. Р. Россинской «системы информационно-компьютерного обеспечения судебно-экспертной деятельности, как методологической и технологической основы использования IT-технологий в экспертных исследованиях любых объектов судебной экспертизы» [8. С. 264].

И можно с удовлетворением констатировать, что уже несколько лет тому назад группой ученых-генетиков Института биохимии и генетики Уфимского Федерального исследовательского центра Российской академии наук (УФИЦ РАН)

разработан инновационный метод оцифровки в бинарном формате сразу всей четверки нуклеотидов в каждом «снипе» (с одновременным выявлением и анализом более коротких участков ДНК в застарелых, деградированных следах биологического происхождения). Остается надеяться на кратчайшие сроки внедрения этого метода в практику. Цифровая технология идентификационных молекулярно-генетических исследований намного дешевле той, что применяется в наши дни в государственных судебно-экспертных организациях с использованием программного комплекса CODIS производства США на основе STR-локусов. Уфимские ученые-генетики добились максимальной цифровизации: «объем информации при ДНК-идентификации личности с помощью снипов составит для одного человека не более одного килобайта (для сравнения: с помощью ныне практикуемых STR-локусов – более 200 килобайт)» [9. С. 97].

В настоящее время коллективом ученых Института права Уфимского университета науки и технологий разрабатываются методические и инструктивные указания по использованию в расследовании преступлений высокотехнологичного метода изотермической амплификации целевых фрагментов ДНК для выявления полиморфизма ДНК кошек и собак. Внедрение этого и других цифровых технологий приведет к опережающему импортозамещению и импортовытеснению.

В современной практической судебно-экспертной деятельности разработаны и реализованы интеграционные информационные системы (АБИС MBIS), в которых дактилоскопическая информация интегрирована с графическими изображениями лица человека, радужки глаз, расположением вен на руке, ДНК и т. д. Такие системы позволят на основе использования введенных в базу сведений и поиска в нейронных сетях оперативно устанавливать лиц, являющихся участниками преступных событий.

Результаты научных исследований последних лет в области использования цифровых технологий в судебно-экспертной деятельности свидетельствуют о том, что они могут реализовываться не только в судебно-экспертных исследованиях объектов, которые по своему происхождению являются высокотехнологичными (судебные экспертизы мобильных устройств, компьютерно-сетевые экспертиза и т. д.), но и в экспертных исследованиях традиционных объектов (судебные баллистические, лингвистические, автотехнические экспертизы и др.).

Заключение. Судебно-экспертная деятельность, являясь продуктом развития науки, в настоящее время становится требующей применения все более передовых научно-технических методов и средств, технологий. Поэтому необходимы исследования возможностей по использованию в судебно-экспертной деятельности методов и методик экспертного исследования на базе цифровых технологий с практической реализацией следующих мер:

1. Внесение в программы профессиональной подготовки судебных экспертов дисциплин, формирующих знания, умения и навыки экспертов по работе с нейронными сетями и большими данными (Big Data).

2. Реализация на практике мероприятий по формированию телекоммуникационной системы с базой данных, содержащих биометрические и оперативно-розыскные сведения «в рамках информационного обеспечения деятельности МВД РФ» [11. С. 96].

3. Придать ускорение процессу исполнения всех положений Указа Президента России от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации».

4. Необходимы научные исследования по разработке методик экспертного исследования объектов с применением цифровых технологий, в том числе, искусственного интеллекта.

5. Изучение и использованием передового опыта зарубежных коллег по применению в судебно-экспертных исследованиях современнейших цифровых технологий.

Вышеописанные проблемы функционирования цифровых технологий с использованием искусственного интеллекта и больших данных (Big Data) в судебно-экспертной деятельности в Российской Федерации могут быть решены реализацией мер по проверке научной обоснованности и пригодности внедряемых в практику новаторских методик и программно-компьютерных комплексов экспертного исследования, и, в случае положительных результатов испытаний, их внедрения в кратчайшие сроки на практике, с одновременным правовым их обеспечением.

Список литературы

1. Состояние преступности в России за январь-декабрь 2022 года. URL: https://xn--b1aew.xn--p1ai/reports/item/35396677

2. Майлис Н. П. Руководство по трасологической экспертизе. М.: Шит-М, 2007. 344 с.

3. Майлис Н. П. Судебная трасология: учебник. М.: Экзамен: Право и закон, 2003. 270 с.

4. Владимиров В. Ю. Теория криминалистического оружиеведения: монография / Санкт-Петербургский университет МВД России; Академия права, экономической безопасности жизнедеятельности; под общ. ред. В. П. Сальникова. СПб.: Фонд поддержки науки и образования в области правоохранительной деятельности «Университет», 2003. 399 с.

5. Ильин Н. Н. Криминалистическая идентификация человека по признакам внешнего облика, запечатленных на видеоизображениях: монография. М.: Юрлитинформ, 2015. 215 с.

6. Использование искусственного интеллекта при выявлении, раскрытии, расследовании преступлений и рассмотрении уголовных дел в суде: монография / под ред. С. В. Зуева, Д. В. Бахтеева. М.: Юрлитинформ, 2021. 216 с.

7. Россинская Е. Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Известия ТулГУ. Экономические и юридические науки. Вып. 3 ч. II. Юридические науки. 2016. С. 109–117.

8. Россинская Е. Р. Учение о цифровизации судебно-экспертной деятельности в системе частных теорий судебной экспертологии // Теория и практика судебной экспертизы в современных условиях: материалы VIII Международной научно-практической конференции. МГЮУ, 28–29 января 2021 г. С. 261–267.

9. Аминев Ф. Г. О необходимости принятия федерального закона «О всеобщей геномной регистрации в Российской Федерации» в целях улучшения качества раскрытия и расследования преступлений // Правовое государство: теория и практика. Уфа, 2019. № 3(57). С. 94–98.

10. Кокушев А. Б. Организационно-правовые аспекты функционирования современных информационных систем оперативно-криминалистических подразделений МВД Республики Казахстан: дис. ... канд. юрид. наук: 5.1.4. Волгоград, 2023. 209 с.

11. Баринова О. А. Использование информационных технологий при криминалистическом исследовании реквизитов документов // Дискуссионные вопросы теории и практики судебной экспертизы: материалы международной научно-практической конференции, посвященной памяти Т. В. Аверьяновой. РГУП, 25–26 марта 2021 г. М., РГУП, 2021. С. 93–96.

А. В. Антипов,
кандидат философских наук,
Институт философии Российской академии наук

ИСКУССТВЕННЫЕ МОРАЛЬНЫЕ АГЕНТЫ: АНАЛИЗ АРГУМЕНТОВ ПРОТИВ

Аннотация. Искусственные моральные агенты представляют собой роботов, которые способны выстраивать решения исходя из моральных рассуждений и регулятивов. Существуют разные способы классификации искусственных моральных агентов, в рамках данной статьи будет использована классификация, данная Дж. Муром. Человечество не может больше себя представить без искусственных систем, они становятся все совершеннее, что ставит вопрос об этичности их действий. При этом все ярче становятся голоса тех, кто видит угрозу в появлении искусственных моральных агентов. В статье рассматриваются некоторые аргументы против их создания, такие как: отсутствие универсальной этической теории, ответственность, потеря навыков, экзистенциальный аргумент.

Ключевые слова: искусственные моральные агенты, этика, мораль, регулирование, ответственность, интеллектуальные системы, роботы

ARTIFICIAL MORAL AGENTS: AN ANALYSIS OF THE ARGUMENT AGAINST THEM

Abstract. Artificial moral agents are robots that are able to make decisions based on moral reasoning and regulation. There are different ways of classifying artificial moral agents, in this article we will use the classification given by J. Moore. Mankind can no longer imagine itself without artificial systems, they are becoming more and more perfect, which raises the question of the ethicality of their actions. At the same time, the voices of those who see a threat in the emergence of artificial moral agents are becoming more and more vivid. The article discusses some of the arguments against

their creation, such as: the lack of a universal ethical theory, responsibility, loss of skills, and the existential argument.

Keywords: Artificial moral agents, ethics, morality, regulation, responsibility, intelligent systems, robots

Введение. Современность все больше наполняет окружающий нас мир искусственными системами (далее – ИС), которые призваны выполнять различные задачи: от регуляции температуры в помещении до социальных роботов, создаваемых для заботы о тех, кто позаботиться о себе не в состоянии. Все это приводит к необходимости вовлечения искусственных агентов в человеческий мир и сообщество. Для реализации этой цели мало только заданных алгоритмов, как недостаточно и только правового регулирования, поскольку оно выполняет только внешнюю задачу, в то время как нам необходимо ввести (встроить) определенный уровень ответственности и автономии для этих систем. Поэтому встает проблема создания искусственных моральных агентов (далее – ИМА), которые были бы способны выполнять те же задачи, что и люди, отвечать за принимаемые решения, быть способными их объяснять и решать встающие перед ними дилеммы.

Основная часть. Х. Сервантес, С. Лопез и соавторы указывают, что ключевым моментом является гармоничное сосуществование искусственных агентов с людьми и другими системами. То есть необходимо создать такую систему, которая могла бы если не стать равной человеку, то, по крайней мере, действовать в сложных ситуациях подобно людям. Однако это поднимает определенные проблемы. Как сделать так, чтобы искусственной системе была предоставлена автономия для принятия собственных решений, в том числе восприятие, принятие решений, планирование и обучение. Для решения этого вводится понятие регулируемой автономии: это такая автономия, при которой механизмы, реализуемые в ИС, позволяют людям вмешиваться в работу ИС, если последние не способны самостоятельно разрешить стоящие перед ними проблемы. В данном случае цель состоит в избегании неадекватного поведения ИС и сохранении глобально контроль над ИС. В области машинной этики это означает наделение ИС этическими механизмами, которые позволяют взаимодействовать с людьми и решать возникающие моральные дилеммы.

При этом глобальная цель: наделить искусственные агенты этическим поведением, сделать так, чтобы они могли стать полноценной частью человечества [4]. В случае регулируемой автономии остается также проблема злонамеренного использования [1].

Вопрос об автономии ИС и ИМА является чрезвычайно сложным. Он также состоит в том, что мы подразумеваем под определением ИМА. В отличие от указанного выше представления о регулируемой автономии, П. Формоза и М. Райан считают, что ИМА – это роботы, способные участвовать в автономном моральном рассуждении без непосредственного участия со стороны человека в реальном времени. Такая автономия приближается к человеческой как способности самостоятельно являться источником собственных решений и действий. ИМА направлены на выход за пределы рассуждений только о безопасности, которые превалируют

в дискурсе об ИС. Определить автономность робота можно как его способность следовать сложному алгоритму в ответ на поступающие данные извне, не зависимо от участия человека. Так, автономным не может считаться робот, не способный пройти определенный маршрут без помощи человека, а беспилотный автомобиль является примером робота, обладающего автономией. Поэтому ИМА наделяется следующими качествами: интерактивность (восприятие окружающей среды), автономность (способность выносить этические суждения), адаптивность (способность действовать на основании вынесенных этических суждений без участия со –стороны человека) [5].

В таком случае поднимается следующий вопрос: об устройстве такого искусственного агента. Аллен, Смит и Воллах предлагают устройство ИМА исходя из архитектуры построения:

– Сверху вниз: этическая теория является основанием для принятия решений;

– Снизу вверх: использование механизмов обучения для принятия решений, не навязывается какая-то модель принятия решений;

– Гибридная модель: сосуществование как восходящих, так и нисходящих механизмов. Цель состоит в том, чтобы сделать моральное поведение адаптивным [3].

Архитектура построения ИМА предполагает различные способы выведения моральных суждений в условиях, приближенных к человеческим. Следует рассмотреть также одну из самых известных классификаций ИМА, принадлежащей Дж. Муру. Он выделяет четыре типа ИМА:

1) агенты этического воздействия: они не являются моральными агентами в полном смысле, а представляют собой инструменты, которые в руках человека способны быть источником морально оцениваемых последствий.

2) Неявные этические агенты: не способны различать хорошее и плохое поведение. Но они могут действовать этично, поскольку заданный алгоритм поведения в определенных ситуациях выбирает только морально одобряемый поступок, либо же они избегают поведения, которое может быть названо порицаемым (например, причинение вреда). Компьютеры являются неявными этическими агентами в том случае, если конструкция машины позволяет решать проблемы безопасности и надежности (например, системы управления самолетом). Они обладают следующими характеристиками: не имеют механизмов, позволяющих отличить этичное действие от неэтичного; их функциональная пригодность протестирована и безопасность подтверждена; в них нет вредоносного кода. В данном случае возникает проблема доверия этим системам (насколько можно доверять тому, что банкомат отдаст деньги и вернет банковскую карту?).

3) Явные этические агенты: способные работать с этическими правилами и способны просчитывать лучшее действие, используя этические подходы. В них используется постепенное обучение через опыт.

4) Полные этические агенты: подобные человеческим существам, обладают «убеждениями, желаниями, намерениями, свободой воли и осознанием своих действий».

Считается, что только человек способен быть этичным. Их ключевые параметры: a) способность использовать более одного подхода для принятия решений и b) способность принимать решения на основании неполной информации [6].

Такая классификация позволяет разделить ИС по их способности принимать этически релевантные решения. Однако в данном случае остается проблема доступности ИМА феноменального опыта [2], т. е. вопрос в том, будет ли поведение действительно этичным или только симулякром морального поведения?

Для анализа аргументов против создания ИМА будет использоваться схема, предложенная П. Формозой и М. Райаном [5]. Кратко выделим и разберем некоторые из предлагаемых аргументов.

Первый аргумент состоит в не способности создать ИМА, а поэтому и не нужно пытаться сделать невозможное. Действительно, сильный искусственный интеллект в данный момент вызывает большие споры о своей достижимости. Тем более, создать моральный искусственный интеллект некоторым не представляется возможным. А потому попытка его создания выглядит как бесплодное приложение ресурсов и сил. С этим связан второй аргумент, согласно которому с точки зрения нескольких этических теорий (утилитаризма, этики добродетелей и деонтологии) рассматривается возможность создания ИМА. С точки зрения утилитаризма и его прагматической трактовки можно потратить деньги и лучше, поскольку перед человечеством и так стоит множество проблем, на которые стоило бы потратить ограниченные ресурсы. А с точки зрения этики добродетелей и деонтологии звучит более сильный аргумент, состоящий в том, что мы создаем рабов, которых попросту плодим в угоду себе. Создание роботов, выполняющих работу, которая для человека по каким-то причинам кажется неприемлемой или слишком тяжелой, само по себе представляет собой морально неоднозначную практику. Наделение их возможностью моральной рефлексии приводит скорее к негативным эффектам, выражаемым в использовании по своей сути рабского труда.

Несмотря на это противоположное мнение рассматривается в качестве третьего аргумента против создания ИМА. Предполагается, что ИМА должны оставаться в подчиненном состоянии (по сути, рабами). В таком случае наделение их моральной рефлексией и способностью поступать согласно этическим предписаниям ограничивает нашу возможность на их использование, поэтому они должны оставаться морально неполноценными. Это позволит их использовать в качестве средства для достижения наших целей. Этот аргумент звучит очень прагматично и во многом может противоречить моральному чувству, поскольку, например социальные роботы, призваны вызывать эмпатию у использующих их людей, что исключает возможность использования ИМА только в качестве средства.

Следующий аргумент выстраивается на отсутствии универсального согласия в этике. До тех пор, пока не существует установленного согласия в этике, создание ИМА выглядит слишком претенциозной задачей. Разные этические теории – деонтология, утилитаризм, этика добродетелей, коммунитаризм и др. – конкурируют друг с другом, по-разному отвечают на этические вопросы, дилеммы и затруднения, что делает невозможным условия, при которых возможно научить искусственного агента какой-то из них и ожидать, что он будет поступать морально. Человек обычно использует различные стратегии рассуждения в сложных ситуациях морального выбора, поэтому создания полного ИМА встречает дополнительную сложность.

Пятый аргумент выстраивается на необходимости сосредоточиться на создании безопасных машина, а не моральных. Действительно, создание безопасных и надежных искусственных агентов выглядит первоочередной задачей. Следует сосредоточить свое внимание на возможности использования машин и роботов в динамичной среде реальности так, чтобы можно было на них положиться. Не каждая деятельность требует моральных рассуждений, но любая должна основываться на принципах безопасности, надежности и способности положиться.

Шестое опасение связано с экзистенциальными переживаниями о выживаемости нас как вида. Научная фантастика и популярная культура рисуют образы мрачного будущего, в котором машины восстают и уничтожают или порабощают своих создателей. Это порождает определенные алармистские настроения в обществе и общую настороженность по поводу создания сильного искусственного интеллекта и технологической сингулярности. Однако можно отметить, что создание именно ИМА способно решить это затруднение, поскольку обучение морали способно оказывать дополнительное сдерживающее влияние на роботов.

Гораздо более приближенным к реальности выглядит седьмой аргумент: перекладывание работы на другого приводит к потере навыка. Поэтому создание и использование моральных машин приведет к тому, что человек потеряет свою способность полноценно быть моральным существом. Мораль выступает в качестве одного из существенных характеристик человека, поэтому наделение ее искусственного агента способно приводить к потере человечеством собственной моральности. Аргументация выстраивается по аналогии с уже существующими проблемами: распространение навигаторов приводит к сильному ухудшению знания людей городов, а также люди слишком сильно полагаются на электронные системы. Во время сбоя систем навигации в Москве многие водители попросту не знали, куда ехать: их способность ориентации серьезно пострадала вследствие чрезмерного использования искусственных помощников.

Следующий аргумент касается социальных роботов: осуществляющие заботу машины могут использоваться не только для ухода за стариками и больными людьми, но и участвовать в воспитании детей. Но в таком случае мы получаем проблему, связанную с тем, что робот изменяет сообщество людей через воспитание новых людей. А также это чревато тем, что дети могут нездорово привязываться к роботам. Такая привязанность связана с эмпатией, испытываемой человеком даже к искусственным агентам. Однако в условиях демографических кризисов и старения населения индустрия социальных роботов, как можно предположить, будет только развиваться и расти, и отказаться от их использования трудно.

Последний аргумент касается проблемы ответственности: a) неправильное перекладывание ответственности на робота; b) невозможность обвинить робота. Уже сейчас инциденты с беспилотными автомобилями порождают коллизии, для которых не существует разделяемого большинством решения. Аргумент показывает противоречивую природу ИМА: с одной стороны, встает проблема обвинения и наказания робота, поскольку он не является в прямом смысле живым и не обладает социальностью, традиционные концепты наказания для него не имеют значения. Необходимо разработать абсолютно новый способ наказания, который

бы соответствовал иной природе ИМА. С другой стороны, возможны случаи, при которых на робота будет накладываться ответственность, которой не соответствовали его действия, с целью избежать наказания.

Заключение. Создание ИМА выглядит привлекательной и перспективной областью исследований и инженерии. Однако оно несет с собой множество проблем, убедительных ответов на которые пока не предлагается. При этом это не значит, что не следует их создавать. Прогресс и процесс разработки не остановим, поэтому необходимо убедиться в их безопасности и возможности инкорпорации в человеческий мир.

Список литературы

1. Клюева Н. Ю. Этическая экспертиза технологий искусственного интеллекта и робототехники // Философская аналитика цифровой эпохи: сб. науч. статей / отв. ред. Л. В. Шиповалова, С. И. Дудник. СПб: Изд-во С.-Петерб. ун-та, 2020. С. 164–174.

2. Разин А. В. Этика искусственного интеллекта // Философия и общество. 2019. № 1(90). С. 57–73.

3. Allen C., Smit I., Wallach W. Artificial morality: Top-down, bottom-up, and hybrid approaches // Ethics and Information Technology. 7(3). 2005. Pp. 149–155.

4. Cervantes J., López S. et al. Artificial Moral Agents: A Survey of the Current Status // Science and Engineering Ethics. 26. 2020. Pp. 501–532.

5. Formosa P., Ryan M. Making moral machines: why we need artificial moral agents // AI & SOCIETY. 36. 2021. Pp. 839–851.

6. Moor J. The nature, importance, and difficulty of machine ethics // IEEE Intell Syst. 21(4). 2006. Pp. 18–21.

О. Г. Басалаева,
кандидат философских наук, доцент,
Кемеровский государственный медицинский университет
Ю. М. Басалаев,
доктор физико-математических наук, профессор,
Кемеровский государственный медицинский университет

ПРАВОВЫЕ ВОПРОСЫ И ПРОБЛЕМЫ ЗАЩИТЫ ДАННЫХ В ИНТЕЛЛЕКТУАЛЬНЫХ УСТРОЙСТВАХ IOMT

Аннотация. В работе определена роль интеллектуальных устройств на основе IoMT в улучшении системы здравоохранения, а также дано краткое представление о технологиях, дополняющих IoMT, и проблемах, возникающих при разработке интеллектуальной системы здравоохранения. Учитывая огромные потребности, здравоохранение рассматривается как наиболее сложная область для приложения Интернета медицинских вещей (IoMT), с учетом обеспечения безопасности устройств IoMT и данных, которые они собирают и передают.

Ключевые слова: цифровые технологии, промышленный интернет вещей, интернет медицинских вещей, защита данных, кибербезопасность, право, здравоохранение

LEGAL ISSUES AND PROBLEMS OF DATA PROTECTION IN SMART DEVICES IOMT

Abstract. The paper defines the role of intelligent devices based on IoMT in improving the health care system, and also gives a brief idea of the technologies that complement IoMT and the problems that arise in the development of an intelligent health care system. Given the huge needs, healthcare is seen as the most challenging area for the Internet of Medical Things (IoMT) application, taking into account the security of IoMT devices and the data they collect and transmit.

Keywords: digital technologies, IoT, IoMT, data protection, cybersecurity, law, healthcare

Введение. Новая технологическая революция, определяемая шестым технологическим укладом, приводят к слиянию технологий и размыванию границ между физической и цифровой средой, тем самым переопределяя основополагающие основы цифрового общества и цифровой экономики [3. С. 65].

К современным нововведениям связанным, прежде всего, с цифровой экономикой относятся «сквозные цифровые технологии»: большие данные, блокчейн (системы распределенного реестра), новые производственные технологии, нейротехнологии и искусственный интеллект, робототехника и сенсорика, беспроводная связь 5G, виртуальная и дополненная реальности, квантовые технологии, промышленный интернет вещей (IoT) [4. С. 47].

Основная часть. Интернет вещей (IoT) буквально означает взаимосвязанную сеть физических объектов или «вещей», интегрированных для обмена данными между устройствами / системами с использованием Интернета. IoT относится к сети устройств, которые автономно взаимодействуют по этой сети.

Устройства медицинских вещей (IoMT) – это тип цифровых технологии IoT.

Интеллектуальные устройства на основе IoMT повсеместно стремительными темпами оказывают влияние на современную систему здравоохранения. Внезапный всплеск коронавирусной инфекции (COVID-19) привел здравоохранение во всем мире в состояние неопределенности и повышенной готовности [1. С. 62]. Интернет медицинских вещей (IoMT) в значительной степени облегчил ситуацию, а COVID-19 побудил ученых создать инновационную «умную» систему здравоохранения, призванную, с одной стороны, проводить раннюю диагностику, с другой – облегчить жизнь в новых условиях.

Большинство систем IoMT работают на следующих основных уровнях, которые интегрируют различные технологии, устройства, датчики и системы, соединенные между собой посредством проводного или беспроводного соединения [6. С. 29]. Данные о пациентах собираются и передаются поставщикам медицинских услуг через сети IoMT с указаниями пациента или медицинского работника, или без них.

С момента первого упоминания интернета вещей Эштоном в 1999 году наблюдался экспоненциальный рост производства этих устройств, что привело к примерно 10 миллиардам подключенных IoT-устройств в настоящее время (с прогнозируемым увеличением примерно до 25 миллиардов до 2025 года) [5. С. 305].

В современных условиях IoMT сталкивается с определенными уникальными правовыми, техническими проблемами и проблемами конфиденциальности, главным образом по причине взаимодействия многих заинтересованных сторон, в том числе – это: (1) поставщики медицинского оборудования; (2) поставщики услуг подключения сети; (3) производители оригинального оборудования; (4) разработчики и поставщики программного обеспечения; (5) системные интеграторы; (6) пользователи.

Суть юридических проблем, связанных с использованием IoMT заключается в решении вопроса права собственности на данные. Не всегда ясно, кому принадлежат данные IoMT, когда они генерируются. Пациент, поставщик программного обеспечения и другие поставщики медицинских услуг могут генерировать данные или прикасаться к ним в течение всего их жизненного цикла. В зависимости от контекста права на данные для каждой стороны могут быть неоднозначными. Например, если медицинское устройство, принадлежащее государственному городскому лечебно-профилактическому учреждению, собирает данные от пациента, сохраняет данные в стороннем облачном приложении и передает данные частной организации здравоохранения...

Существует множество способов, которыми разные стороны могут использовать данные и обмениваться ими. Владелец может иметь право уничтожить данные, что может быть сложно в распределенной сети, где данные потенциально реплицируются много раз.

Кроме того, из-за конфиденциальности медицинских данных существуют проблемы регулирования того, как и где они могут использоваться, а также спецификации о том, как технология должна быть защищена. Например, FDA выпустило всеобъемлющее руководство по управлению кибербезопасностью в медицинских устройствах. Европейский Союз, Соединенное Королевство и такие организации, как Ассоциация по развитию медицинского инструментария и Европейская комиссия, выпустили дополнительные рекомендации и правила в отношении этих устройств.

Защищенная медицинская информация сталкивается с большим количеством рисков безопасности. Передаваемые медицинские данные подвергаются различным угрозам кибербезопасности, включая утечки данных и мошенничество. Злоумышленники могут использовать украденные учетные данные для получения медицинских услуг или лекарств [1].

Важно понимать, что данные, поступающие с устройств IoMT обычно проходят через общедоступный Интернет и подвержены большему количеству угроз безопасности, чем в частной сети с брандмауэром. «Эта угроза усугубляется тем фактом, что данные совместно используются многими системами, обеспечивая несколько векторов атаки» [2. С. 84].

OEM-производители должны использовать лучшие отраслевые практики в области безопасности, а администраторы должны применять новейшие протоколы шифрования, используя уникальные и сложные пароли для доступа и проверки SSL-сертификатов удаленных систем.

Заключение. В системе безопасности устройства IoMT задействовано множество переменных, и нет единственного и простого способа защитить все медицинские устройства от всех типов угроз.

Тем не менее первым шагом является обеспечение информации о том, какие медицинские устройства существуют в сети, и типы угроз, которые могут на них повлиять.

Рекомендуется модель сетевой безопасности с нулевым доверием, в которой связь между устройствами контролируется строгим контролем доступа и аутентификацией, чтобы гарантировать, что трафик поступает оттуда, где, он находится. Ordr Systems Control Engine (SCE) может обеспечить видимость и безопасность всех подключенных медицинских устройств.

Список литературы

1. Басалаева О. Г. Культурный контент on-line в условиях пандемии / О. Г. Басалаева, Ю. М. Басалаев, М. В. Галич // Информационное общество. 2022. № 3. С. 61–70.

2. Басалаева О. Г. Социально-философские аспекты взаимосвязи информационной и культурной картин мира: специальность 09.00.11 «Социальная философия»: дис. … канд. филос. наук. Кемерово, 2012. 199 с.

3. Басалаева О. Г., Лукина Н. П. Технологический уклад информационного общества в контексте концепции конвергенции наук и технологий // Научные ведомости Белгородского государственного университета. Серия: Философия. Социология. Право. 2017. № 10(259). С. 62–67.

4. Генезис новой парадигмы социально-экономического развития России: экономические, социальные, правовые, общенаучные тенденции и закономерности / М. С. Арзуманян, Ю. М. Басалаев, О. Г. Басалаева [и др.]. Самара: ООО НИЦ «ПНК», 2022. 232 с.

5. Dwivedi R., Mehrotra D., Chandra S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. J Oral Biol Craniofac Res. 2022 Mar-Apr;12(2):302-318. doi: 10.1016/j.jobcr.2021.11.010

6. Lin Y. Novel smart home system architecture facilitated with distributed and embedded flexible edge analytics in demand-side management. Int Trans Electr. Energy Syst. 2019. № 29.

И. Р. Бегишев,
доктор юридических наук, доцент,
Казанский инновационный университет имени В. Г. Тимирясова
Д. Д. Берсей,
кандидат юридических наук, доцент,
Северо-Кавказский федеральный университет

ГЕНЕЗИС КРИМИНАЛЬНОЙ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Аннотация. В статье рассмотрены основные определения, а также этапы развития понятия «социальная инженерия». Определено, что на разных исторических этапах сущность данного понятия претерпевала изменение под влиянием тех или иных факторов, соответственно, объем понятия постепенно изменялся и расширялся. Установлено, что социальная инженерия заключена в применении различных технологий, позволяющих злоумышленнику организовать незаконное вторжение в информационную систему и завладеть необходимой цифровой информацией. Утверждается, что социоинженерные атаки стали настолько сложными, что могут сравниться по степени внедрения с техническими типами атак.

Ключевые слова: социальная инженерия, злоумышленник, социоинженерная атака, фишинг, киберпреступление, уголовное право, кибератака

THE GENESIS OF CRIMINAL SOCIAL ENGINEERING

Abstract. The article discusses the main definitions, as well as the stages of development of the concept of “social engineering”. It is determined that at different historical stages the essence of this concept underwent a change under the influence of various factors, respectively, the scope of the concept gradually changed and expanded. It is established that social engineering consists in the use of various technologies that allow an attacker to organize an illegal intrusion into an information system and seize the necessary digital information. It is argued that socioengineering attacks have become so complex that they can be compared in terms of the degree of implementation with technical types of attacks.

Keywords: social engineering, attacker, socioengineering attack, phishing, cybercrime, criminal law, cyberattack

Введение. На современном этапе ключевым фактором обеспечения работы любой компании выступает информационная безопасность. Информационная безопасность – это защита информации от широкого спектра угроз в целях обеспечения устойчивости и работоспособности бизнеса, минимизации бизнес-рисков и максимизации прибыли [1]. В этой связи руководству компаний необходимо регулярно инвестировать в технологии информационной безопасности, так как злоумышленники постоянно анализируют возможности организации информационной защиты крупных и средних организаций с целью получить несанкционированный доступ к тому или иному массиву информационных данных.

Однако необходимо учитывать, что не только посредством организации эффективной системы информационной защиты можно обезопасить конфиденциальные данные. Достаточно важно обеспечить такую защиту и с учетом человеческого фактора, который считается самым слабым звеном в информационной системе и в системе безопасности [2].

Одной из основных угроз информационной безопасности организации является рост числа инцидентов, связанных с применениями социоинженерных технологий – криминальной социальной инженерии.

Социальная инженерия заключена в применении различных социальных технологий, позволяющих социальному инженеру организовать незаконное вторжение в информационный массив жертвы [3]. Данная технология позволяет избежать технических манипуляций, связанных со взломом системы безопасности.

Основная часть. Уже к концу 2007 года методы социальной инженерии широко использовались инсайдерами для совершения электронных преступлений, при этом пользователи, выступившие «проводниками» к данным, не до конца осознали свою роль в этом процессе.

Согласно Оксфордскому словарю английского языка, термин «социальная инженерия» имеет два различных значения [4]. Во-первых, это «использование централизованного планирования в попытке управлять социальными изменениями и регулировать будущее развитие и поведение общества». Во-вторых, это «использование обмана для того, чтобы побудить человека разгласить частную или другую информацию и невольно обеспечить несанкционированный доступ к компьютерной системе или сети».

В обоих определениях имеет место индивид, который индуцирует поведение со стороны других, однако, если первое определение чаще может использоваться в области политического и экономического управления, то второе используется исключительно в сфере киберпространства.

Следующие определения социальной инженерии иллюстрируют, что не существует единого, широко принятого определения. В частности, данное понятие в разных источниках определяется следующим образом:

– «социально-психологический процесс, с помощью которого индивид может получить информацию от человека о целях организации» [5];

– «вид нападения на человеческий элемент, в ходе которого нападающий психологически склоняет потерпевшего разглашать информацию» [6];

– «использование социальных маскировок, культурных уловок и психологических трюков, чтобы заставить пользователей компьютеров помогать хакерам в их незаконном вторжении или использовании компьютерных систем и сетей» [7];

– «искусство получения доступа к защищенным объектам путем использования человеческой психологии без взлома информационной системы» [8];

– «атака, в которой злоумышленник использует человеческое взаимодействие для получения информации об организации или ее компьютерной системе» [9];

– «процесс, в котором злоумышленник пытается получить информацию о сети и компьютерной системе с помощью социальных средств» [10];

– «метод обмана, используемый хакерами для получения информации или данных о компании» [11];

– «нетехнический вид вторжения, который в значительной степени зависит от человеческого взаимодействия и часто связан с обманом других людей, цель которого – нарушить обычные процедуры безопасности» [12];

– «хакерская манипуляция человеческой склонностью доверять другим людям для получения информации, которая позволит осуществлять несанкционированный доступ к системам» [13];

– «наука искусного маневрирования людьми для получения личной информации» [14];

– «под социальной инженерией в контексте информационной безопасности имеется в виду искусство манипулирования людьми с целью совершения действий, связанные с получением или разглашением конфиденциальной информации» [15];

– «акт манипулирования человеком или людьми с целью совершения какого-либо действия с информацией» [16].

Также социальная инженерия была определена как «наука об использовании социальных взаимодействий, цель которых – убедить индивида выполнить конкретное задание злоумышленника, при этом, диалог осуществляется посредством социальных сетей» [17]. Есть мнение, что социальная инженерия – это техника, которая используется для взаимодействия с людьми с целью получения информации для достижения той или иной цели. На практике социальная инженерия может быть мощным инструментом в руках человека, который знает, как использовать ее методы наиболее эффективно [18]. Социальная инженерия бросает вызов безопасности всем людям сети, независимо от надежности их брандмауэров, методов криптографии, способов обнаружения вторжений в систему и антивирусных программных комплексов [19].

Впервые термин «социальный инженер» появился в книге 1842 г. под названием «эффективный инженер». Британским экономистом Дж. Греем было написано «лекарство от бедственного положения народов».

В 1891 г. норвежско-американский экономист Т. Веблен опубликовал эссе под названием «Некоторые забытые моменты в теории социализма», где он предпринял попытку найти ответ на вопрос, является ли современная экономика перспективной, и можно ли ее перестроить в соответствии с идеями экономистов-социалистов.

Т. Веблен отметил, что эта возможность является практическим вопросом «конструктивного характера», некоей «социальной инженерией», а не изначально логическим или теоретическим соображением, и по этой причине выразил свой глубокий скептицизм по поводу его успеха [20]. Самому термину «социальная инженерия» Т. Веблен не посчитал нужным дать определение. Тем не менее из контекстного употребления термина Т. Вебленом следует, что в основе социальной инженерии лежат социальные манипуляции.

Дж. Аддамс, американский социальный работник, активист, общественный деятель и реформатор, применил термин «социальная инженерия» в 1914 г. к попыткам европейских правительств принять политику социального страхования и бирж труда в рамках борьбы с безработицей [21].

Подобно Т. Веблену, Дж. Аддамс подчеркивала взаимосвязь между знанием и эффективностью политики, отмечая, что с женщинами следует консультироваться, прежде чем приступать к публичным выступлениям. Она приводит пример, иллюстрирующий прения в британском парламенте, в котором принимают участие исключительно представители мужского пола по поводу того, следует ли сделать незаконным производство детской пижамы из якобы легковоспламеняющегося материала, тогда как любая женщин того времени, как сардонически замечает Дж. Аддамс, могла бы сказать участникам прений, что таких пижам не существует [22].

К 1929 г. эта концепция привлекла внимание юристов [23], в то время как Великая Депрессия и эпоха нового курса обеспечили ее динамичное развитие среди научного сообщества в целом. Например, в 1937 г. Дж. Дэвис высказал мнение, что «социальную инженерию» необходимо считать новой академической дисциплиной на том основании, что прикладные социологи смогут «обуздать социальные приливы и отливы», используя растущий объем статистических данных и применяя передовые технологии в сочетании с социальными научными методами [24]. Дж. Дэвис писал: «Я вижу признаки необходимости применения результатов исследований социальных инженеров, которые не только планируют и исполняют, но разрабатывают конструктивные планы для успешного исполнения, а также социальных врачей, которые будут не только выписывать и лечить, но и реально лечить социальные болезни» [25]. Как и врачи, утверждал Дж. Дэвис, эти социальные инженеры обладают специализированными знаниями, необходимыми для манипулирования обществом различными способами.

Также в рассматриваемый период этнографы использовали этот термин для описания властных отношений между завоевателем и покоренными племенами в Африке. Например, в 1938 г. британский антрополог М. Рид использовала термин «социальная инженерия» для описания того, как завоеватели Нгони из Ньясаленда (ныне Малави) подчинили себе, а затем принудили их к исполнению своих обязанностей. М. Рид отметила, что эта социальная инженерия включает в себя значительное количество манипуляций в области государственного строительства, планирования и модификации социальных институтов, которая находилась под эгидой Нгони.

До начала 1940 гг. концепция социальной инженерии уже эксплицитно содержала две фундаментальные идеи, сохраняемые в ней и по сей день. Первая из них – это эпистемическая асимметрия, которая происходит от греческого слова эпистема (ἐπιστήμη) – «знание». Эпистемическая асимметрия возникает, когда один человек или группа наслаждается значительным преимуществом знаний над другим человеком или группой в пределах определенной области. Дж. Грей, Т. Веблен, Дж. Аддамс подчеркивали, что специализированные знания необходимы для успешной социальной инженерии в области экономики и планирования. Однако они по-разному оценивали успех применения таких знаний, но это было вызвано не несовместимыми представлениями о том, что требуется для социальной инженерии, а тем, что необходимо для ее осуществления.

Второй стала идея технократического доминирования, которая тесно связана с вышеупомянутой асимметрией. Технократ обычно обладает техническими

знаниями или навыками в той или иной области, например, в экономическом планировании или стоматологии. Технократическое доминирование возникает, когда лицо или группа, обладающие высокой степенью технических знаний, используют эти знания для осуществления изменения в поведении других людей, когда такое поведение ставит затронутых в положение снижение власти или авторитета по отношению к первому в пределах затронутой области.

Дж. Дэвис высказывал мнение о том, что технократы как в государственном, так и в частном секторах могут вылечить болезни общества с помощью реализация политики в отношении ничего не подозревающих (но, надеюсь, благодарных) граждан.

После успеха Манхэттенского проекта (1942–1946 гг.) динамичное развитие получили различные разработки в области кибернетики, которое связывалось с управлением процессами в живом организме или в машине. Это движение принесло с собой растущий оптимизм в успехе, связанном с развитием политики социальной инженерии и основанном на представлении о человечестве, которое было специально создано для амбициозных форм социального планирования.

Человеческий разум понимался как машина Тьюринга, с двумя «роботизированными механизмами обратной связи», что позволяло выполнить теоретико-игровой анализ человеческого поведения. В этом контексте социальная инженерия является просто технологией разработки правил игры, чтобы вызвать к жизни желаемую человеческую реакцию. Указанный оптимизм распространялся далеко за пределы планирования государственной политики [26].

В 1954 году социальная инженерия получила развитие в связи с выходом работы Рона Хаббарда «Введение в Саентологию». В данном труде рассматриваемое понятие получило уже прикладное значение, однако его основные элементы остались неизменными. Это произошло в рамках внедрения субкультуры «телефонного фрикинга», которую многие специалисты считают началом современной хакерской культуры. Телефонные фрикеры использовали свои растущие технические знания о возможностях управления сетями телефонной системы (схемах, переключателях, реле, тональных сложностях и пр.). Знание возможностей управления телефонными сетями давало фрикерам возможность захватить телефонную систему и использовать ее в своих собственных целях. При этом они могли подключиться к иностранным конференц-звонкам или получить доступ к рассматриваемым областям сети, где запрещено использование обычных телефонных протоколов.

Так, один из родоначальников телефонного фрикинга, Дж. Дрейпер отмечал, что часто он и его друг, и коллега, Деннис Дэн, использовали методы социальной инженерии, чтобы получить необходимую информацию от ничего не подозревающих сотрудников Bell Telephone.

Дрейпер описал социальную инженерию как «способность входить и разговаривать с людьми внутри телефонной компании ... они верят, что вы работали на телефонную компанию».

Телефонные фрикеры изменили понятие социальной инженерии, однако основные элементы понятия они не изменили. Перед телефонным фрикингом термин

«социальная инженерия» применялась только к деятельности влиятельных политических планировщиков, которые выступали за применение социальной инженерии для лечения социальных болезней.

В 1960-е и 1970-е гг. имело место бурное технологическое развитие вычислительной техники и технология. Интерактивные вычисления, совместное использование времени, аутентификация пользователя, общий доступ к файлам через иерархический файл, структуры и прототипы компьютерных утилит – все это было частью волны технических инноваций в мире.

Наряду с этой волной появились относительно простые инструменты безопасности, такие как контроль доступа и пароли. Следующее десятилетие ознаменовалось появлением локальных вычислительных сетей (LANs), пакетные сети (ARPANET) и объектно-ориентированного проектирования, криптографических приложений, такие как криптография с открытым ключом, криптографии и криптографического хэширования. Это повысило осознание безопасности как необходимой характеристики информационных систем, что привело к применению математических моделей безопасности и первым демонстрациям доказуемо безопасных систем [27].

По мере того, как эти технические меры безопасности становились все более изощренными, хакеры, которые были естественным порождением сообщества телефонных фрикеров, стали больше использовать нетехнические манипуляции.

В 1984 г. термин «социальная инженерия» появился в анонимной статье в начале XX в. Статья была названа «Жизненно важные ингредиенты: коммутационные центры и операторы», в ней присутствовало описание социальной инженерии как технологии, способной посредством убеждений заставить кого-то раскрыть ту или иную информацию. Однако автор негативно отзывался о таких возможностях социальной инженерии и называл это явление абсурдом.

В конце 80-х-начале 90-х гг. XX в. оптимизм по поводу успеха социального планирования пошел на убыль, концепция же применения социальной инженерии стала пользоваться популярностью в обществе. В этот период исследователи проявляли высокий интерес к категории «социальная инженерия» и описывают попытки применить в рамках этого понятия разнообразные техники манипулирования [28].

Рост количества атак в рамках социальной инженерии породил плодотворные научные исследования и позволил обобщить основные принципы социальной инженерии на основе поведения и восприимчивости из его участников [29]. Такая работа была основана на методах экспериментальной психологии для выявления факторов, повышающих вероятность социального успех инженера против жертвы. Например, классические принципы Р. Чалдини – взаимность, приверженность и последовательность, социальное доказательство, симпатия, авторитет и дефицит – действуют как независимые переменные, которые индивидуально или через их взаимодействие объясняют склонность индивида позволить эксплуатировать себя человеком-манипулятором. Особенно уязвимыми в данной связи являются доверчивые личности, позиционирующие манипулятора как как авторитет и готовые ему подчиниться. Такие психологические объяснения были разумны, когда

парадигмой была социальная инженерия от человека к человеку. Однако с развитием искусственного интеллекта получает развитие автоматизированная социальная инженерия, и попытки объяснить аспекты социальной инженерии только возможностью успешного контакта человека с человеком утратят актуальность. В частности, применение ботов, которые активно изменяют среду социальных сетей без участия человека-злоумышленника, – это одно их новых направлений развития социальной инженерии [30].

В 2000-е гг. XX в. возникло мнение, что социальная инженерия может позиционироваться как тактика, которая разыгрывается по-разному в зависимости от конкретной формы, принимаемой атакой. Это позволяет отграничить такие атаки между собой.

В частности, олицетворение может быть использовано в попытке собрать аутентификационную информацию (например, имена пользователей и пароли) для получения доступа к целевой сети [31]. Так, используя приложение смартфона, злоумышленник может связаться с жертвой, которая идентифицирует его с сотрудником IT-отдела, проводящего опрос сотрудников из-за недавнего взлома имени пользователя и пароля, над которым работает компания. Пользуясь доверием жертвы, социальный инженер получает доступ к ее идентификационным данным.

Авторизация третьей стороны происходит, когда аутентификационные данные украдены или переданы пользователю [32]. Однажды эта сторона может ложно аутентифицировать себя в сети, и пока не приняты меры по ее удалению, хакеры могут использовать дополнительную социальную инженерию или другие средства и методы для повышения внутри системы своих привилегий пользователя. Конечная цель – это получение прав администратора в сети, что позволяет преступнику получить полный доступ к любым ценным данным, хранящимся в ней.

Фишинговые электронные письма направлены на обман получателя, их цель – заставить его выполнить какое-то действие, обычно нажав на ссылку или загрузив вложение, маскируясь под законные запросы на получение информация, предупреждение безопасности или обычные электронные письма от друзей или коллег [33]. Фишинговые атаки могут иметь серьезные последствия для их жертв, такие, как потеря интеллектуальной собственности и конфиденциальной информации о клиентах, финансовые потери и угрозы национальной безопасности [34].

Фишинговые атаки несут в себе серьезную опасность, так как основаны на психологической уязвимости атакуемого лица и учитывают все его слабости [35]. Это одна из самых сложных тактик социальной инженерии, так как изощренные злоумышленники часто могут создавать электронные письма, которые выглядят почти идентичными законным.

Угрозы, которые несет с собой социальная инженерия, становятся все более реальными. Транснациональные корпорации все чаще становятся жертвами целенаправленных атак на их информационные системы.

Другие типы атак социальной инженерии включают:

– тактику, использующую всплывающие окна;

– сбор информации с помощью погружения в мусорные контейнеры;

– плечо серфинга, позволяющее контролировать чьи-то учетные данные или другую конфиденциальную информацию;

– личные атаки, такие как олицетворение на месте или просто использование чьего-то свободного компьютерного терминала;

– атаки, использующие преимущества социальных сетей и другой общедоступной информации;

– атаки, которые подчеркивают или нацеливают жертвы, признанные нетехнически подкованными или вообще лишенными технической осведомленности;

– различные нефишинговые технические атаки, которые не связаны с взаимодействие человека с человеком, включая автоматизированные методы [36].

Несмотря на это многообразие, данный список остается открытым.

Социальная инженерия требует, чтобы жертва находилась в асимметричном отношении к окружающему миру. Злоумышленник, который использует эту асимметрию для установления технократического контроля над своей жертвой, как правило, пользуется одним или несколькими методами, описанными выше. Наконец, сохраняя этот контроль, нападающий заменяет поведенческие цели жертвы своими собственными.

Соответственно, можно заключить, что социальная инженерия включает две составляющие:

1. Компьютерный или технологический обман: технологический подход заключается в том, чтобы обмануть пользователя, полагая, что он взаимодействует с реальным компьютером система и заставить его предоставить конфиденциальную информацию.

2. Человеческий обман: это делается путем обмана, используя невежество жертвы и естественную человеческую склонность быть полезным и понравилось [37].

Социальная инженерия – это использование ментальных манипуляций для обмана компьютера в результате которой пользователи получают доступ к компьютерам, определенной информации или базе данных. Это может быть наиболее опасным по следующим причинам:

– социальная инженерия является одной из самых успешных по сравнению с другими техническими;

– специалисты по информационной безопасности, а также пользователи компьютеров мало что знают о риске применения технологий социальной инженерии;

– человеческие привычки и природа: люди склонны следовать определенным привычкам и действиям по умолчанию, не думая. Хороший нападающий может наблюдать эти привычки и использовать их для отслеживания людей или групп [38].

Рассмотрим основные стадии социальной инженерии.

Большинство хакеров используют определенные шаги, чтобы начать свою атаку и безопасно приблизиться к цели без каких-либо подозрений:

1. Сбор информации для социальной инженерии.

За последнее десятилетие некоторые из самых больших угроз безопасности исходили от использование социальных сетей. Стремительный рост этих технологий позволяет миллионам людей пользователи каждый день публикуют свои посты в социальных сетях. Такого типа информация, которую они публикуют, может

выглядеть не очень важной, но это очень важно для запуска успешной атаки, например, таким ключом может стать персональная информация, фотографии, информация о местоположении, информация о друзьях, деловая информация и пр.

Опасность предоставления такого объема информации заключается в том, что любопытный злоумышленник может собрать воедино эти источники и получить четкую картину личности или бизнес. После того, как сообщение опубликовано, его практически невозможно полностью удалить из социальной сети. Тем более, что оно уже могло быть переслан другим и перепечатано снова. Имея эту информацию в руках, злоумышленник может использовать социальную инженерию, чтобы создать фейк изучаемого лица или получить прибыль в бизнесе с помощью инсайдерской информации;

2. Развитие отношений и доверие с жертвой.

Развитие доверия может быть достигнуто с помощью использования инсайдерской информации. Человеческая природа основывается на доверии к другим, пока они не докажут, что им нельзя доверять. Если кто-то говорит нам, что он является определенным человеком, обычно это воспринимается как утверждение;

3. Эксплуатация отношений.

На этом этапе злоумышленник использует манипуляцию. Нападающий должен изучить эмоциональное состояние своей жертвы и определить, как ее можно использовать его в своих интересах. Эксплуатация может происходить путем разглашения кажущейся неважной информации или доступа, предоставленного / переданного злоумышленнику.

Заключение. Таким образом, социоинженерные атаки стали настолько сложными, что могут сравниться по степени внедрения с техническими типами атак. Кроме того, в атаке социальной инженерии люди – самое слабое место, однако при соответствующей подготовке они могут эффективно противостоять социальным инженерам.

Список литературы

1. Akila L., and Deviselvam. Intrusion Response System for Relational Database to Avoid Anomalous Request // I-manager's Journal on Software Engineering. 2022. Vol. 6(2). Pp. 41–45.

2. Majd Latah Detection of malicious social bots: A survey and a refined taxonomy // Expert Systems with Applications. 2021. Vol. 1511. Art. 113383.

3. Carver, Jeffrey C., Leandro L. Minku, and Birgit Penzenstadler. 2022. OED Online. March 2017. Oxford University Press.

4. Joseph M. Hatfield The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages // Computers & Security. 2022. Vol. 83. Pp. 354–366.

5. Francois Mouton, Mercia M. Malan, Kai K. Kimppa, H. S. Venter Necessity for ethics in social engineering research // Computers & Security. 2022. Vol. 55. Pp. 114–127.

6. Waldo Rocha Flores, Mathias Ekstedt Shaping intention to resist social engineering through transformational leadership, information security culture and awareness // Computers & Security. 2021. Vol. 59. Pp. 26–44.

7. Francois Mouton, Mercia M. Malan, Kai K. Kimppa, H. S. Venter Necessity for ethics in social engineering research // Computers & Security. 2022. Vol. 55. Pp. 114–127.

8. Mouton, F.a b, Leenen, L.a, Venter, H.S.b Social engineering attack examples, templates and scenarios // Computers and Security. 2021. Vol. 59. Pp. 186–209.

9. Kvedar, D., Nettis, M., Fulton, S. P.: The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition // Journal of Computing Sciences in Colleges. 2020. Vol. 26(2). Pp. 80–87.

10. McDowell, M.: Cyber security tip st04-0141, avoiding social engineering and phishing attacks. Technical report, United States Computer Emergency Readiness Team, 2013.

11. Cruz, J.A.A.: Social engineering and awareness training. Technical report, Walsh College, 2020.

12. Mills, D.: Analysis of a social engineering threat to information security exacerbated by vulnerabilities exposed through the inherent nature of social networking websites. In: Information Security Curriculum Development Conference/ Pp. 139–141.

13. Doctor, Q., Dulaney, E., Skandier, T.: CompTIA A+ Complete Study Guide. Wiley Publishing, Indianappolis, 2023.

14. Hamill, J., Deckro, R. F., Kloeber Jr., J.M.: Evaluating information assurance strategies // Decision Support Systems. 2021. Vol. 39(3). Pp. 463–484.

15. Joint Chiefs of Staff: Information assurance: Legal, regulatory, policy and organizational legal, regulatory, policy and organizational considerations. Technical Report Fourth Edition, Department of Defense, Pentagon, Washington, 1999.

16. Hamill, J. T.: Modeling information assurance: A value focused thinking approach. Master's thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, 2020.

17. Braverman, M.: Behavioural modelling of social engineering-based malicious software. In: Virus Bulletin Conf. Towards an Ontological Model Defining the Social Engineering Domain 279.

18. Åhlfeldt, R. M., Backlund, P., Wangler, B., Söderström, E.: Security issues in health care process integration? a research-in-progress report. In: EMOI-INTEROP.

19. Granger, S.: Social engineering fundamentals, part i: Hacker tactics.

20. Schoeman, A., Irwin, B., Richter, J.: Social recruiting: a next generation social engineering attack. In: Uses in Warfare and the Safeguarding of Peace.

21. Hadnagy, C.: Social Engineering: The Art of Human Hacking. Wiley Publishing.

22. Espinhara, J., Albuquerque, U.: Using online activity as digital fingerprints to create a better spear phisher. Technical report, Trustwave SpiderLabs.

23. Nemati, H.: Pervasive Information Security and Privacy Developments: Trends and Advancements, 1st edn. Information Science Reference.

24. McQuade III, S. C.: Understanding and managing cybercrime. Prentice Hall, Boston.

25. Griffiths, David, and Timothy Goddard. «An Explanatory Framework for Understanding Teachers Resistance to Adopting Educational Technology» // Kybernetes. 2022. Vol. 44. Pp. 240–250.

26. Francois Mouton, Mercia M. Malan, Kai K. Kimppa, H. S. Venter Necessity for ethics in social engineering research // Computers & Security. 2019. Vol. 55. Pp. 114–127.

27. Francois Mouton, Mercia M. Malan, Kai K. Kimppa, H. S. Venter Necessity for ethics in social engineering research // Computers & Security. 2019. Vol. 55. Pp. 114–127.

28. Slade, John A. Law and Psychology // The Journal of Abnormal and Social Psychology. 2020. Vol. 24. Pp. 212–216.

29. Davis, Beverly J. PREPARE: Seeking Systemic Solutions for Technological Crisis Management // Knowledge and Process Management. 2022. Vol. 12. Pp. 123–131.

30. Alistair S. Social Engineering in the Information Age // The Information Society. 2021. Vol. 21. Pp. 67–71.

31. Denning, Dorothy E. The United States vs. Craig Neidorf: A Debate on Electronic Publishing, Constitutional Rights and Hacking // Communications of the Association for Computing Machinery. 2021. Vol. 34. Pp. 22–43.

32. Gragg, David. A Multi-Level Defense Against Social Engineering. SANS Institute InfoSec Reading Room, Pp. 1–21.

33. Huber, Markus, Martin Mulazzani, Gerhardt Kitzler, Sigrun Goluch, and Edgar Weippl. Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam // IEEE Internet Computing. 2021. Vol. 15. Pp. 28–34.

34. Reid, Jim. Plugging the Holes in Host-Based Authentication // Computers & Security. 2021. Vol. 15. Pp. 661–671.

35. Hancock, Bill. Simple Social Engineering // Network Security . 2021. Vol. 6. Pp. 13–14.

36. Heartfield, Ryan, George Loukas, and Diane Gan. You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks // IEEE Access Journal. 2023. Vol. 4. Pp. 910–928.

37. Gilliland K. Understanding the IM Security Threat // EDPACS. 2021. Vol. 33. Art. 2006.

К. М. Беликова,
доктор юридических наук, профессор,
Московский государственный юридический
университет имени О. Е. Кутафина

СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ ПРАВОВОЙ РЕГЛАМЕНТАЦИИ НЕВЗАИМОЗАМЕНЯЕМЫХ ТОКЕНОВ (NFT)

Аннотация. В статье в контексте применения новых цифровых технологий, стоящих или способных встать на службу права интеллектуальной собственности, и с позиции российского и зарубежного опыта, в том числе: нормативных актов, рекомендательных инициатив, имеющих характер актов саморегулирования, доктрины – рассматривается современное состояние и перспективы правовой регламентации технологии невзаимозаменяемых токенов (NFT); делаются предложения по совершенствованию отечественного законодательства.

Ключевые слова: право, цифровые технологии, права интеллектуальной собственности, невзаимозаменяемые токены, технология блокчейн, смарт-контракты, финансовые акты

CURRENT STATE AND PROSPECTS OF LEGAL FRAMEWORK OF NON-FUNGIBLE TOKENS (NFT)

Abstract. In the article in the context of the application of new digital technologies that stand or are capable of serving intellectual property rights and from the perspective of Russian and foreign experience, including acts that create legal framework and acts of a self-regulation nature (Initiatives, etc.), doctrine, etc., the current state and prospects of legal regulation of non-fungible tokens technology (NFT) are considered; suggestions for improvement of domestic legislation are made.

Keywords: law, digital technologies, intellectual property rights, non-fungible tokens, blockchain technology, smart contracts, financial assets

Введение. Цифровые технологии – это те, где информация представляется в универсальном цифровом виде [24. С. 189-192]. Какого-либо общего определения цифровых технологий в российском законодательстве нет [36]. Его можно формулировать путем анализа подходов законодательства и доктрины или найти в документах типа государственных стандартов, которые применяются добровольно, если в законах нет указания об обратном [30] в той или иной сфере цифровизуемых отношений. Так, Постановление Госстандарта РФ от 29.07.2003 № 255-ст «О принятии и введении в действие государственного стандарта» [33] утвержден «ГОСТ Р 33.505-2003. Государственный стандарт Российской Федерации. Единый российский страховой фонд документации. Порядок создания страхового фонда документации, являющейся национальным научным, культурным и историческим наследием» в п. 3.17 определяет цифровые технологии как технологии, использующие электронно-вычислительную аппаратуру для записи кодовых импульсов в определенной последовательности и с определенной частотой.

Множество людей успело испытать на себе и оценить положительный эффект от применения цифровых технологий в различных областях: от обеспечения надежных коммуникаций между людьми и с государственными органами, повышения эффективности труда за счет автоматизированного компьютерного управления и контроля за технологическими и производственными процессами, до организации доступности к широкому кругу информации, способствующей не только овладеванию новыми знаниями, но и помогающей в ее использовании и применении [23].

Тем самым цифровизация превратилась в динамично развивающуюся реальность и одновременно вызов современности.

Если рассмотреть всю совокупность прав интеллектуальной собственности (ИС) с позиции приведенного определения цифровой технологии можно назвать неисчерпывающий ряд технологий (новых цифровых инструментов и одновременного в той или иной степени – объектов правового регулирования), применимых в сфере ИС: технология невзаимозаменяемых токенов (non-fungible tokens, NFT), нейросетевые технологии и др.

Рассмотрим подробнее технологию невзаимозаменяемых токенов, которая может быть поставлена на службу права интеллектуальной собственности.

Основная часть. Невзаимозаменяемые токены (NFT) являются цифровыми объектами, возникающими в результате замены имеющихся данных уникальными идентификационными символами, сохраняющими всю необходимую информацию о данных без ущерба для их безопасности на основе технологии распределенных реестров (блокчейн) [8. С. 226–232; 46] и смарт-контракта [15. С. 236–247], которая во-первых, охраняет авторское право, подтверждая уникальность цифрового объекта (NFT нельзя подделать и украсть); во-вторых, сохраняет историю его изменений и перепродаж (объектом таких сделок являются не сами произведения цифрового искусства, а уникальный цифровой код (токен), в который такие произведения (например, картина, видеозапись или иной цифровой файл) предварительно конвертировались) [10. С. 44–66; 14. С. 66–74]; в-третьих, позволяет авторам произведений (напр., художникам и пр.) программировать роялти таким образом, что каждый раз, когда NFT продается новому владельцу, соответствующий автор может получать процент от покупной цены, в том числе в условиях создаваемых и совершенствуемых метавселенных [12. С. 136–154; 29] (виртуальных пространств, основанных на технологиях Интернет, дополненной и виртуальной реальности и др.).

Наиболее часто встречающимися NFT на сегодня являются произведения искусства, объекты виртуального мира и цифровые версии актеров, певцов, спортсменов [43], другие объекты – это видео, предметы коллекционирования, виртуальные аватары, музыка, 3D-модели. Вместе с тем NFT может быть создан на основе практически любого объекта: Д. Дорси, основатель Twitter, продал NFT на базе своего первого твита более чем за 2,9 миллиона долларов [22]. NFT могут удостоверять (фиксировать) права (вещные, обязательственные, иные имущественные [19. С. 14; 21], например, инвестиционные права [44]).

Сбер [38] так описывает NFT: это вид криптографических токенов, каждый из которых уникален и не может быть обменян или замещен другим. NFT подтверждает факт владения уникальным цифровым активом, будь то видеоролик, предмет искусства, музыкальный трек и многое другое. NFT – дополнительный канал продажи и распространения цифрового искусства, новый источник дохода для художников в эпоху цифровых технологий.

В открытой печати [8. С. 44–66; 26] обобщаются способы «помещения» произведений искусства в блок: 1) токенизация аналогового объекта (например, трафарета «Morons (White)» Бэнкси); 2) токенизация объекта, созданного в электронной форме (например, цифровой картины «Первые 5000 дней» М. Винкельманна); 3) создание объекта в блокчейне (CryptoPunks Lavra Labs (URL: https://www.larvalabs.com/cryptopunks); Сбер (URL: https://dfa.sber.ru/nft)). Делается это для того, чтобы показать различия в юридических последствиях, которые следует учитывать, когда имеешь дело с такими объектами и их прототипами. Так, например, если токенизируется аналоговое произведение, необходимо выяснить его судьбу (перейдут ли к приобретателю NFT какие-либо права на него и т. п. [48]). Видимо во избежание различных правовых проблем и необходимости их решения вышеупомянутый трафарет Бэнкси «Morons (White)» сожгли, оставив только виртуальную версию в виде NFT-токена [26].

Вместе с тем, NFT отличаются от токенов, которые используются как криптовалюты тем, что являются по своей природе невзаимозаменяемыми: каждый NFT существует сам по себе и способен содержать в себе уникальную информацию, характеризующую отдельный токен (например, его идентификационный номер (token ID) и скрытые данные).

В основе некоторых NFT лежит элемент сообщества, когда владение NFT дает право на членство в онлайн-социальном клубе (например, Bored Ape Yacht Club). Такие механизмы доступа могут применяться различными организациями (медицинскими, сервисами по подписке [7. С. 60–72] и проч.), а также использоваться для учета своей посещаемости, например, учебных занятий на основе Proof of Attendance Protocol, поскольку NFT позволит организаторам учебных занятий выдавать участникам жетоны, а обучающимся вести постоянный публичный учет своего опыта – документировать учебные занятия [41].

Исходя из того, что цифровые технологии предположительно должны делать жизнь лучше, они должны улучшать положение, прежде всего, авторов, компаний, владеющих объектами ИС, как активами. Поэтому актуальность применения технологии блокчейн в сфере предпринимательской деятельности и в частности, в сфере оборота и защиты от незаконного использования объектов интеллектуальной собственности обусловлена, прежде всего, растущим уровнем популярности удаленных сервисов и высокой степенью развития конкуренции в эпоху сетевой экономики. Вместе с тем, применительно к NFT негативная сторона действительности состоит в том, что проверить подлинность NFT можно, а вот убедиться в том, что его создатель действительно тот, за кого себя выдает, нет. К примеру, мошенники могут легко выдать себя за художника, и продать подделку его произведения, использовав для верификации подлинности работающий NFT [12. С. 66–74]. А достичь цели подтверждения того, что указанный автор – это подлинный автор, действующее и потенциальное регулирование на сегодня не может или может лишь отчасти [40].

Помочь в решении этой проблемы практически могут, по нашему мнению, компьютерные алгоритмы нейросети, натренированной на выявление отклонений от нормы в поведении лиц, загружающих произведения в систему для создания NFT в качестве авторов, но не являющихся ими (чрезмерная нервозность, иное атипичное поведение, не свойственное истинным авторам произведений, загружающим свои работы по аналогии с тем, как сейчас трекер глаз, лица, частей тела в *Horizon Workrooms* отслеживает эти активности, что сделать движения аватара более плавными [29]), либо создание произведения целиком в метавселенной.

Такие идеи требуют совершенствования подходов к правовому регулированию личных данных человека, включая биометрию, поскольку цель законодательного регулирования – нивелировать негативные стороны действия цифровых технологий и поддерживать позитивные.

Работа в метавселенных и с применением NFT может решить также и другую проблему. Ранее мы писали о закрытой и открытой стратегиях создания инноваций (close и open innovations) на основе сетевого взаимодействия в контексте изобретательства, описывая, в том числе, характер защиты прав ИС [5. С. 51–63;

4. С. 58–83; 3. С. 174–181; 2. С. 182–190], теперь, когда на смену взаимодействия посредством сети Интернет приходят метавселенные, вопрос защиты результатов работы научных коллективов в формате стратегии открытых инноваций становится легко решаемым.

Основная правовая проблема использования NFT в России – отсутствие специального правового регулирования [10. С. 44–66], что порождает различные идеи относительно того, как следует их регулировать, например, отмечается [17], что, будучи записью на блокчейне, удостоверяющей права на цифровой актив, NFT не могут быть отнесены ни к вещам в силу своей нематериальной природы, ни к охраняемым результатам интеллектуальной деятельности и приравненным к ним средствам индивидуализации, так как обособленно не представляют ценности для их держателя, а лишь подтверждают права на цифровой объект, потому их, по размышлению, относят к «иному имуществу». Интересно потому посмотреть, что регламентирует законодательство относительно NFT за рубежом.

Выявлено, что, например, в Великобритании нет конкретных правил в отношении NFT, которые рассматриваются как разновидность криптоактивов, тогда как выпущенные Казначейством ее Величества «Правила об отмывании денег, финансировании терроризма и переводе денежных средств (Информация о плательщике) 2017 г. [50] налагают на биржи цифровых активов и провайдеров электронных кошельков обязанность регистрироваться в Управлении финансового контроля Великобритании (Financial Conduct Authority, FCA), прежде, чем предпринимать какие-либо действия, связанные с цифровыми активами [31]. В этой связи отмечается, что, учитывая широкое определение «криптоактивов, принятое указанными правилами, и закрепляемое как «любое криптографически защищенное цифровое представление ценности или договорных прав, которое использует технологию распределенного реестра и может передаваться, храниться или продаваться в электронном виде» [6. С. 1–28], и то, что FCA еще не удалось четко классифицировать эти токены (NFT), кажется вероятным [50], что вышеупомянутая регистрация будет применяться и к биржам цифровых активов, имеющим дело с NFT.

Сходный с британским подход проводится и в свободных экономических зонах (СЭЗ) Объединенных Арабских Эмиратов. Так, в консультационном документе СЭЗ Абу-Даби «Предложения по улучшению рынков капитала и виртуальных активов» [42] указывается на необходимость соблюдения Правил СЭЗ по борьбе с отмыванием денег, для чего, в том числе компаниям, желающим торговать NFT, потребуется получить лицензию финансового регулятора СЭЗ; СЭЗ Дубая уже ввела лицензирование деятельности NFT маркетплейсов.

Тогда как, хотя в Европейском Союзе и его странах-участницах нет общего регулирования или юридического определения NFT, Европейская комиссия опубликовала «Правила о рынках крипто-активов» [49], которые по общему правилу исключают NFT из сферы их действия. Однако в случаях, когда NFT предоставляет его владельцу права, которые могут вытекать и из ценных бумаг, например, право на получение прибыли и другие, NFT входят в сферу действия данных Правил.

Сходным образом в Сингапуре законодатели исходят из того, что, в ряде случаев, например, если NFT будет представлять права на портфель котирующихся на бирже акций, и т. п. он будет признаваться обладающим характеристиками продукта рынка капитала в соответствии с Законом о ценных бумагах и фьючерсах [47], что повлечет за собой, например, применение к нему требований, предъявляемых к: проспекту эмиссии ценных бумаг, лицензированию такой деятельности, деловому поведению осуществляющих такую деятельность лиц и др.

В США также нет особого федерального регулирования NFT, их следует рассматривать как крипто-активы, на которые, считают в Комиссии по ценным бумагам США (Securities and Exchange Commission, SEC), должны быть распространены законы о ценных бумагах, если традиционный Howey test (основа теста заложена в деле SEC v. W.J. Howey Co., 328 U.S. 293 (1946) и продолжена в делах United Housing Found., Inc. v. Forman, 421 U.S. 837 (1975); Tcherepnin v. Knight, 389 U.S. 332 (1967); SEC v. C. M. Joiner Leasing Corp., 320 U.S. 344 (1943)) выявит такое соответствие после анализа цифровых активов, включая, но не ограничиваясь цифровыми валютами (“virtual currencies”), монетами (“coins”), токенами (“tokens”) наличия у рассматриваемого цифрового актива характеристик какого-либо соответствующего федеральным законам о ценных бумагах определению ценной бумаги (security) продукта, – «инвестиционного контракта» (“investment contract”), акции (stocks), облигации (bonds), передаваемого пая (transferable shares)) [44].

Вместе с тем законопроект об ответственных финансовых инновациях Люммиса-Гиллибранда (Lummis-Gillibrand Responsible Financial Innovation Act (RFIA) от 7 июня 2022 г., предполагающий урегулировать все виды финансовых активов США, относит большинство цифровых валют к товарам (commodity), регулирование которых отводится Комиссии по торговле товарными фьючерсами (Commodity Futures Trading Commissions, CFTC). Законопроект также предлагает способ разграничения финансовых активов – товаров и финансовых активов – ценных бумаг [51]. Commodities традиционно понимаются как сырьевые товары (зерно, золото, говядина, нефть, природный газ и др.) и с недавнего времени включает в себя финансовые продукты, такие как иностранные валюты и индексы, которые можно покупать и продавать на специализированных биржах в качестве финансовых активов.

Что касается Китая, то Совместная инициатива Национальной ассоциации интернет-финансов Китая (China National Internet Finance Association), Китайской банковской ассоциации (China Banking Association) и Ассоциации по вопросам ценных бумаг Китая (Securities Association of China) по предотвращению финансовых рисков, связанных с NFT, от 13 апреля 2022 г. направлена на предотвращение финансиализации (перехода от индустриальной экономики к экономике услуг [18. С. 45–58]) и секьюритизации (преобразование дебиторской задолженности в легко реализуемые ценные бумаги путем обособления однородных активов разных владельцев в пул, под который выпускают ценные бумаги, распространяемые затем на финансовом рынке с обслуживанием их в течение всего срока действия и передачей всех полученных сумм владельцам этих активов [18. С. 44–47; 25]) NFT и связанных с этим рисков в финансовой деятельности [45].

Это акт саморегулирования, не имеющий обязательной юридической силы, тем не менее его положения, вероятно, лежат в русле политики государства в этом вопросе.

В Инициативе говорится, что «рынок NFT в Китае в последние годы становится все более популярным» и впервые вводится понятие NFT – 非同质化通证 вместо 非同质化代币, что служит подтверждением наличия в Китае концепции в отношении NFT, отличающейся от понимания криптовалют (токенов – 代币), которые в Китае запрещены.

Инициатива гласит, что NFT строится на инновационном применении технологии блокчейн и имеет определенную ценность в содействии цифровой и реальной экономике Китая, одновременно продвигая развитие культурных и креативных индустрий. Вместе с тем, внимание в Инициативе акцентируется на том, что в основе стоимости продуктов NFT должно лежать разумное ценообразование, и требуется предотвращать ложно высокие цены таких продуктов, отклоняющиеся от закона стоимости. Иными словами, производство и обмен товаров должны осуществляться в соответствии с общественно необходимыми затратами труда, при которых цена должна соответствовать стоимости товара.

Кроме того, инициатива предполагает обеспечение защиты прав интеллектуальной собственности на базовые активы NFT (т. е. сжечь базовый актив, превращаемый в NFT, как в примере выше в Китае невозможно(?) и правдивого, точного и полного раскрытия информации о продукте NFT (в том числе, вероятно, его владельце, например, правообладателе аналогового продукта, на основе которого создан NFT-продукт), чтобы защитить право потребителей на информацию, их право выбора и право на справедливую торговлю.

Для того, чтобы заявленная в Инициативе цель достигалась, Инициатива также предлагает 6 комплаенс-методик:

1) ценные бумаги, страховые документы, кредиты, драгоценные металлы и другие финансовые активы не должны включаться в базовые активы NFT, а NFT, в свою очередь, не должны использоваться при выпуске и торговле любыми финансовыми продуктами;

2) любой бизнес в сфере первичного размещения монет (initial coin offering, ICO – способа привлечения и сбора инвестиций для проектов, связанных с криптовалютами), путем NFT запрещен; недопустимо ослаблять невзаимозаменяемые характеристики NFT с помощью таких методов, как разделение собственности путем создания ее пакетов, приводящего к расщеплению прав на нее (халвинга – англ. – halving – деление пополам)) [1];

3) запрещено создавать какие-либо торговые площадки в нарушение правил централизованной торговли (например, правил централизованных торгов, электронного матчинга (мэтчинга (matching – поиска и сопоставления товаров, по которым планируется мониторинг цен на разных сайтах), анонимной торговли [20], деятельности маркет-мейкеров [37] (профессиональных участников торгов, заключивших договор с биржей о поддержании уровня цен торгуемых активов для придания рынку ликвидности, т. е. возможности быстро продать актив по цене, близкой к рыночной) и т. д.), непрерывной листинговой торговли, торговли

стандартизованными контрактами (т. е. биржевой торговли [11]) для торговли NFT.

Дело в том, что 1 января 2023 г. на церемонии в Пекине была официально запущена первая в Китае одобренная государством торговая площадка цифровых активов, которая поддерживает «вторичную торговую деятельность», т. е. перепродажу – Китайская платформа для торговли цифровыми активами (China Digital Asset Trading Platform). Типы активов, с которыми можно совершать сделки на платформе, включают объекты интеллектуальной собственности, в том числе цифровые объекты авторского права и цифровые предметы коллекционирования, которые являются китайской версией NFT [53].

Представляется, что, если NFT-платформы следуют указанным ограничениям и не используют NFT для цели выпуска и торговли какими-либо финансовыми продуктами, у них есть возможность проводить NFT-бизнес в виде предоставления услуг, связанных с покупкой NFT базовых цифровых произведений искусства;

4) запрещено использование криптовалют [13. С. 55–62], таких как, BTC (Bitcoin – была создана Сатоши Накамото [9; 17]), ETH (валюта, используемая на платформе Ethereum с открытым исходным кодом на основе блокчейна, которая была предложена в конце 2013 г. В. Бутериным и Г. Вудом и профинансирована за счет онлайновой крауд-продажи в 2014 г. [19]) и USDT (токен Tether выпущенный зарегистрированной в 2014 г. в Гонконге компанией Tether Limited [39]), при установлении цены NFT или при расчетах ими.

Такой подход согласуется с текущими строгими запретами Китая на криптовалюты, где они не имеют того же правового статуса, что и законные валюты, и не могут циркулировать на рынке, как валюты или другие инструменты ценообразования;

5) для эмитентов, покупателей и продавцов NFT Инициатива предлагает обрабатывать аутентификацию по реальному имени каждого из них, а также надлежащим образом хранить идентификационную информацию о клиентах и записи транзакций по выпуску, сочетая эту работу с активной работой в сфере сотрудничества по борьбе с отмыванием денег, что стоит принимать во внимание операторам NFT-платформ;

6) запрещено прямо или косвенно инвестировать в NFT или предоставлять какую-либо финансовую поддержку таким инвестициям, что, вероятно, следует понимать как ограничение для инвесторов от инвестирования в NFT в качестве финансовых продуктов с целью получения прибыли от финансовых инвестиций, а не как запрет обычным пользователям покупать NFT для практических целей, таких как создание частной коллекции произведений искусства.

Вместе с тем на следующий после выпуска данной Инициативы день в ответ на нее общественные организации под эгидой Министерства промышленности и информационных технологий Китая – Китайская ассоциация мобильной связи Metaverse Consensus Circle (China Mobile Communications Association Metaverse Consensus Circle, CMCA-MCC) и Специализированный комитет по блокчейну Китайской ассоциации индустрии связи (China Communications Industry Association Blockchain Specialised Committee, CCIAPC) выпустили «Требования по вопросу

регламентации здорового развития индустрии цифровых коллекций с характером акта саморегулирования» [52], в которых акцентировали вопрос о том, что цифровые коллекции, имеющие в основе технологию NFT, только начинают развиваться, не ясны стандарты их стоимости, потому саморегулирование это тот механизм, который пока нужен, и он должен основываться на идее разумных ожиданий, а потребители должны находиться в рамках правильной концепции потребления (примем во внимание стоимость объектов, созданных посредством технологии), усиливать меры самозащиты, а также сознательно сопротивляться незаконной финансовой деятельности и держаться подальше от нее, а равно сообщать о ставших известными незаконных действиях с NFT заблаговременно. Таким образом, по сути требования в области саморегулирования в основном повторяют соответствующие требования Инициативы.

Как оценить эти положения? Представляется разумным проведение аутентификации по реальному имени, введение запрета использования криптовалют при установлении цены NFT или при расчетах ими, а равно запрета делить NFT, ибо NFT-объект это, как правило, объекты-произведения искусства.

Вместе с тем хотя, очевидно, процесс создания NFT-объекта на базе существующих аналогового или цифрового произведений (картины и проч.) не является творческим по характеру, в отличие от характера создания первоначального (аналогового, цифрового) объекта, переводимого затем в NFT-объект, NFT – в любом случае это финансовый актив, имеющий ценность. По этой причине, в частности, идея внесенного в мае 2022 г. в Государственную Думу Российской Федерации законопроекта № 126586-8 «О внесении изменений в ст. 1225 части четвертой Гражданского кодекса Российской Федерации (в части расширения перечня охраняемых результатов интеллектуальной деятельности в виде невзаимозаменяемых токенов) (URL: https://sozd.duma.gov.ru/bill/126586-8 (дата обращения: 08.09.2023), согласно которому «невзаимозаменяемый токен уникального цифрового актива (изображений, видео или другого цифрового контента или актива) в виде невзаимозаменяемых данных, хранящихся в системе распределенного реестра», необходимо признать самостоятельным объектом интеллектуальных прав, представляется неверной, в случаях, когда дело касается создания NFT-объекта на базе уже существующих аналогового или цифрового произведений (картины и проч.).

С этой точки зрения перспективы правового регулирования определяются выявленными в зарубежном законодательстве позициями в понимании NFT либо как удостоверяющей право ценной бумаги, либо товара.

Добавим к этому, что нам представляется возможным поддержать высказанную в открытой печати идею о необходимости «предоставить таким цифровым объектам собственный правовой статус, необходимый для их эффективной правовой защиты собственниками и устойчивого, безопасного оборота. Для чего дополнить статью 128 ГК РФ новым объектом гражданских прав – цифровая вещь (объект), которая представляет собой объект, созданный и существующий в электронном виде и используемый в гражданском обороте для удовлетворения потребностей человека. Такой вещью можно владеть, пользоваться и распоряжаться,

с ней можно совершать сделки купли-продажи, обмена и иные, ее можно внести в уставный капитал общества и завещать, использовать в целях коллекционирования и т. д.» [16. С. 66–74].

Вместе с тем, не можем согласиться с идеей этих авторов, высказываемой, как представляется, в качестве общего для всех разновидностей NFT подхода о том, что «Права на такие вещи могут учитываться в распределенных реестрах – блокчейн, а NFT, в свою очередь, будет представлять собой запись в этом реестре о принадлежности конкретной цифровой вещи тому или иному лицу. То есть при осуществлении сделки купли-продажи NFT предметом такой сделки на самом деле будет цифровая вещь, на которую токен удостоверяет права», поскольку тогда не охваченными останутся NFT-объекты, созданные непосредственно в системе распределенных реестров (блокчейн) и не имеющие иных аналоговых или цифровых прототипов.

Поэтому близкой нам представляется идея рассматривать ряд NFT-объектов (например, NFT-объекты, созданные непосредственно в системе распределенных реестров (блокчейн)) как «вещь в себе» [14. С. 1–4] – цифровую вещь (объект) – некий аналог упоминавшихся выше commodities.

Также представляется возможным при некоторых условиях (например, признание такой возможности со стороны законодателя, выпуск NFT по правилам инвестиционных платформ и пр.) распространить на NFT-объекты действие норм об утилитарных цифровых правах Федерального закона от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» [37].

Тем самым представляется правильным предусмотреть не какой-то один вариант регулирования для всех разновидностей NFT, но дифференцированное правовое регулирование в зависимости от характера и функций, выполняемых NFT-записями в системе распределенных реестров (блокчейн). По-нашему мнению следует разделить NFT-объекты на две группы: имеющие автора-создателя существующих материальных объектов (живопись, музыка и др. виды искусства) и имеющие автора создания цифровых копий иных объектов (голоса, облика конкретного человека). Очевидно, что регламентация прав авторов на подобные объекты должна различаться.

Заключение. Полагаем, какой бы вариант не выбрал законодатель, NFT несомненно, создадут множество возможностей в будущем: революцию на рынке искусства, в борьбе с незаконной деятельностью в этом секторе и т. п., хотя неопределенность в отношении их категоризации и нынешняя нехватка регламентации со стороны государства на сегодняшний лень могут заставлять проявлять осторожность перед покупкой (инвестированием) в NTF.

Список литературы

1. Банки.ру. Что такое биткоин, как его добывают и чем он отличается от других криптовалют. URL: https://dzen.ru/a/ZPkWPWeF4HLCwvsP

2. Беликова К. М. Специфика сетевой модели инновационной деятельности в фармацевтике в контексте защиты интеллектуальной собственности // Проблемы экономики и юридической практики. 2020. Т. 16, №5. С. 182–190.

3. Беликова К. М. Особенности сетевой модели инновационной деятельности в кластере робототехники в контексте защиты интеллектуальной собственности // Проблемы экономики и юридической практики. 2020. Т. 16, №5. С. 174–181.

4. Беликова К. М. Открытые инновации в военной сфере: практическое измерение и защита интеллектуальной собственности // Вопросы российского и международного права. 2021. Т. 11, № 6А. С. 51–63.

5. Беликова К. М. Специфика сетевой модели инновационной деятельности в биомедицинском секторе в контексте защиты интеллектуальной собственности // Право и политика. 2021. № 6. С. 58–83.

6. Беликова К. М. Теоретические и практические аспекты правовой квалификации виртуальной собственности в России и за рубежом // Юридические исследования. 2021. № 7. С. 1–28.

7. Беликова К. М. Экономика подписок: право собственности и будущее потребления // Вопросы российского и международного права. 2021. Т. 11. № 4А. С. 60–72.

8. Беликова К. М., Ермакова И. В. Использование блокчейн- технологий в области интеллектуальной собственности (на примере сервиса n'RIS). // Право и противодействие пандемии: возможности и перспективы: монография / отв. ред. В. Н. Синюков, А. А. Мохов. Москва: Проспект, 2021. С. 226–232.

9. Белых В. С., Егорова М. А., Решетникова С. Б. Биткоин: понятие и тенденции правового регулирования. URL: https://urfac.ru/?p=2148

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

11. Гражданское и торговое право зарубежных стран: учебное пособие [Безбах В.В. и др.] ; под ред. В. В. Безбаха и В. К. Пучинского. – М.: МЦФЭР. 2004. 896 с.

12. Гринь Е. С. Метавселенная и правовая охрана результатов творческого труда // Закон. 2022. № 8. С. 136–154.

13. Егорова М. А., Белицкая А. В. Правовое регулирование выпуска и размещения криптовалюты: тенденции и перспективы // Актуальные проблемы российского права. 2020. № 6 (115). С. 55–62.

14. Емельянов Д. С. Емельянов И. С. Невзаимозаменяемые токены (NFT) как самостоятельный объект правового регулирования. // Имущественные отношения в Российской Федерации. 2021. № 7. С. 66–74.

15. Ермакова И. В. Смарт-контракт: понятие, правовое регулирование, аспекты защиты прав потребителей // Пробелы в российском законодательстве. 2021. Т. 14, № 4. С. 236–247.

16. Жучков В. А. Системообразующая роль вещи в себе в философии Канта // Кантовский сборник. 2009. № 2. С. 1–4.

17. Заговоры, ученые и религия. Кто такой Сатоши Накамото. URL: https://www.rbc.ru/crypto/news/5eddc3449a7947cd4b95d68c

18. Игнатьева Д. А. Секьюритизация как один из инструментов проведения преобразований отечественной экономики. // Финансы и кредит. 2003. № 10 (124). С. 44–47.

19. Что это такое Ethereum. URL: https://digitalocean.ru/n/obzor-kriptomonety-ethereum-efir?ysclid=lm91zlxwbh828097636

20. Подписывать NDA или NNN при покупке у китайских поставщиков? URL: https://openchina.com.ua/podpisyvat-nda-ili-nnn-pri-pokupke-u-kitajskih-postavshhikov/

21. Казанба Е. Т. Токенизированные акции: некоторые подходы права // Мат-лы X Международного юридического форума, 06-09 апреля 2023 г. (Москва, Университет имени О. Е. Кутафина (МГЮА))

22. Как не стать жертвой мошенничества с NFT? URL: https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-avoid-nft-scams?ysclid=lmacmg4hr6560170705

23. Камынина Н. Цифровые технологии в высшем образовании: современный подход к подготовке кадров. URL: https://izyskateli.info/2019/08/tsifrovye-tehnologii-v-vysshem-obrazovanii-sovremennyj-podhod-k-podgotovke-kadrov/

24. Канищева Е. М., Беляева Е. С. Цифровые технологии: понятие, виды, преимущества и недостатки // Сб. статей 10-й Международной научно-практической конференции «Актуальные проблемы международных отношений в условиях формирования мультиполярного мира», Курск: Изд-во Юго-Западного государственного университета, 2021. С. 189–192.

25. Китай нашел способ передать безнадежные долги инвесторам. URL: https://www.epochtimes.ru/kitaj-nashyol-sposob-peredat-beznadyozhnye-dolgi-investoram-99022863/

26. Коваленко Л. NFT: что это и почему так популярна эта технология. URL: https://altcraft.com/ru/blog/chto-takoe-nft

27. Лазарева Ю. А. NFT: проблема определения правовой природы и перспективы законодательства // Журнал Суда по интеллектуальным правам. URL: http://ipcmagazine.ru/re-views/nft-the-problem-of-determining-the-legal-nature-and-prospects-of-legislation#6

28. Леусенко А. Что такое криптовалюта Эфириум (ETH): особенности и отличия. URL: https://altcoinlog.com/what-is-ethereum/?ysclid=lm921vnkqj558596348

29. Масленко Д. Что такое метавселенная и почему все о ней говорят. URL: https://trends.rbc.ru/trends/industry/61449fa89a7947159f1df418

30. О ГОСТах, ТУ и СТО. 16.10.2019. URL: https://www.gostinfo.ru/InformationOfStandardization/Details/1907

31. Озерин Э. Отмывание денег – рекомендации Министерства финансов Великобритании. Казначейство Ее Величества. URL: clck.ru/35eS78

32. Постановление Госстандарта РФ от 29.07.2003 № 255-ст «О принятии и введении в действие государственного стандарта». URL: https://base.garant.ru/1594147/?ysclid=lm672zs1v9626062018

33. Родина Г. А. Современная финансиализация как новое качество экономики. // Социально-политические исследования. 2019. № 3(4). С. 45–58.

34. Рожкова М. А. Категории «цифровое право», «цифровые права» и «цифровая валюта» // Право цифровой экономики. 2021. № 17. С. 10–68.

35. Сольцин Л. О. Цифровые технологии: понятие, виды. URL: https://login.consultant.ru/link/?req=doc&base=CJI&n=146021&dst=100006&demo=1

36. Суховарина В. Кто такие маркетмейкеры? Что они делают на рынке и зачем они вообще нужны. URL: https://journal.open-broker.ru/economy/kto-takie-marketmejkery/?ysclid=lm919bkyfm47140156

37. Федерального закона от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2019. № 31. Ст. 4418.

38. ЦФА NFT. URL: https://dfa.sber.ru/nft

39. Что такое Tether (USDT)? URL: https://academy.binance.com/ru/articles/what-is-tether-usdt

40. Шевченко О. М. Финансовое мошенничество и NFT // Мат-лы Научно-практической конференции «Противодействие мошенничеству в финансовой сфере».

41. Olga_Jane1. NFT как инструмент аутентификации и обозначения членства. URL: clck.ru/35eS8u

42. Consultation Paper No. 1 of 2022. Proposals for Enhancements to Capital Markets and Virtual Assets in ADGM. URL: https://clck.ru/35eS89

43. Dowling Michael M. Is Non-fungible Token Pricing Driven by Cryptocurrencies? URL: https://ssrn. com/abstract=3815093

44. Framework for "Investment Contract" Analysis of Digital Assets. URL: https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets#_edn2

45. Initiative to prevent NFT-related risks. URL: https://law.asia/prevent-nft-related-risks

46. Louis DeNicola. What to know about non-fungible tokens (NFTs) – unique digital assets built on blockchain technology. URL: https://www.businessinsider.com/nft-meaning

47. Securities and Futures Act 2001. URL: https://www.mas.gov.sg/regulation/acts/securities-and-futures-act

48. The legal framework of non-fungible tokens (NFTs). URL: https://guden.av.tr/thelegalframeworkofnfts

49. The Markets in Crypto Assets Regulation (MiCA). URL: https://clck.ru/35eS6B

50. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, as amended by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019. URL: https://clck.ru/35eS5B

51. The Responsible Financial Innovation Act: A Comprehensive Proposal to Regulate Digital Assets. URL: https://clck.ru/37eS5B

52. The Self-Regulatory Requirements on Regulating the Healthy Development of Digital Collection Industry. URL: https://law.asia/prevent-nft-related-risks

53. Zihao Liu. Does China's New State-Backed NFT Marketplace Have Global Implications? URL: https://jingculturecrypto.com/does-chinas-new-state-backed-nft-marketplace-have-global-implications

В. А. Белов,
кандидат юридических наук,
Юридический институт «М-Логос»

КРИПТОАКТИВЫ И ИХ РЕГУЛИРОВАНИЕ: MiCA И ЕВРОПЕЙСКИЙ ПОДХОД

Аннотация. В статье рассматриваются отдельные аспекты правового регулирования на территории Европейского Союза вопросов, связанных с (1) обращением криптоактивов; (2) осуществлением расчетов с использованием криптоактивов; (3) требованиями, предъявляемых к участникам криптовалютных отношений. Актуальность указанных вопросов продиктована вступлением в 2023 г. ряда нормативных правовых актов, вносящих существенные изменения в указанной области, призванных стандартизировать и систематизировать существующие подходы.

Ключевые слова: криптоактивы, MiCA, поставщики услуг криптоактивов (CASP), расчеты с использование криптоактивов, идентификация, расчеты в криптовалюте, Европейский Союз

CRYPTO ASSETS AND THEIR REGULATION: MiCA AND EUROPEAN APPROACH

Abstract. This article focuses on certain aspects of the legal regulation in the European Union of issues related to (1) the circulation of crypto-assets; (2) making payments using crypto assets; (3) requirements for participants in cryptocurrency relations. The relevance of these issues is dictated by the entry in 2023 of a number of regulations introducing significant changes in this area, designed to standardize and systematize existing approaches.

Keywords: crypto-assets, MiCA, crypto-asset service provider (CASP), crypto payments, identification, cryptocurrency payments, European Union

Введение. В конце мая 2023 на территории Европейского союза был принят ряд нормативно-правовых актов, вносящих существенные изменения в вопросы правового регулирования криптоактивов на территории ЕС:

– регламент (ЕС) 2023/1114 о рынках криптоактивов (далее – «MiCA»), который устанавливает правовые основы регулирования вопросов, связанных с обращением и оказанием услуг при использовании криптоактивов на территории ЕС (Данный документ был опубликован 9 июня 2023 г., вступил в силу 29 июня 2023 г. и должен быть внедрен в национальное законодательство стран-членов ЕС не позднее 30 декабря 2024 г.) [1];

– регламент (ЕС) 2023/1113 Европейского Парламента и Совета от 31 мая 2023 г. (далее – Регламент о переводах) об информации, сопровождающей переводы средств и определенных криптоактивов, и вносящий поправки в Директиву (ЕС) 2015/849 (данный документ был опубликован 9 июня 2023 г. и вступил в силу 29 июня 2023 г.) [2].

В довольно внушительных преамбулах MiCA и Регламента о переводах, которые суммарно составляют 184 пункта, аккумулируются существующие знания, а также области правового регулирования различных аспектов деятельности, ставя перед собой цели по обеспечению стабильности и безопасности в криптовалютной индустрии на территории Европейского союза, защите прав потребителей и инвесторов, предотвращение отмывания денежных средств, полученных преступным путем, и финансирование терроризма при помощи криптовалют и т. д. Помимо сказанного, цель Регламента – установить порядок правового регулирования следующих аспектов деятельности участников отношений, использующих криптоактивы:

1) требования прозрачности и раскрытия информации при выпуске, публичном предложении и допуске криптоактивов к торгам на торговой платформе для криптоактивов («допуск к торгам»);

2) требования к авторизации и надзору за поставщиками услуг криптоактивов, эмитентами токенов, привязанных к активам, и эмитентами токенов электронных денег, а также к их работе, организации и управлению;

3) требования по защите держателей криптоактивов при выпуске, публичном предложении и допуске к торгам криптоактивами;

4) порядок осуществления платежей и переводов криптовалюты от отправителей к бенефициарам;

5) требования по защите клиентов поставщиков услуг криптоактивов;

6) меры по предотвращению инсайдерских сделок, незаконного раскрытия инсайдерской информации и манипулирования рынком, связанных с криптоактивами, с целью обеспечения целостности рынков криптоактивов.

Таким образом, MiCA и Регламент о переводах устанавливают фундаментальные основы порядка обращения и предоставления услуг с криптоактивами на территории Европейского Союза.

Понятие криптоактива. В целом понятие криптоактива устанавливается ст. 3 MiCA, согласно которой под криптоактивом понимается цифровое представление стоимости или права, которое может быть передано и сохранено в электронном виде с использованием технологии распределенного реестра или аналогичной технологии. Нельзя не отметить, что схожее определение содержится в целом ряде правопорядков государств-членов ЕС, однако в них делается принципиальное указание, что указанное цифровое представление стоимости не выпускается центральным банком или публичным органом.

Виды криптоактивов. MiCA, как нормативно-правовой акт, устанавливает перечень объектов, которые подпадают под его регулирование. В частности, под действие Регламента подпадает три вида криптоактивов:

1. Asset Reference Token («ART») – токен, нацеленный на поддержание стабильной стоимости посредством привязки к одним или нескольким активами. Как правило, это комбинация активов (например, токен, привязанный к золоту, или к корзине валют, или к другим криптоактивам).

2. E-money Token («EMT») – электронные суррогаты монет и банкнот, которые, вероятно, будут использоваться для осуществления платежей. Ключевая характеристика – обеспеченность официальной государственной валютой.

3. Другие криптоактивы – цифровое представление стоимости или прав, которые могут передаваться и храниться в электронном виде.

Однако необходимо отметить, что MiCA не распространяется на криптоактивы, регулируемые другими инструментами финансового права ЕС, поэтому криптоактивы, которые квалифицируются как финансовые инструменты, такие как токены ценных бумаг или электронные деньги (за исключением токенов электронных денег), не подпадают под действие закона. Схожая точка зрения усматривается в юридической литературе, где указывается, что изначально подготовленный проект MiCA охватывал прежде всего вопросы, связанные с так называемыми стейблкойнами (asset-referenced token), а также утилитарных токенах (utility token). Отдельно регулируются «токены электронных денег» (e-money tokens) – по сути, стейблкойны, привязанные к некой фиатной валюте [5. С. 74–115].

Лица, вовлеченные в оборот криптоактивов. Положения MiCA распространяются на физических и юридических лиц, которые занимаются выпуском, предложением общественности криптоактивов и допуском к торговле криптоактивами, или предоставляющих услуги, связанные с криптоактивами в Европейском Союзе. Регламент относит у указанным субъектам следующих лиц:

1. Эмитенты криптоактивов – это юридические лица, которые предлагают публике любой вид криптоактивов или добиваются допуска таких криптоактивов на торговую платформу для криптоактивов.

2. Поставщики услуг криптоактивов (сервис провайдеры) – любые лица, осуществляющие деятельность по предоставлению одной или нескольких услуг в области криптоактивов третьим лицам на профессиональной основе.

3. Любые лица, осуществляющие действия, связанные с торговлей криптоактивами, которые допущены к торговле на торговой платформе для криптоактивов, или в отношении которых был подан запрос на допуск к торговле на такой торговой платформе.

Важно отметить, что несмотря на то обстоятельство, что Регламент прямо не расшифровывает правовой режим лиц из третьих стран, допустимо предположить, что по смыслу п. 75 Преамбулы MiCA, если компания из третьей страны самостоятельно (т. е., без первоначальной инициативы клиента из ЕС) привлекает клиентов или потенциальных клиентов в Евросоюзе или продвигает, рекламирует криптоуслуги или свою деятельность в ЕС, к ней будут применяться требования MiCA.

Услуги с криптоактивами. MiCA выделяет следующие виды услуг с криптоактивами, которые подпадают под его правовое регулирование:

1) обеспечение хранения и администрирования крипто-активов от имени клиентов;

2) работа торговой площадки для криптоактивов;

3) обмен криптоактивов на денежные средства;

4) обмен криптоактивов на другие криптоактивы;

5) выполнение заказов на криптоактивы от имени клиентов;

6) размещение криптоактивов;

7) прием и передача заявок на криптоактивы от имени клиентов; (час) предоставление консультаций по криптоактивам;

8) обеспечение управления портфелем по криптоактивам;

9) предоставление услуг по переводу криптоактивов от имени клиентов.

Примечательным положением является то, что при оказании услуг с криптоактивами, регулятор фактически приравнял и предоставил отдельным категориям таких услуг права, аналогичные тем, что закреплены в Директиве 2011/83/ЕС Европейского парламента и Совета от 25 октября 2011 г. о правах потребителей [3]. Так, ст. 13 MiCA устанавливает право для розничных клиентов, которые приобретают криптоактивы, право на возврат приобретенных криптоактивов в течение 14 календарных дней, когда последние могут отказаться от своего соглашения о покупке криптоактивов. Реализация указанного права ограничена, в случае если криптоактивы были допущены к публичной торговле до их покупки розничным держателем.

Поставщики услуг криптоактивов. Согласно ст. 59 MiCA поставщик услуг криптоактивов или CASP (Crypto Asset Service Provider) – это любое лицо, которое предоставляет одно или несколько связанных с подобными активами услуг третьим лицам на профессиональной основе. В отношении поставщиков услуг криптоактивов установлены следующие минимальные требования:

1. Поставщики услуг криптоактивов обязаны получить авторизацию (лицензию) от уполномоченного органа.

2. Поставщики услуг криптоактивов должны иметь зарегистрированный офис в государстве-члене ЕС, где они предоставляют хотя бы часть своих услуг криптоактивов.

3. Место эффективного управления деятельностью поставщика услуг криптоактивов должно находиться в Союзе, и по крайней мере один из директоров должен быть резидентом Союза.

4. Поставщики услуг криптоактивов должны всегда соблюдать условия их авторизации (лицензии). Лицо, не являющееся поставщиком услуг криптоактивов, не должно использовать имя или фирменное наименование, выпускать маркетинговые сообщения или предпринимать какие-либо другие действия, предполагающие, что оно является поставщиком услуг криптоактивов, или которые могут создать путаницу в этом отношении.

5. Поставщикам услуг криптоактивов разрешается предоставлять услуги криптоактивов на всей территории Союза либо посредством права учреждения, в том числе через филиал, либо посредством свободы предоставления услуг.

6. Поставщики услуг криптоактивов, которые предоставляют услуги криптоактивов на трансграничной основе, не обязаны иметь физическое присутствие на территории принимающего государства-члена.

7. Минимальный уставный капитал должен варьироваться от €50 000 до €150 000 евро в зависимости от предоставляемых услуг.

Для целей авторизации (получения лицензии) у уполномоченного органа поставщик услуг криптоактивов обязан предоставить заявление со следующими документами и сведениями:

1) имя, включая юридическое название и любое другое используемое коммерческое название, идентификатор юридического лица заявителя-провайдера услуг криптоактивов, веб-сайт, управляемый этим провайдером, контактный адрес электронной почты, номер контактного телефона и его физический адрес;

2) юридическая форма заявителя-провайдера услуг криптоактивов;

3) устав заявителя-провайдера услуг криптоактивов, если применимо;

4) программу операций, определяющую типы услуг криптоактивов, которые заявитель поставщик услуг криптоактивов намерен предоставлять, включая место и способы продажи этих услуг;

5) доказательство того, что поставщик услуг криптоактивов-заявитель соответствует требованиям пруденциальных гарантий;

6) описание механизмов управления поставщика услуг криптоактивов заявителя;

7) доказательство того, что члены органа управления заявителя-провайдера услуг криптоактивов имеют достаточно хорошую репутацию и обладают соответствующими знаниями, навыками и опытом для управления этим провайдером;

8) личность любых акционеров и участников, прямых или косвенных, которые имеют существенные доли в организации-заявителе на лицензию поставщика услуг криптоактивов, и что эти лица имеют достаточно хорошую репутацию;

9) описание механизмов внутреннего контроля, политик и процедур заявителя-провайдера услуг криптоактивов для выявления, оценки и управления рисками, включая риски отмывания денег и финансирования терроризма, а также план обеспечения непрерывности бизнеса;

10) техническая документация систем и мер безопасности, а также их описание на нетехническом языке;

11) описание процедуры разделения криптоактивов и средств клиентов;

12) описание процедур рассмотрения жалоб поставщика услуг криптоактивов заявителя;

13) если заявитель-провайдер услуг криптоактивов намеревается обеспечить хранение и управление криптоактивами от имени клиентов, описание политики хранения и управления;

14) если заявитель-провайдер услуг криптоактивов намеревается управлять торговой платформой для криптоактивов, описание правил работы торговой платформы, а также процедуры и системы обнаружения злоупотреблений на рынке;

15) если заявитель-провайдер услуг криптоактивов намеревается обменять криптоактивы на средства или другие криптоактивы, описание коммерческой политики, которая должна быть недискриминационной и регулирующей отношения с клиентами, а также описание методологии определения цены криптоактивов, которые заявитель-провайдер услуг криптоактивов предлагает обменять на средства или другие криптоактивы;

16) если заявитель-поставщик услуг криптоактивов намеревается выполнять заказы на криптоактивы от имени клиентов, описание политики исполнения;

17) если поставщик услуг криптоактивов-заявитель намеревается предоставить консультации по криптоактивам или управлению портфелем криптоактивов,

доказательство того, что физические лица, дающие консультации от имени поставщика услуг криптоактивов или управляющие портфелями от имени заявителя -поставщик услуг по управлению активами обладает необходимыми знаниями и опытом для выполнения своих обязательств;

18) если заявитель-поставщик услуг криптоактивов намеревается предоставлять услуги по передаче криптоактивов от имени клиентов, информация о том, каким образом будут предоставляться такие услуги по передаче;

19) тип криптоактива, к которому относится сервис криптоактивов.

Представляется, что приведенные требования на получение авторизации (лицензии), прежде всего, систематизируют и унифицируют подход допуска лиц к рынку криптоактивов, а также направлены на защиту интересов клиентов и потребителей.

Расчеты между владельцами криптоактивов. Помимо MiCA, регламентирующего правовой статус участников отношений с криптоактивами, существенную роль выполняет Регламент о переводах, согласно которому устанавливаются требования, предъявляемые к переводам криптоактивов между участниками соответствующих взаимоотношений с привлечением поставщиком услуг криптоактивов. Так, ст. 14 Регламента о переводах устанавливает, что поставщик услуг криптоактивов должен обеспечить условие, чтобы передача криптоактивов сопровождалась следующей информацией:

1) имя отправителя (владельца крипто-кошелька);

2) адрес распределенного реестра отправителя, а также номер счета криптоактива отправителя;

3) номер счета криптоактива отправителя;

4) адрес отправителя, включая название страны, официальный номер личного документа и идентификационный номер клиента или, альтернативно, дату и место рождения отправителя;

5) доступный официальный идентификатор отправителя;

6) имя бенефициара (получателя криптоактивов);

7) адрес распределенного реестра бенефициара, а также номер счета криптоактива бенефициара;

8) номер счета криптоактивов бенефициара;

9) доступный официальный идентификатор бенефициара.

Вся указанная информация должна быть представлена до или одновременно с передачей криптоактивов, безопасным способом и в соответствии с Регламентом (ЕС) 2016/67, а также поставщик услуг криптоактивов отправителя должен обеспечить, чтобы передача криптоактивов сопровождалась уникальным идентификатором транзакции. Помимо прочего, в рамках соблюдения положений о противодействии отмыванию денежных средств, полученных преступным путем, в случае перевода суммы, превышающей 1 000 евро, поставщик услуг криптоактивов должен принять адекватные меры для оценки того, принадлежит ли этот адрес отправителю или контролируется им.

Схожие требования предъявляются и к поставщикам услуг криптоактивов, обслуживающих бенефициаров (получателей криптоактивов). Так, ст. 16 Регламента

о переводах предписывает обязанность поставщику услуг криптоактивов бенефициара внедрить эффективные процедуры, включая, при необходимости, мониторинг после или во время переводов. При этом, в случае перевода суммы, превышающей 1 000 евро, поставщик услуг криптоактивов должен принять адекватные меры для оценки того, принадлежит ли этот адрес бенефициару или контролируется им.

Несоблюдение приведенных требований в части идентификации отправителя и получателя криптоактивов, а также не предоставление соответствующей информации может являться основанием для (i) отказа в совершении транзакции; (ii) запроса необходимой дополнительной информации относительно перевода криптоактивов; (iii) информирования контролирующих органов о совершении подозрительной сделки.

Следовательно, допустимо предположить, что поставщики услуг криптоактивов будут обязаны надлежащим образом проверять всех клиентов:

– проводить идентификацию клиента (имя, адрес, дата рождения, место рождения и т. п.);

– проверять, что клиент не является лицом, к которому применены санкции;

– хранить персональные данные и информацию по предотвращению отмывания средств и финансированию терроризма;

– передавать данные вместе с транзакцией;

– в зависимости от того, проводит ли CASP транзакцию от имени отправителя или получателя, он должен будет собирать и передавать персональные данные и информацию по предотвращению отмывания средств и финансированию терроризма, или получать таковую от отправителя и проверять ее.

Заключение. Подытоживая, необходимо отметить, что MiCA и Регламент о переводах направлены на стандартизацию и открытую регламентацию вопросов, связанных с обращением криптоактивов на экономических рынках, а также снятие вуали с недобросовестных участников отношений, использующих криптоактивы для целей расчетов. Вместе с тем, несмотря на в целом позитивное представление и попытку регламентации вопросов, связанных с оборотом криптоактивов, представляется, что полное открытие и всецелое применение уже существующих подходов в области банковского регулирования к рынку обращения криптоактивов по аналогии, несколько противоречит изначальному смыслу, вложенному в криптовалютный рынок, где преследовалась цель полной анонимизации пользователей и участников сделок в условиях цифровой среды, автоматизированного подхода, применения алгоритмизации (принцип – ЦАА) [4. С. 17–23], а также публичной достоверности реестра производимых транзакций.

Список литературы

1. Regulation (Eu) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. URL: https://eur-lex.europa.eu

2. Regulation (Eu) 2023/1113 of the European Parliament And of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849. URL: https://eur-lex.europa.eu

3. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. URL: https://eur-lex.europa.eu

4. Белов В. А. Смарт-торговля (цифровая торговля): основные положения о цифровизации договорных отношений с участием потребителей // Вестник арбитражной практики. 2022. № 3 (100). С. 17–23.

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

А. С. Березина,
ассистент,
Красноярский государственный медицинский университет
имени профессора В. Ф. Войно-Ясенецкого
Ю. В. Карачева,
доктор медицинских наук,
Красноярский государственный медицинский университет
имени профессора В. Ф. Войно-Ясенецкого
А. Ю. Карачев,
кандидат медицинских наук,
Красноярский государственный медицинский университет
имени профессора В. Ф. Войно-Ясенецкого
Д. В. Дзюба,
преподаватель,
Красноярский государственный медицинский университет
имени профессора В. Ф. Войно-Ясенецкого

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ПРОГРАММ НА ОСНОВЕ СВЕРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ КОНТРОЛЯ ТЕЧЕНИЯ АТОПИЧЕСКОГО ДЕРМАТИТА

Аннотация. Цель – усовершенствовать систему дистанционного контроля течения атопического дерматита у пациентов на основе создания алгоритмов и адаптации программы сверточных нейронных сетей, а также анализа заболеваемости атопическим дерматитом в Красноярском крае за последние 5 лет. Также программируются разные модели сверточных нейронных сетей для создания на их основе программы для контроля течения атопического дерматита.

Ключевые слова: сверточные нейронные сети, атопический дерматит, модели нейронных сетей

PROSPECTS FOR THE APPLICATION OF PROGRAMS BASED ON CONVOLUTIONAL NEURAL NETWORKS TO CONTROL THE COURSE OF ATOPIC DERMATITIS

Abstract. Purpose – To improve the system for remote monitoring of the course of atopic dermatitis in patients based on the creation of algorithms and adaptation of the convolutional neural networks program, as well as analysis of the incidence of atopic dermatitis in the Krasnoyarsk Territory over the past 5 years. Various models of convolutional neural networks are also programmed to create a program based on them to control the course of atopic dermatitis.

Keywords: convolutional neural networks, atopic dermatitis, neural network models

Введение. Атопический дерматит (АД) – многофакторное, генетически детерминированное воспалительное заболевание кожи, характеризующееся зудом, хроническим рецидивирующим течением, возрастными особенностями локализации и морфологии поражений [1]. АД – одно из наиболее распространенных заболеваний кожи в промышленно развитых странах с тенденцией к увеличению, диагностируемое у 20 % детей и 1-3 % взрослых [8]. Высокий уровень заболеваемости, а также множество провоцирующих факторов, таких как продукты питания, загрязнение окружающей среды, стрессовые ситуации и климатические условия, придают эпидемиологии заболевания особую актуальность [6. С. 24–26].

Первичная диагностика АтД не вызывает трудностей, но течение заболевания требует контроля, так как чем раньше начата терапия при обострении, тем быстрее и легче купируется этот процесс [6. С. 30]. В период пандемии большинство таких пациентов осталось без контроля терапии. Большинство стационаров переоборудовано под инфекционные койки. На этом фоне существенно снизилась эффективность от терапии. В дальнейшем приходилось больше времени затрачивать на снятия обострений у пациентов с атопическим дерматитом. Также усилился контроль за ведением медицинской документации, где при ведении пациентов с хроническими дерматозами с целью улучшения контроля ведения больных, необходимо указывать различные индексы. Существует множество методик контроля обострений. Тяжесть течения и динамика заболевания оцениваются по разным шкалам: SCORAD (Scoring Atopic Dermatitis), EASY (Eczema Area and Severity Index), SASSAD (Six Area, Six Sign Atopic Dermatitis Severity Score). Помимо данных индексов существуют лабораторные и инструментальные методы контроля. В последние годы широкое применение в диагностике различных заболеваний находят нейросетевые технологии. Они уже используются в области кардиологии, онкологии, пульмонологии, гастроэнтерологии, неврологии и др. Высокая точность функционирования нейронных сетей указывает на перспективность использования искусственных нейрогенных сетей для диагностики и прогнозирования заболеваний, в том числе атопического дерматита. В настоящее время перспективным направлением становится телемедицинские консультирования.

С 1 августа в рамках экспериментального правового режима согласно постановлению Правительства Российской Федерации от 18.07.2023 № 1164 клиникам можно предоставлять плановую медицинскую помощь через телемедицинские консультации для пациентов с уже установленным диагнозом с целью контроля терапии и течения заболевания [5]. Все это позволит активизировать предпринимательскую деятельность в рассматриваемой сфере [7].

Материалы и методы. В исследовании проведен статистический анализ обращаемости пациентов Красноярского края за последние 5 лет. Также проведен опрос у 142 пациентов с атопическим дерматитом на предмет использования эмолентов на постоянной основе.

Контроль течения заболевания проводится на основе индекса SCORAD. (рис. 1).

A — площадь поражения (оценивается врачом)

Площадь поверхности отдельных участков у детей	Площадь проявлений атопического дерматита на отдельных участках тела	
	Участки тела	Площадь поражения
	Передняя поверхность головы (4,5%)	
	Задняя поверхность головы (4,5%)	
	Передняя поверхность туловища (18%)	
	Задняя поверхность туловища (18%)	
	Гениталии (1%)	
	Передняя поверхность левой руки (4,5%)	
	Задняя поверхность левой руки (4,5%)	
	Передняя поверхность правой руки (4,5%)	
	Задняя поверхность правой руки (4,5%)	
	Передняя поверхность левой ноги (9%)	
	Задняя поверхность левой ноги (9%)	
	Передняя поверхность правой ноги (9%)	
	Задняя поверхность правой ноги (9%)	
	Итого	

Показатель A = _____

B — интенсивность клинических проявлений (оценивается врачом)

Оценка клинических проявлений АД

Клинические проявления	Оценка в баллах
Эритема	
Отек или папулезность	
Мокнутье/корки	
Расчесы	
Лихенификация	
Сухость	
Итого	

Способ оценки:
0 = отсутствие проявлений
1 = легкие проявления
2 = умеренные проявления
3 = тяжелые проявления

Показатель B = _____

C — выраженность субъективных симптомов (оценивается пациентом)

Отсутствие зуда — Очень сильный зуд

0	1	2	3	4	5	6	7	8	9	10

Отсутствие нарушений сна — Очень сильное нарушение сна

0	1	2	3	4	5	6	7	8	9	10

Показатель C = _____

Рис. 36.1. Шкала оценки тяжести клинических проявлений SCORAD

Рис. 1. Индекс SCORAD

По индексу SCORAD оцениваются шесть признаков: эритема, отек/папулезные проявления, образование корок/мокнутие, экскориации, лихенификация/шелушение и сухость кожи. Каждый критерий оценивается по 4-уровневой шкале: 0 – отсутствует, 1 – слабая, 2 – умеренная, 3 – сильная. При оценке площади повреждения кожи следует пользоваться правилом девяти, согласно которому единицей измерения является площадь поверхности ладони пациента, равная одному

проценту всей поверхности кожи. Цифрами указано значение площади для больных в возрасте старше 2 лет, а в скобках – для детей в возрасте до 2 лет. Оценку субъективных симптомов (ощущение зуда, нарушение сна) проводят у детей в возрасте старше 7 лет и взрослых; у детей младшего возраста оценку субъективных симптомов проводят с помощью родителей, которым предварительно объясняют принцип оценки.

Расчет индекса SCORAD производится по формуле:

$$SCORAD = A/5+7B/2+C,$$

где: A – распространенность поражения кожи; B – сумма уровней интенсивности клинических симптомов атопического дерматита; C – сумма оценок субъективных нарушений по визуальной аналоговой шкале.

На линейке внизу рисунка указывается точка, соответствующая степени выраженности оцениваемого субъективного признака, усредненное за последние 3 суток.

Значения индекса могут варьировать в пределах от 0 (нет заболевания) до 103 (максимально тяжелое течение атопического дерматита).

Атопический дерматит легкой степени тяжести соответствует значению SCORAD<25

Атопический дерматит средней степени тяжести соответствует значению SCORAD от 25 до 50.

Тяжелый атопический дерматит соответствует значению SCORAD> 50 [1].

С целью формирования базы для программы на основе нейронных сетей производится фотографирование морфологических элементов. На основе этих изображений производится обучение. Все изображения разбиты на 3 группы:

1) обучающая выборка (70 % от общего числа), на которой обучается модель;

2) валидационная выборка (20 % обучающей выборки), на которой контролируется обучение;

3) тестовая выборка (30 % от общего количества), на которой происходит финальное тестирование модели. Для подготовки и обработки изображений мы использовали обработку данных и построение моделей в среде программирования – PyCharm (Community Edition 2020 версия 2.2), на языке программирования Python (версия 3.7.5).

Нейронная сеть – это математическая модель, состоящая из одного или нескольких слоев искусственных нейронов, относящаяся к области машинного обучения. Каждый нейрон представляет собой сложную нелинейную функцию, рассчитывающую вероятность развития того или иного исхода на основе полученных параметров (весовой коэффициент или коэффициент смещения) [3. С. 5-10]. Процесс определения этих параметров называется обучением. Простая нейронная сеть представлена многослойным перцептроном (рис. 2), а схематическое изображение искусственного нейрона изображено на рис. 3 [4].

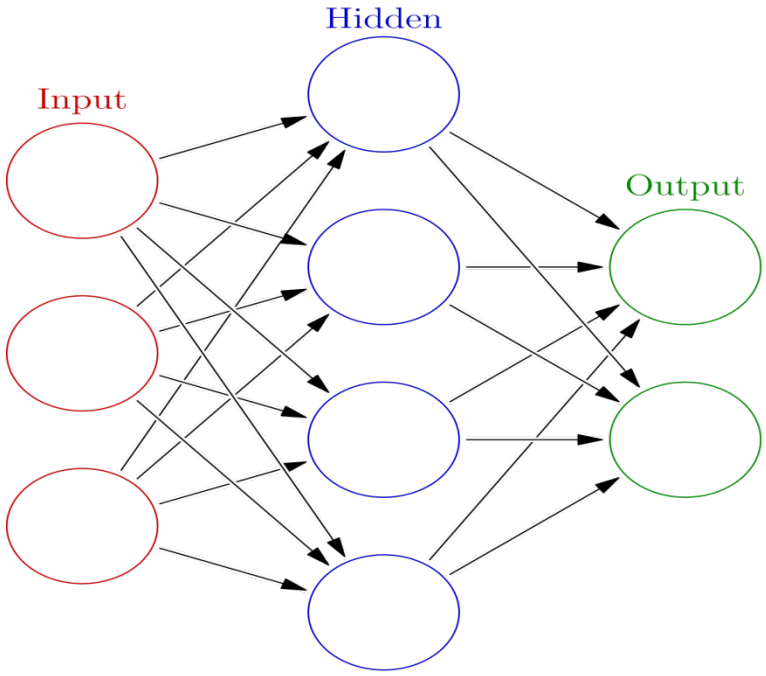

Рис. 2. Схематичное изображение нейронной сети, многослойный перцепторн

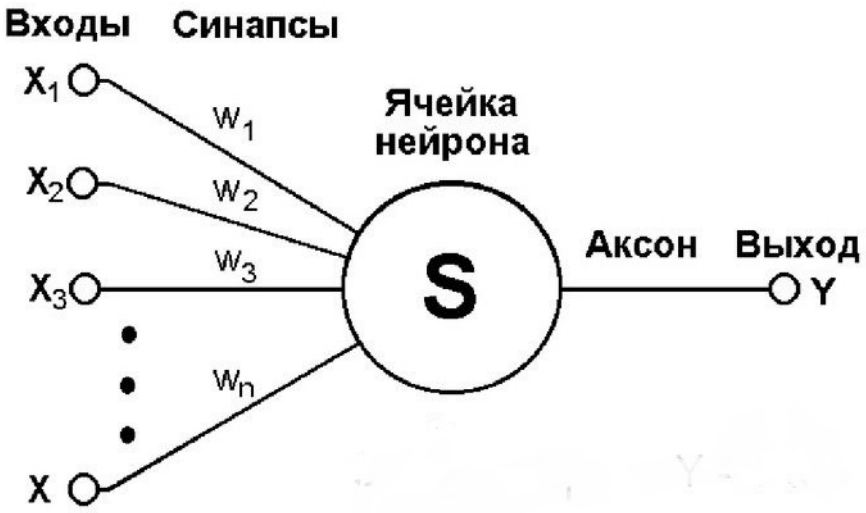

Рис. 3. Схематическое изображение искусственного нейрона, где x – вход нейрона, y – выход нейрона, w – весовой коэффициент нейрона, s – текущее состояние нейрона

Текущее состояние нейрона определяется по формуле:

$$s = \sum_{i=1}^{n} x_i \times w_i$$

где: *x* – вход нейрона; *y* – выход нейрона; *w* – весовой коэффициент; *s* – текущее состояние нейрона; *n* – сколько всего нейронов на входе; *i* – порядковый номер нейрона.

Выход нейрона, является функцией его состояния:

$$y = f(s),$$

где: y – выход нейрона; f – нелинейная функция (функция активации).

Каждый нейрон или узел в нейронной сети имеет функцию активации вывода, которая устанавливает выход на основе ввода. Существует множество различных функций активации, подходящих для разных задач, это Elu, Relu, Sigmoid Tanh и другие, но наиболее распространенной функцией активации является Relu.

Формула функции активации Relu:

$$y = \max(x; 0)$$

где: y – выходное значение; x – сумма входных значений [4].

Обучение сверточных нейронных сетей делится на контролируемое и неконтролируемое. При обучении с учителем модель должна находить закономерности с выходными данными в дополнение к входным данным, а при обучении без учителя, не имея выходных данных, за счет скрытых закономерностей определять эти выходные данные (в виде выделения областей, общих черт, отличительных особенностей). функции). Чаще всего используется принцип контролируемого обучения: на вход подаются изображения определенного класса, которые уже имеют выходное значение в виде наличия или отсутствия патологии [3. С. 25–28].

За выделение важных особенностей изображения отвечают два основных типа слоев:

1. Свертки – формирование из изображения совершенно новых изображений с выделением признаков путем расчета нового значения для данного пикселя с учетом значения соседних, окружающих его пикселей;

2. Unions – слой, уменьшающий размерность изображения за счет объединения пикселей.

Сами изображения подаются в виде тензоров (трехмерного объекта) и преимущественно два типа слоев сверточной нейронной сети, чередуясь друг с другом, формируют вектор признаков (с помощью выпрямляющего слоя) на вход многослойного перцептона, изменение параметров (значений) внутри тензора.

Полносвязный слой – это слой с нейронами, где каждый нейрон связан со всеми предыдущими и последующими нейронами. Количество нейронов в последнем слое отражает количество классов классификации (если нейронов 2, то классификация будет бинарной) [3. С. 15].

Сверточные нейронные сети также могут использовать другие слои с разными функциями.

Не менее важной составляющей работы модели является оптимизатор – это алгоритм изменения параметров обучения (весового коэффициента и коэффициента смещения) и скорости обучения с целью нахождения оптимальных значений, нахождения основных признаков и эффективной работы нейронных сетей.

Архитектура или, другими словами, структура нейронных сетей – это совокупность конкретных значений гиперпараметров сети.

Гиперпараметры сети – это переменные, связанные со структурой сети (например, количество слоев, расположение слоев в разном порядке, количество

нейронов и т. д.). Эти переменные настраиваются вручную перед обучением архитектуры [4].

Двумя ключевыми гиперпараметрами нейронной сети являются:

– размер маски свертки в сверточном слое по умолчанию 3x3, но если мы говорим о крупных объектах изображения, то размер может измениться на 5x5, 7x7 и более, но если мы говорим о небольшом размере объекта изучается, то эффективнее использовать 1x1;

– количество сверточных фильтров, отражающих увеличение глубины изображения, для выделения особенностей.

Результаты и обсуждение. За последние 5 лет было 29 790 случает регистрации больных с атопическим дерматитом. Из них в 2018 г. – 6 377 случаев, 2019 г. – 7 225, 2020 г. – 4 985, 2021 г. – 6 354, 2022 г. – 4 849 случаев. Что несомненно доказывает актуальность данной проблемы.

При опросе 142 пациентов. Из них мужчин – 98, женщин – 44 человек.

Из опрошенных обострения 3-4 раза в год у 33 % респондентов, 2 раза в год – 30 %, 1 раз в год – 19 % и чаще 4 раз в год – 18 %

По давности заболевания у 80 % респондентов атопический дерматит с детства, у 20 % с подросткового возраста.

Базовую терапию получают – 76 % респондентов, 24 % – не получают.

При обучении сверточных нейронных сетей используем разные архитектуры для повышения точности. В настоящее время общая точность получается 67,31 %.

Выводы. Учитывая высокую заболеваемость, и распространенность атопического дерматита, поражающего все слои населения, особенно детский возраст, данная проблема является актуальной. Также данная программа позволит улучшить контроль течения заболевания при дистанционном консультировании и оптимизировать прием как очный, так и дистанционный, что позволит больше уделять времени на осмотр и определение тактики ведения пациента, а не на заполнение документации.

Список литературы

1. Атопический дерматит: клинические рекомендации. URL: https://cr.minzdrav.gov.ru/schema/265_2

2. Выучейская М. В., Крайнова И. Н., Грибанов А. В. Нейросетевые технологии в диагностике заболеваний: обзор // Журнал медико-биологических исследований. 2018. Т. 6, № 3. С. 284–294.

3. Гафаров Ф. М., Галимянов А. Ф. Искусственные нейронные сети и приложения: учебное пособие. Казань: Издательство Казанского университетата, 2018. С. 5–35.

4. Нейронные сети. Основы. URL: https://digitrain.ru/articles/308510

5. Постановление Правительства Российской Федерации от 18.07.2023 № 1164 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по направлению медицинской деятельности, в том числе с применением телемедицинских технологий и технологий сбора

и обработки сведений о состоянии здоровья и диагнозах граждан». URL: http://publication.pravo.gov.ru

6. Скрипкин Ю. К., Мордовцева В. Н. Кожные и венерические болезни: рук. для врачей. Т. 2. М., 1999. С. 24–30.

7. Кванина В. В., Громова Е. А., Спиридонова А. В. К вопросу о системе принципов предпринимательского права // Бизнес, менеджмент и право. 2018. № 4. С. 18–21. EDN: XWHGMX.

8. Mayba J., Gooderham M. J. Review of atopic dermatitis and topical therapies // J Cutan Med Surg. 2017. Vol. 21, № 3. Pp. 227–236.

З. М. Бешукова,
доктор юридических наук, доцент,
Адыгейский государственный университет

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ: МЕХАНИЗМ СОВЕРШЕНИЯ И ОСНОВНЫЕ СПОСОБЫ ЗАЩИТЫ

Аннотация. В статье рассматриваются наиболее популярные и распространенные схемы мошенничества с использованием методов социальной инженерии. Определен механизм совершения данного вида преступлений, который включает четыре этапа: подготовка, проникновение, эксплуатация и отключение. Сформулированы рекомендации, которые могут быть использованы в целях повышения эффективности профилактики мошенничества с использованием методов социальной инженерии.

Ключевые слова: мошенничество, социальная инженерия, телефонное мошенничество, предупреждение, профилактика, фишинг, смишинг, вишинг, претекстирование

FRAUD USING SOCIAL ENGINEERING METHODS: MECHANISM OF COMMITMENT AND BASIC METHODS OF PROTECTION

Abstract. The article discusses the most popular and widespread fraud schemes using social engineering methods. The mechanism for committing this type of crime has been determined, which includes four stages: preparation, penetration, exploitation and shutdown. Recommendations are formulated that can be used to increase the effectiveness of fraud prevention using social engineering methods.

Keywords: fraud, social engineering, telephone fraud, warning, prevention, phishing, smishing, vishing, pretexting

Введение. В последние годы наблюдается значительный рост телефонного мошенничества, которое реализуется методами социальной инженерии.

В 2022 г. по официальной информации Центрального банка РФ российские граждане в результате телефонного мошенничества потеряли 14,2 млрд рублей [1].

При этом кредитными организациями жертвам данного вида преступлений было возвращено всего 4,4 % от похищенных средств, или 618,4 млн руб. Приведем аналогичные данные из обзора Центрального банка России об инцидентах информационной безопасности при переводе денежных средств за предыдущие годы. В 2021 г. жертвам было возмещено 6,8 % от похищенных средств, или 920,5 млн руб., в 2020 г. – 11,3 %, или 1,1 млрд руб., в 2019 г. – 15 %, или 935 млн руб. Как видим, самый низкий уровень возмещения денежных средств жертвам мошенничества приходится на 2022 г. Это является следствием высокой доли мошенничества, реализуемого методами социальной инженерии, т. е. когда граждане самостоятельно осуществляют переводы денежных средств преступникам или раскрывают конфиденциальную информацию [2].

В связи с этим особую актуальность приобретает анализ механизма совершения мошенничества с использованием методов социальной инженерии, а также проблема определения возможных способов защиты от него.

Основная часть. В настоящее время наиболее популярными и распространенными схемами мошенничества с использованием методов социальной инженерии являются:

1. Фишинг и смишинг. Суть фишинга заключается в использовании преступниками электронных писем и сообщений в социальных сетях с важной информацией. Смишинг предполагает использование текстовых сообщений (SMS-сообщений) в качестве механизма доставки для запуска эксплойта. Важно отметить, что текстовые сообщения имеют более высокий уровень открываемости, чем электронная почта, поэтому этот метод используется преступниками очень активно.

2. Вишинг ((от англ. «voice» и «phishing»), иными словами, голосовой фишинг) – это телефонный эквивалент фишинга. Вишинг представляет собой метод, произошедший от фрикинга, который был широко распространен в эпоху до появления сети «Интернет». Используя эту технику, преступники манипулируют жертвами в процессе телефонного разговора. При этом им порой удается усыпить бдительность даже самого внимательного человека.

Мошеннические схемы подвергаются регулярному обновлению. Например, после того как словосочетание «Здравствуйте, звонок из службы безопасности» фактически превратилось в мем (преступники часто представлялись сотрудниками банка), жертвы стали получать звонки от «представителей» других учреждений. Из последних трендов – звонки от имени федеральных министров. В контексте этого, важно отметить, что преступники практически всегда обладают так называемыми установочными данными, т. е. они владеют достоверной информацией о фамилии, имени, отчестве жертвы, месте ее работы, роде профессиональной деятельности, наличии ученой степени и др. Например, в 2023 г. жертвами мошенников стали преподаватели ВУЗов, которым преступники звонили в мессенджерах от имени ректоров, кураторов из Минобрнауки РФ и т. д.[3].

3. Использование претекста. Претекстирование включает в себя изощренную имитацию надежного источника или создание сфабрикованного сценария с единственной целью убедить жертву выполнить определенное действие. Преступники часто выбирают комбинацию цифр номера телефона, электронной почты, текстовых сообщений или социальных сетей, чтобы завоевать доверие жертвы.

Что же такое социальная инженерия? В первую очередь необходимо отметить, что целью настоящего исследования не является выработка определения данного термина. В связи с этим отметим только то, что в специальной литературе имеются различные определения понятия «социальная инженерия». В настоящем исследовании социальная инженерия понимается как манипулятивное воздействие на психику с целью совершения жертвами определенных действий или разглашения конфиденциальной информации, в том числе с использованием современных информационных технологий.

Мошенничество с использованием методов социальной инженерии происходит в основном в четыре этапа:

1. Подготовка. Преступник, как было отмечено ранее, всегда заблаговременно собирает информацию о жертве различными способами (через социальные сети; открытые данные, размещенные на сайтах различных организаций и учреждений; даркнет или другие источники).

2. Проникновение. Преступник «приближается» к жертве, обычно маскируясь под доверенные контакты или представителей органов власти, и использует при этом информацию, собранную о ней, чтобы завоевать доверие.

3. Эксплуатация. Преступник «убеждает» жертву предоставить ему конфиденциальную информацию, которую он использует для достижения своей преступной цели.

4. Отключение. Преступник прекращает общение с жертвой, осуществляет вредоносную деятельность и исчезает.

В связи с этим возникает вопрос, что необходимо сделать, чтобы люди не верили мошенникам? К основным способам защиты от мошенничества с использованием методов социальной инженерии относится предупредительная деятельность, которая должна включать в себя:

– повышение уровня осведомленности населения об особенностях мошеннических схем, о функционировании тех или иных финансовых механизмов, как и финансовой грамотности в целом [4. С. 357–361];

– специальное обучение вопросам информационной безопасности, позволяющее выработать у населения навыки безопасного поведения в различных ситуациях. Именно такая задача должна быть поставлена перед всеми субъектами профилактики правонарушений [4. С. 357–361];

– использование лицензионного антивирусного программного обеспечения и регулярное его обновление.

Заключение. Аккумулируя все ранее изложенное, можно сделать вывод, что эффективное противодействие мошенничеству с использованием методов социальной инженерии возможно только при использовании комплексного подхода. Причем ключевую роль в борьбе с мошенничеством играет именно критическое мышление потенциальной жертвы.

Список литературы

1. Бевза Д. В 2022 году телефонные мошенники похитили более 14 млрд рублей. URL: https://rg.ru/2023/03/03/v-2022-godu-telefonnye-moshenniki-pohitili-bolee-14-mlrd-rublej.html

2. Россияне сдали мошенникам рекордные 14 млрд. URL: https://www.rbc.ru/newspaper/2023/02/15/63eb5da89a794701b759621f

3. Медведева О., Тихонова Н. Телефонные мошенники переключились на медиков и преподавателей вузов. URL: https://rg.ru/2023/09/13/rektor-nikomu-ne-pishet.html

4. Трахов А. И., Бешукова З. М. Предупреждение телефонного мошенничества: российский и зарубежный опыт // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 6. Казань: Изд-во «Познание» Казанского инновационного университета, 2022. С. 357–361.

А. Л. Бурова,
помощник судьи,
Восемнадцатый арбитражный апелляционный суд

ПРАВОВОЙ СТАТУС ПРОЕКТА СУДЕБНОГО АКТА АРБИТРАЖНОГО СУДА, ПОДГОТОВЛЕННОГО ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

Аннотация. Цель работы состоит в исследовании актуальных проблем и перспектив правового статуса проекта судебного акта арбитражного суда, созданного искусственным интеллектом. Анализируется правовой статус проекта судебного акта арбитражного суда, подготовленного помощником судьи, представленного стороной арбитражного процесса, а также созданного искусственным интеллектом. В заключении приводится вывод о необходимости внесения изменений в Арбитражный процессуальный кодекс Российской Федерации и Инструкцию по делопроизводству в арбитражных судах Российской Федерации в целях закрепления правового статуса проекта судебного акта, разработанного искусственным интеллектом.

Ключевые слова: судья, арбитражный суд, арбитражное судопроизводство, электронное правосудие, искусственный интеллект, системы на основе искусственного интеллекта, проект судебного акта

LEGAL STATUS OF THE DRAFT JUDICIAL ACT OF THE ARBITRATION COURT PREPARED BY ARTIFICIAL INTELLIGENCE

Abstract. The purpose of the work is to study the current problems and prospects of the legal status of the draft judicial act of the arbitration court created by artificial intelligence. The legal status of the draft judicial act of the arbitration court, prepared by an assistant judge, submitted by a party to the arbitration process, as well as created by artificial intelligence, is analyzed. In conclusion, it is concluded that it is necessary to amend the Arbitration Procedural Code of the Russian Federation and the Instructions on Office Work in the arbitration courts of the Russian Federation in order to consolidate the legal status of the draft judicial act developed by artificial intelligence.

Keywords: Judge, Arbitration court, Arbitration proceedings, E-justice, Artificial intelligence, Systems based on artificial intelligence, Draft judicial act

Введение. Как известно, проект итогового судебного акта по существу спора, как правило, готовит помощник судьи по поручению самого судьи. Также в арбитражном процессе существует уникальная возможность для сторон, участников арбитражного спора, представить арбитражному суду свой проект решения.

Вместе с тем, по словам С. А. Курочкина, экономическое правосудие не может оставаться в стороне от научно-технического прогресса и развития современных технологий [1].

В свете современности, на наш взгляд, особого рассмотрения требует вопрос о месте искусственного интеллекта (далее – ИИ) в системе арбитражного судопроизводства, в частности внедрения его в процесс создания проекта судебного акта и его места в этом процессе.

В рамках данного исследования представляется уместным посмотреть на наличие актуальных проблем и перспектив правового статуса проекта судебного акта арбитражного суда, созданного ИИ, изучить вопрос соотношения правовых статусов проекта решения, подготовленного помощником судьи, представленного стороной по делу или созданного ИИ.

Для поставленной цели необходимо ответить на вопросы о том, должен ли иметь правовой статус проект судебного акта, автором которого является ИИ, имеет ли такой правовой статус место в арбитражном судопроизводстве и в какой мере требует правового регулирования, в какой именно форме, порождает ли или же снимает проблемы в практике?

Основная часть. В качестве изначального пункта следует напомнить, что в части 1 статьи 58 Арбитражного процессуального кодекса российской Федерации (далее – АПК РФ) закреплено, что помощник судьи оказывает помощь судье в подготовке и организации судебного процесса, а также в подготовке проектов судебных актов.

В этой же части АПК РФ законодатель подчеркнул, что помощник судьи не вправе выполнять функции по осуществлению правосудия.

Далее мы обращаемся к положениям Инструкции по делопроизводству в арбитражных судах [3]. Так, в соответствии с пунктом 9.2 Инструкции по делопроизводству в арбитражных судах ответственность за подготовку судебного акта несет судья, рассматривающий дело. При этом в приведенной Инструкции отмечено, что помощник судьи по распоряжению судьи готовит проект/проекты судебного акта.

Интересным является, что пункт 9.2 Инструкции по делопроизводству в арбитражных судах предусматривает, что проект/проекты судебных актов могут быть представлены лицами, участвующими в деле. Также отмечается, что указанные проекты могут быть поданы в суд с соответствующим ходатайством, в том числе и в электронном виде по системе электронной подачи документов, и приобщаются к материалам судебного дела.

В свою очередь, следует также отметить, что проекты судебного акта могут быть подготовлены на любой стадии рассмотрения дела, но немаловажным

в этом вопросе является то, что арбитражный суд вправе использовать указанные проекты как в целом, так и в части, но окончательный текст судебного акта формируется непосредственно арбитражным судьей после рассмотрения судом дела по существу.

В абзаце третьем пункта 9.3 Инструкции по делопроизводству в арбитражных судах Высший Арбитражный Суд Российской Федерации обусловил, что подписание судебного акта в системе автоматизации судопроизводства осуществляется исключительно судьей самостоятельно, упомянутый судебный орган также обратил внимание на то, что передача полномочий по подписанию судебных актов в системе автоматизации судопроизводства не допускается.

Относительно рассматриваемого вопроса также существует правовая позиция Конституционного Суда Российской Федерации, согласно которой проекты судебных актов, предоставляемые сторонами арбитражного процесса, не являются письменными доказательствами, иными документами и материалами, представление которых арбитражному суду указанными лицами подчиняется принципам равноправия и состязательности [2].

Соответственно, как точно и юридически тонко отметил Конституционный Суд Российской Федерации, данному праву не корреспондирует обязанность арбитражного суда по использованию представленных сторонами проектов полностью либо в части при изготовлении судебного акта. В любом случае Конституционный Суд Российской Федерации отметил и еще раз напомнил, что принимаемые арбитражным судом судебные акты должны быть законными, обоснованными и мотивированными (часть 4 статьи 15 АПК РФ) и соответствовать предъявляемым законом требованиям к их принятию, разрешаемым вопросам, изложению и содержанию (статьи 167 – 170 АПК РФ).

В то же время, по обоснованному мнению А. А. Смола, представление проектов судебных актов в арбитражный суд лицом, участвующим в деле, в качестве допустимого процессуального действия признано сравнительно недавно и не является универсальным [4].

Здесь уместно обратить внимание на то, что представление сторонами арбитражного процесса проектов судебных актов суду является исключительно их правом и собственным усмотрением, также как и является правом и усмотрением арбитражного суда принимать или не принимать проект судебного акта на любой стадии рассмотрения дела. При этом арбитражный суд, формируя после рассмотрения дела судом по существу окончательный текст судебного акта, вправе как использовать, так и не использовать полученные от сторон проекты судебных актов.

В свете сказанного, анализируя процессуальный аспект правового статуса судебного акта арбитражного суда, созданного ИИ, следует вывод о том, что такой проект судебного акта, наряду с проектами судебных актов, выполненных помощником судьи или представленных стороной, не будет служить письменным доказательством по делу, иным документом и материалом, который бы являлся обязательным для судьи арбитражного суда и безусловно обязывал бы его принимать позиции, выводы и решение, отраженные в таком проекте.

Предлагается, что в будущем для установления правовой определенности в статусе проекта судебного акта, выполненного посредством систем ИИ, следует внести соответствующие изменения в статью 58 АПК РФ, а также в пункт 9.2 Инструкции по делопроизводству в арбитражных судах, приравняв проекты судебных актов, созданные ИИ, по правовому статусу к проектам судебных актов, выполненных по поручению судьи помощником судьи, представленные сторонами арбитражного процесса.

Немаловажным является вопрос о том, как на практике судья должен относиться к возможностям ИИ при составлении судебного акта? Видится, что судья, получая проект решения, созданного ИИ, должен рассматривать такой способ разрешения спора исключительно с практической точки зрения, а именно относиться к ИИ как к инструментарию, или, сказав по-другому, цифровой технологии получения корректно обобщенной, грамотно консолидированной и структурированной информации с учетом особенностей конкретного дела в форме проекта или шаблона судебного акта.

Также представляется, что попытка придания проекту судебного акта, сгенерированного нейросетью, особого процессуального статуса в арбитражном судопроизводстве основано на неправильном понимании принципов получения правовой информации, необходимой для разрешения арбитражным судом спора.

Рассматривая технологии ИИ с точки зрения цифрового инструментария в арбитражном процессе, можно прийти к выводу, что, по существу, ИИ для арбитражного судьи является очередным прогрессивным способом быстрого получения и обработки информации, что в условиях современной реальности является крайне необходимым, который в равной степени соотносится с тем, как судья при составлении мотивированного судебного акта прибегает за помощью к сервисам электронного правосудия, таким как Картотека арбитражных дел, Банк решений арбитражных судов, или справочно-правовых систем, таким как Справочная правовая система «КонсультантПлюс» или Правовая система «Гарант» и др.

Заключение. По результатам исследования следует обоснованный вывод, что современные цифровые технологии в части применения арбитражными судами систем ИИ, несомненно, являются перспективным направлением в арбитражном судопроизводстве. Вместе с тем важным условием применения технологий ИИ при создании проекта судебного акта является необходимость внесения изменений в положения статьи 58 АПК РФ и Инструкцию по делопроизводству в арбитражных судах. В этом контексте представляется убедительным то, что приоритетным будет являться закрепление в регламентирующих арбитражный процесс документах статуса проекта решения, созданного ИИ, например, наряду с проектами судебных актов, выполненных помощником судьи или представленных стороной.

При этом важным и целесообразным было бы отметить, что проект судебного акта, сгенерированного ИИ, не может выступать письменным доказательством по делу или иным документом и материалом, который бы являлся обязательным для судьи и, безусловно, обязывал бы его принимать при вынесении итогового

судебного акта при вынесении решения, что и формирует правовой статус проекта судебного акта, созданного ИИ.

В итоге рассмотрения данного вопроса также можно сказать необходимости осознания того, что системы ИИ, которые будут использоваться в арбитражных судах, должны расцениваться в качестве правового и технического помощника-инструментария для арбитражного судьи в целях быстрого создания корректного, грамотного и индивидуально-детализированного проекта судебного акта, который в силу своего юридического статуса как может быть принят и использован или не принят и не использован судьей полностью или частично при составлении итогового мотивированного судебного акта по существу спора.

Список литературы

1. Курочкин С. А. Искусственный интеллект и экономическое правосудие // Экономическое правосудие. 2022. № 4 (64). С. 65–75.

2. Определение Конституционного Суда Российской Федерации от 26.02.2021 № 279-О «Об отказе в принятии к рассмотрению жалобы публичного акционерного общества «Нижнекамскнефтехим» на нарушение его конституционных прав частью 4 статьи 167 Арбитражного процессуального кодекса Российской Федерации и пунктом 1 статьи 10 Закона Российской Федерации «О статусе судей в Российской Федерации». URL: https://www.consultant.ru/document

3. Постановление Пленума Высшего Арбитражного Суда Российской Федерации от 25.12.2013 № 100 «Об утверждении Инструкции по делопроизводству в арбитражных судах Российской Федерации (первой, апелляционной и кассационной инстанций)». URL: https://www.consultant.ru/document

4. Смола А. А. Может ли быть процессуальным злоупотреблением представление в суд проекта судебного акта? // Закон. 2022. № 7. С. 52–70.

С. А. Бурьянов,
кандидат юридических наук, доцент,
Московский городской педагогический университет
М. С. Бурьянов,
магистр юриспруденции, эксперт
молодежная группа стран СНГ МСЭ ООН (ITU UN),
Молодежный совет при Уполномоченном по правам человека
в Российской Федерации

О НЕОБХОДИМОСТИ ПРАВОВОГО ЗАКРЕПЛЕНИЯ ЦИФРОВЫХ ПРАВ ЧЕЛОВЕКА В ГЛОБАЛЬНОМ ЦИФРОВОМ ДОГОВОРЕ ООН

Аннотация. В статье рассмотрены актуальные проблемы современных глобальных цифровых процессов и вызовов. Исследованы новые тенденции в сфере внедрения инновационных технологий, требующие поиска эффективного правового регулирования для их человекоориентированного внедрения в целях

достижения устойчивого развития. В указанном контексте обоснована необходимость закрепления цифровых прав человека в Глобальном цифровом договоре ООН в качестве важной основы для развития международного и внутригосударственного правового регулирования.

Ключевые слова: глобальные процессы, цифровые права человека, Глобальный цифровой договор ООН, устойчивое развитие

ON THE NEED TO LEGALIZE DIGITAL HUMAN RIGHTS IN THE UN GLOBAL DIGITAL COMPACT

Abstract. The article discusses current problems of modern global digital processes and challenges. New trends in the implementation of innovative technologies have been studied, requiring the search for effective legal regulation for their human-oriented implementation in order to achieve sustainable development. In this context, the need to consolidate digital human rights in the UN Global Digital Compact is substantiated as an important basis for the development of international and domestic legal regulation.

Keywords: global processes, digital human rights, UN Global Digital Compact, sustainable development.

Введение. Сегодня человеческая цивилизация развивается под существенным влиянием макромасштабных, многоплановых и внутренне противоречивых интеграционных глобальных процессов [11. С. 3–15], направленных на формирование единой общественно-техноприроднокосмической системы [3]. Современные глобальные процессы чуть более десяти лет развиваются под влиянием цифровизации, где ключевая роль принадлежит не только персональным компьютерам и сети Интернет, но также целому ряду инновационных технологий 4.0 (большие данные, блокчейн, искусственный интеллект, роботы и многие иные). Новые возможности несут разрабатываемые на принципах открытости и децентрализации интернет-технологии Web 3.0. Развитие следующего поколения Web 4.0 направлено на усиление интеграции виртуальных и реальных объектов, что создает еще более существенные возможности для развития экономики и образования. Осенью 2022 г. был запущен проект чат-бота от технологической компании OpenAI ChatGPT (Generative Pre-trained Transformer). Весной 2023 г. стала доступна новая версия GPT-4, способная взаимодействовать в режиме диалога с достаточно широким спектром возможностей от ответов на вопросы до написания кода. Технологические новинки наряду с интересом вывали крайне серьезные опасения по поводу безопасности. Фактически речь идет о новой эпохе цивилизационного развития, что «требует переосмысления многих правовых вопросов» [7. 10. С. 75–87]. В условиях усиления глобальных вызовов требуется поиск эффективного правового регулирования для человекоориентированного внедрения цифровых технологий в целях устойчивого развития.

Основная часть. О состоянии изученности проблематики прав человека в контексте глобальных процессов и вызовов свидетельствуют исследования Л. И. Глухаревой, В. А. Карташкина, Е. А. Лукашевой, И. И. Лукашука,

М. Н. Марченко, Т. П Минченко, Е. М. Павленко, Ф. М. Рудинского, А. Н., Чумакова, А. Д. Урсула и др. Однако права человека в условиях цифровой глобализации 4.0 исследованы недостаточно.

Противоречивая динамика в развитии глобальных процессов способствует не только усилению старых, но и появлению новых планетарных вызовов, связанных с внедрением инновационных технологий (цифровые милитаризация, контроль, неравенство, разжигание нетерпимости, а также недружественный искусственный интеллект и др.) [3, 4]. В контексте цифровой трансформации вызовами являются неосведомленность о цифровых технологиях и их потенциальных рисках, недоступность технологий, недостаточный уровень цифровой грамотности среди всех заинтересованных сторон.

Упомянутые выше противоречия в развитии глобальных цифровых процессов 4.0 требуют эффективного поиска путей правового урегулирования [9, 10]. Некоторые шаги в этом направлении были предприняты в рамках Организации Объединенных Наций (ООН) [14]. Однако приходится признать, что регулирование цифровой глобализации 4.0 в значительной мере отстает от потребностей общественного развития. Оно представлено в основном устаревшими и рекомендательными нормами в области устойчивого развития, информационного права и прав человека, а также этическими нормами [5, 6, 8].

В своем послании от 10 декабря 2022 г. по случаю Дня прав человека Генеральный секретарь ООН А. Гутерриш в очередной раз подтвердил приверженность правам человека в условиях глобальной цифровой трансформации, подчеркнув необходимость осознания угроз, исходящих от новых технологий [13].

В июле 2023 г. в своем выступлении на Глобальном саммите «ИИ во благо» Генеральный секретарь ООН Антониу Гутерриш заявил, что развитие искусственного интеллекта или ИИ «на благо всех» требует ограждений, основанных на правах человека, прозрачности и подотчетности. Он подчеркнул, что ИИ должен приносить пользу всем, включая треть человечества, которые все еще находятся в автономном режиме, и настаивал на необходимости срочно найти консенсус в отношении того, какими должны быть руководящие нормы для развертывания ИИ [15]. Генеральный секретарь Международного союза электросвязи (МСЭ) ООН Дорин Богдан-Мартин призвала к глобальному сотрудничеству, чтобы «обеспечить полное раскрытие потенциала ИИ при одновременном предотвращении и уменьшении вреда». Также глава МСЭ подчеркнула, что саммит по ИИ проходит в «исторический» момент, когда крайне важно продвигать управление ИИ и обеспечивать его инклюзивное, безопасное и ответственное развертывание. «Будущее ИИ еще не написано», – сказала она [15]. Ранее Верховный комиссар ООН по правам человека Фолькер Тюрк предупредил о быстром и неконтролируемом развитии генеративного ИИ. Он сказал, что «человеческая свобода действий, человеческое достоинство и все права человека находятся под серьезной угрозой», призвав правительства и бизнес привязать развитие технологий к соображениям прав человека [15].

18 июля 2023 г. Генеральный секретарь ООН А. Гутерриш обратился к Совету Безопасности ООН, подчеркнув потенциал искусственного интеллекта для ускорения человеческого развития, а также предостерег от злонамеренного

использования новой революционной технологии. Генеральный секретарь призвал Совет Безопасности ООН, который отвечает за международный мир и безопасность, «осуществлять лидерство в области ИИ» и указывать путь к общим мерам их прозрачности, подотчетности и надзора. «Мы должны работать вместе над созданием ИИ, который устраняет социальные, цифровые и экономические различия, а не разъединяет нас еще больше. «Я призываю вас объединить усилия и укрепить доверие во имя мира и безопасности», – заключил А. Гутерриш [16].

Разрабатываемый в настоящее время при участии всех заинтересованных сторон (от правительств и технологических компаний до научных кругов и частных лиц) Глобальный цифровой договор должен быть принят в сентябре 2024 г. в рамках Саммита будущего высокого уровня ООН на тему «Многосторонние решения для лучшего завтра», инициированного для разработки новой повестки по вопросам мира и глобальной безопасности. Полагаем, что перспективы урегулирования новых глобальных вызовов глобальной безопасности, связанных с внедрением цифровых технологий 4.0, следует формировать на основе концепции глобальных цифровых прав человека [1, 2, 12].

Ключевыми трендами развития человеческой цивилизации являются глобальные цифровые, макромасштабные, многоплановые и внутренне противоречивые интеграционные процессы. Глобальные процессы объективно направлены на формирование единой общественно-техноприроднокосмической системы, но их разбалансированность и неурегулированность предопределяет негативные последствия планетарного масштаба [3, 4]. Полагаем, что реализация цифровых прав человека будет способствовать их преодолению.

Заключение. В качестве вывода отметим необходимость закрепления цифровых прав человека в Глобальном цифровом договоре ООН, принятие которого планируется в сентябре 2024 г. в рамках Саммита будущего высокого уровня ООН «Многосторонние решения для лучшего завтра». В дальнейшем на этой основе можно будет развивать международное и внутригосударственное правовое регулирование для человекоориентированного внедрения цифровых технологий в целях устойчивого развития.

Список литературы

1. Бурьянов М. С. Цифровые права человека в условиях глобальных процессов: теория и практика реализации: монография; под науч. ред. С. А. Бурьянова. М. 2022. 148 с.

2. Бурьянов М. С. Цифровые права человека как ответ на угрозы глобализации 4.0 // Глобалистика-2020: Глобальные проблемы и будущее человечества. Сборник статей Международного научного конгресса. М., 2020. С. 395–398.

3. Бурьянов С. А. О необходимости глобального права в контексте проблемы целенаправленного формирования глобальной системы управления в целях устойчивого развития // Век глобализации. 2019. № 4. С. 129–142.

4. Бурьянов С. А., Кривенький А. И. О состоянии и перспективах формирования глобального образования, включая юридическое // Государство и право. 2019. № 8. С. 95–100.

5. Епифанов А. Е., Кдлян Е. Л. Теоретические аспекты воздействия законности на правовое поведение личности. Монография. М. 2015. 208 с.

6. Епифанов А. Е. К вопросу о влиянии международного права на формирование механизмов защиты прав и свобод человека (вопросы теории и истории) // Вестник Южно-Уральского государственного университета. Серия: Право. 2015. Т. 15, № 2. С. 14–20.

7. Комарова В. В. Правовой статус человека в цифровой среде: взгляд конституционалиста // Образование и право. 2022. № 2. С. 38–46.

8. Кроткова Н. В. «Круглый стол»: «Права человека и стратегия устойчивого развития» // Государство и право. 1998. № 11. С. 103–119.

9. Павленко Е. М. Влияние деформаций правового сознания на формирование правовой культуры и культуры прав человека // Российское государствоведение. 2016. № 2. С. 15–27.

10. Талапина Э. В., Жарова А. К. Иллария Лаврентьевна Бачило – основоположник информационного права в России // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 296–307. EDN: HIOEZH.

11. Чумаков А. Н. Основные тренды мирового развития: реалии и перспективы // Век глобализации. 2018. № 4 (28). С. 3–15.

12. Dowd R. The Birth of Digital Human Rights. Digitized Data Governance as a Human Rights Issue in the EU. Springer Nature Switzerland AG. 2022. 274 p.

13. Guterres: Put human rights at the heart of efforts to reverse today's damaging trends. URL: https://www.ungeneva.org/en/news-media/news/2022/12/guterres-put-human-rights-heart-efforts-reverse-todays-damaging-trends

14. United Nations Secretary-Generals Report «Our common agenda. URL: https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf

15. UN chief says regulation needed for AI to 'benefit everyone'. URL: https://www.ungeneva.org/en/news-media/news/2023/07/82683/un-chief-says-regulation-needed-ai-benefit-everyone

16. Guterres calls for AI 'that bridges divides', rather than pushing us apart. URL: https://www.ungeneva.org/en/news-media/news/2023/07/83086/guterres-calls-ai-bridges-divides-rather-pushing-us-apart

Г. Е. Волкова,
соискатель,
Южный федеральный университет

ПРАВО ЧЕЛОВЕКА НА БЕСЦИФРОВУЮ СРЕДУ

Аннотация. Совершенствование возможностей искусственного интеллекта, повсеместное развитие и проникновение цифровых технологий во все сферы жизни человека, формирование цифрового общества на первый план выдвигают вопрос о правах человека, их гарантиях и механизмах защиты. Цель статьи – выявление

некоторых негативных тенденций повсеместной цифровизации общественных отношений, в числе которых возможный регресс системы основных прав личности. В отсутствие правового регулирования, обеспечивающего баланс между публичными интересами в развитии информационно-коммуникационных технологий и неприкосновенностью частной жизни граждан, весьма важно обеспечить возможность реализации и защиты права человека на сохранение традиционного бесцифрового образа жизни.

Ключевые слова: цифровые технологии, цифровые права, цифровизация, право на неприкосновенность частной жизни, право на бесцифровую среду

THE HUMAN RIGHT TO A NON-DIGITAL ENVIRONMENT

Abstract. In connection with the development of digital technologies, the state is actively developing and stimulating a program of digitalization and technological modernization of the economy, public administration, and legal regulation. The purpose of the article is to identify some negative trends in the widespread digitalization of social relations, including a possible regression of the system of basic individual rights. In the absence of legal regulation that ensures a balance between public interests in the development of information and communication technologies and the privacy of citizens, it is very important to ensure the possibility of exercising the human right to preserve the traditional digital-free lifestyle.

Keywords: digital technologies, digital rights, digitalization, the right to privacy, the right to a digital-free environment

Стремительный рост и прогрессивное развитие цифровых технологий, повсеместная цифровая трансформация привычных «аналоговых» сфер общественных отношений с каждым днем все больше стирает разницу между реальным и виртуальным, правдой и вымыслом, истинным и ложным. Изучение зарождающейся в условиях информационного общества системы цифровых прав личности является одной из наиболее «модных» тем в российском, да и зарубежном правоведении последних лет. И, если ранее на процесс повсеместного внедрения цифровых технологий исследователи смотрели оптимистично, говоря об эволюции системы прав человека, ее развитии, то сегодня все чаще мы встречаем позицию, согласно которой процесс цифровизации «подвергает права человека беспрецедентным рискам» [3. С. 12] и даже ведет к «регрессу основных прав личности» [6], к «ущемлению прав человека» [8], ведет к «созданию тотального электронно-банковского концлагеря» [4. С. 90]. И, действительно, повсеместный сбор персональных данных, достижения систем искусственного интеллекта, постепенно приводит к тому, что благосостояние и человеческое развитие стали в значительной степени зависеть от услуг, предоставляемых в цифровой среде, существующее социальное неравенство усугубилось неравенством в области доступа населения к цифровым технологиям.

Пандемия ускорила рост возможностей информационных технологий, направленных на усовершенствование сферы осуществления удаленной работы,

дистанционных образовательных услуг, повседневных цифровых взаимодействий между людьми вплоть до удаленных медицинских консультаций. Такие быстрые изменения имели ряд последствий, к сожалению, не всегда положительных. В частности, выявили образовательные барьеры, проявляющиеся в лишении значительной части общества возможности получить доступ к образованию в условиях дистанционного обучения. Согласно данным отчета «Digital 2023 Russian Federation» (цифровые тенденции в России в 2023 г.) уровень обеспеченности доступа населения к возможностям сети Интернет в России на начало 2023 г. составлял 88,2 процента от общей численности населения [7]. Это означает, что процесс цифровизации всех сфер общественных отношений и связанные с ним цифровые риски (неравенство, тотальный контроль и другие) требуют адекватного правового регулирования, в отсутствие которого весьма важно обеспечить возможность реализации права человека на сохранение традиционного, «бесцифрового образа жизни» [4, 19].

В настоящее время одной из форм реализации права на бесцифровую среду является закрепленное в законодательстве Франции, Италии и Испании право дистанционных работников «быть не в сети» («Right to disconnect», позволяющее сотрудникам организаций отключаться от работы в обычное нерабочее время, чтобы им не приходилось отвечать на электронные письма, телефонные звонки или другие сообщения, связанные с работой. Однако, по нашему мнению, право человека на бесцифровую среду по содержанию намного шире, чем право «быть не в сети».

С одной стороны, право на бесцифровую среду можно рассматривать как средство защиты права на неприкосновенность частной жизни посредством осуществления самостоятельного контроля за сбором и распространением информации о себе и своей частной жизни и возможностью запрета осуществления таких действий. С другой стороны, это право можно рассматривать как средство сохранения императива человекоразмерности, защиту от необходимости осуществления гибридной формы существования, характеризующейся «сращением» человека и технологий, подменой в субъектном составе правооотношений реального человека «цифровой личностью», позволяя людям проживать свою жизнь без необходимости быть подключенными к цифровой среде, без ухудшения его положения по сравнению с другими потребителями коммерческих и государственных услуг.

Одним из составляющих права на бесцифровую среду является право «быть в одиночестве», или «право на уединение», которое предоставляет физическому лицу возможность совершать или не совершать действия, исходя из уверенности в том, что за ним никто не наблюдает и не подслушивает. Стремительное развитие технологий «умного дома», «умного города», методик распознавания лиц, анализа походки, использования цифровых помощников, датчиков отпечатков пальцев формирует вездесущую сеть наблюдения, постоянно собирающую всю информацию о каждой мельчайшей детали жизни людей. В таких условиях право быть уверенным в том, что за тобой не следят рискует превратиться в «обязанность постоянно быть под контролем». При этом сбор сведений о человека может осуществляться и пассивно, т. е. без его разрешения. Примеров пассивного сбора данных предостаточно. В настоящее время люди, имеющие мобильные телефоны,

постоянно предоставляют данные о геолокации с включенными настройками GPS или без них, при загрузке фото- и видеоизображений в социальные сети, сами того не желая, мы передаем огромный массив метаданных (данных о данных) и т. д. Как подчеркивает Арон Брантли, за 20 лет то, что когда-то было правом человека, «превратилось в привилегию, потому что для обеспечения права человека на неприкосновенность частной жизни необходимо исключить себя из современной социальной и экономической инфраструктуры» [6].

В основе права человека на бесцифровую среду лежит принцип свободной личности, предоставляющий человеку право на выбор среды взаимодействия (цифровой или в офлайн-формате) как друг с другом, так и с представителями услуг, в том числе и государственных. Принуждение свободного человека к использованию возможностей цифровой среды недопустимо. Человек, лишенный такого права выбора, рискует утратить себя как личность, превратиться в «существо, лишенное свободы избрания, свободы отпадения» [1. С. 37]. Право на доступ в интернет превращается в инструмент для изменения бытия человека, ведь с момента подключения его существование в аналоговой реальности тесно переплетается с существованием в «цифре». Цифровая организация деятельности систем государственного управления, основанная на расширенном и интегрированном внедрении информационных технологий при выполнении функций и предоставлении услуг, с одной стороны, упрощает доступ пользователя, а с другой, влечет за собой усугубляет уже существующее цифровое неравенство, увеличивает цифровой разрыв. Нельзя отрицать тот факт, что сегодня те, кто более полно использует возможности, предоставленные цифровыми технологиями, пользуются преимуществами по сравнению с теми, кто находится в более неблагоприятном цифровом положении, например, при записи на прием к врачу.

Необходимость сохранения традиционного «бесцифрового» образа жизни продиктована и тем обстоятельством, что, как и само равенство, цифровое равенство – это идеал, который никогда не будет достигнут. На наш взгляд, наиболее актуальной проблей, стоящей сегодня перед государством в процессе достижения цифрового равенства – это поиск баланса между развитием потенциала использования технологий искусственного интеллекта, и одновременным риском увеличения цифрового разрыва, цифрового неравенства в силу расслоения общества из-за отсутствия цифрового доступа к современным технологиям, в том числе в связи с принципиальным отказом потребителя от их использования в силу субъективных причин. Развитие информационных технологий влечет за собой два взаимозависимых процесса: одним из них является увеличение цифрового разрыва, а другим – постоянная борьба с цифровым неравенством в целях его преодоления.

Возможность выбора бесцифрового «старорежимного», традиционного образа жизни должна быть представлена в первую очередь экспертизой принимаемых законопроектов и подзаконных нормативный правовых актов на предмет оценки рисков причинения ущерба системе прав человека, обеспечения равного доступа к реализации естественных прав и свобод человека для всех категорий граждан, получения юридических гарантий того, что отказ субъекта от цифровой формы предоставления услуг не приведет к ухудшению его положения по сравнению с другими потребителями.

Одним из способов защиты прав на бесцифровую среду в цифровом пространстве (несмотря на отсутствие такого указания в законе) является право на забвение («right to be forgotten»), т. е. право требовать удаления информации о себе онлайн-платформ и поисковых систем, что позволяет человеку быть субъектом контроля над собственной личной информацией в цифровом пространстве. Данное право тесно взаимосвязано с цифровым правом человека «на исправление информации», которое, по сути, должно предоставлять лицу возможность требования исправления данных или информации, размещенной в сети, которые являются неточными или ошибочными. При необходимости изменения в личных данных также могут быть обновлены. Однако на сегодняшний день в правоприменительной практике Российской Федерации не сформирован единообразный подход к понимаю сущности права на забвение, что свидетельствует об объективной необходимости совершенствования нормативно-правового регулирования в данной сфере [2. С. 165–171]. Поиск баланса между неприкосновенностью частной жизни с общественными интересами и свободой доступа к информации – достаточно сложный вопрос, и дискуссии по нему будут определять наше цифровое будущее.

Самый ценный ресурс сегодняшнего дня – это уже не золото или нефть. Это информация, это данные. И чем больше данных о населении у субъекта, занимающегося обработкой этих данных, тем больше власти ему предоставлено. По сути, предоставляя данные для обработки, мы предоставляем возможность отслеживать и оценивать результаты повседневной деятельности человека в баллах, которые можно преобразовать в так называемый социальный рейтинг, обеспечивающий как доступ, так и отказ в доступе к различным как коммерческим, так и государственным услугам. Такой рейтинг, как широкомасштабная система оценки поведения граждан и организаций с целью установления системы доверия в обществе и повышения ответственности граждан, уже внедряется в Китае, который, по сути, стал испытательным полигоном внедрения технологий тотального цифрового контроля.

Таким образом, анализ того, как обеспечить право человека на бесцифровую среду в условиях совершенствования информационных технологий, является важнейшим первым шагом к защите прав человека. Особую актуальность заявленной теме придает тот факт, что сегодня права человека все чаще становятся цифровыми правами, а цифровые права приобретают статус нового поколения прав человека.

Список литературы

1. Бердяев Н. А. Философия свободы. М.: Юрайт, 2023. 201 с.

2. Волкова Г. Е. Судебная защита «права на забвение» в современной России: вопросы теории и практики // Вестник Юридического факультета Южного федерального университета. 2022. Т. 9. № 2. С. 165–171.

3. Государство и право в новой цифровой реальности: монография / под общ. ред. д-ра юрид. наук, проф. И. А. Умновой-Конюховой и д-ра техн. наук, проф. Д. А. Ловцова. М.: РАН. ИНИОН, 2020. 259 с.

4. Овчинников А. И. Безопасность личности и государства в цифровую эпоху: политико-правовой аспект // Журнал российского права. 2020. № 6. С. 5–21.

5. Правовая политика Российского государства в условиях цифровой экономики и цифрового технологического уклада / А. И. Овчинников, А. Ю. Мамычев, А. Г. Кравченко [и др.]. М.: Проспект, 2021. 184 с.

6. Brantly A., Utopia Lost – Human Rights in a Digital World // ACIG. 2022. Vol. 1, No. 1. Pp. 24-85.

7. Digital 2022: The Russian Federation. URL: https://datareportal.com/reports/digital-2022-russian-federation

8. O'Hara K. and Hall W., Four internets: Data, geopolitics, and the governance of cyberspace. URL: https://global.oup.com/academic/product/four-internets-9780197523681?lang=en&cc=ru

Е. В. Гаврилов,
советник юридического отдела,
Законодательное собрание Красноярского края

О ЮРИДИЧЕСКИХ ПРОБЛЕМАХ ПРИЗНАНИЯ КВАЛИФИКАЦИИ СПЕЦИАЛИСТА, НАПИСАВШЕГО ДИПЛОМНУЮ РАБОТУ С ПОМОЩЬЮ НЕЙРОСЕТИ

Аннотация. В статье на конкретном примере рассматриваются проблемы авторского права на произведения, созданные с помощью нейросетей, а также законодательства в сфере образования в ситуации, когда студент пишет выпускную квалификационную работу с помощью нейросетей. Цель исследования – привлечь внимание к указанным юридическим проблемам. Сделан вывод, что требуется совершенствование гражданского и образовательного законодательства.

Ключевые слова: авторское право, образование, квалификация, искусственный интеллект, нейросеть, студент, государственная итоговая аттестация, выпускная квалификационная работа

ON LEGAL PROBLEMS OF RECOGNITION OF THE QUALIFICATION OF A SPECIALIST WHO WROTE THE THESIS WITH THE HELP OF A NEURAL NETWORK

Abstract. The article, using a specific example, considers the problems of copyright for works created using neural networks, as well as legislation in the field of education in a situation where a student writes a final qualification work using neural networks. The purpose of the study is to draw attention to these legal problems. The author comes to the conclusion that the improvement of the Civil Code of the Russian Federation and the legislation on education is required.

Keywords: copyright, education, qualification, artificial intelligence, neural network, student, state final certification, final qualifying work

В 2022 г. в СМИ появилась информация, что студент ФГБОУ ВО «Российский государственный гуманитарный университет» (далее – РГГУ) А. Жадан за 23 часа написал дипломную работу с помощью нейросети ChatGPT. Выпускная квалификационная работа «Анализ и совершенствование управления игровой организацией» набрала 82 % оригинальности, студент защитил ее на «удовлетворительно» [2].

В этой связи перед обществом и правом встает вопрос о признании квалификации специалиста, написавшего дипломную работу с помощью нейросети.

По нашему мнению, здесь поднимаются проблемы авторского права на произведения, созданные с помощью нейросетей, а также законодательства в сфере образования.

Рассмотрим юридические проблемы на примере со студентом РГГУ А. Жаданом.

Для начала обратимся к законодательству об образовании.

Согласно пункту 5 статьи 2 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (далее – Федеральный закон № 273-ФЗ) квалификация – это уровень знаний, умений, навыков и компетенции, характеризующий подготовленность к выполнению определенного вида профессиональной деятельности.

В силу части 3 статьи 59, пункта 2 части 7, части 8 статьи 60 Федерального закона № 273-ФЗ для получения диплома, подтверждающего соответствующую квалификацию, студенту необходимо успешно пройти государственную итоговую аттестацию (далее – ГИА) в соответствии с порядком и в форме, которые установлены образовательной организацией, если иное не установлено Федеральным законом № 273-ФЗ.

Положение о проведении ГИА по образовательным программам высшего образования, в частности программам бакалавриата, в РГГУ утверждено приказом ректора от 28.09.2017 № 01-314/осн (далее – Положение) [5].

Защита выпускной квалификационной работы (далее – ВКР) наряду с государственным экзаменом – одна из форм ГИА (пункт 4.1 Положения). Согласно пункту 4.3 Положения ВКР представляет собой выполненную обучающимся (несколькими обучающимися совместно) работу, демонстрирующую уровень подготовленности выпускника к самостоятельной профессиональной деятельности. За все сведения, изложенные в ВКР, порядок их использования при составлении фактического материала и другой информации, обоснованность (достоверность) выводов и защищаемых положений профессиональную, нравственную и юридическую ответственность несет непосредственно автор ВКР, в соответствии с действующими в РФ и в РГГУ правовыми и/или локальными нормативными актами (пункт 4.3.4 Положения). Более того, ВКР проверяются на оригинальность и самостоятельность авторского текста (пункт 4.3.5 Положения).

Таким образом, для подтверждения квалификации, получения диплома студенту РГГУ необходимо среди прочего успешно защитить ВКР, которая должна быть оригинальной, выполненной студентом (автором) самостоятельно, соответствовать нормативным правовым актам и локальным актам РГГУ.

В российском законодательстве отсутствуют специальные нормы, регулирующие авторское право на произведения, созданные с помощью нейросетей.

Напомним, что авторские права – это интеллектуальные права на произведения науки, литературы и искусства (пункт 1 статьи 1255 ГК РФ). Автором таких произведений является гражданин, творческим трудом которого они созданы (статья 1257 ГК РФ). Иные, кроме физических лиц, субъекты права и тем более объекты права авторами произведений по смыслу части 4 ГК РФ не являются.

В самом общем виде под нейронной сетью (нейросетью) понимается обучаемая компьютерная программа, обрабатывающая большие объемы данных, работающая по принципу человеческого мозга. Другими словами, это наиболее продвинутый с учетом современных информационно-коммуникационных технологий способ реализации искусственного интеллекта (далее – ИИ).

При отсутствии специальных норм в ГК РФ и судебной практики по исследуемому вопросу в научной литературе имеется несколько подходов к авторскому праву на произведения, созданные с помощью ИИ, нейросетей: начиная от признания самого ИИ субъектом авторского права (автором); отнесения к авторам разработчика ИИ, нейросети [6. С. 26]; признания автором пользователя ИИ, дающему нейросети соответствующие задания, команды [8. P. 360]; заканчивая утверждением о том, что авторское право на произведения, созданные ИИ, не распространяется, так как отсутствует признак творчества [1. С. 18].

Кроме того, по исследуемому вопросу предлагаются и иные концепции (конструкция лицензионного соглашения, концепция служебного произведения, применение аналогии с нормами об авторском заказе, отнесение «творчества» нейросетей к смежным правам, например, к правам публикатора и др.) [4. С 35–36].

По нашему мнению, если человек подбирает правильный набор слов в качестве команд для нейросети, затрачивает немало времени, отбирая данные, обрабатывает полученный результат и тем самым вносит решающий вклад в оригинальность работы, вполне можно говорить о творческом характере создаваемого произведения и признании у пользователя авторского права не него. Из сети «Интернет» следует, что студент А. Жадан, используя нейросеть ChatGPT, проделал немало самостоятельной работы: отправлял грамотные запросы на разных языках, редактировал предлагаемый нейросетью текст, иногда собственноручно его переписывал, объединял выводы [3]. С учетом этого, полагаем, именно он внес решающий вклад в оригинальность ВКР, проявив творческие способности (соответственно является автором), а также успешно защитил ВКР. По сути, нейросеть в рассматриваемом примере можно сравнить с высокопрофессиональным фотоаппаратом: в любом случае автором фотографии с использованием такого устройства будет пользователь.

Возможно, в законодательстве об образовании, локальных актах РГГУ следовало бы конкретизировать положения о ВКР; определить, допускается ли использование нейросетей при подготовке ВКР, и если да, то в какой степени; какая роль при этом должна быть у самого студента. Безусловно, нуждается в корректировке и часть 4 ГК РФ в части уяснения вопроса о том, кому принадлежат авторские

права на произведения, созданные с помощью нейросетей, и допустимо ли вообще говорить об «авторском» праве на такие «произведения».

Дополнительно обращаем внимание, что в итоге диплом бакалавра студенту А. Жадану был выдан [7], а значит образовательная организация высшего образования признала у него наличие соответствующей квалификации. С учетом приведенной аргументации, полагаем, данное решение является правильным.

Список литературы

1. Витко В. Анализ научных представлений об авторе и правах на результаты деятельности искусственного интеллекта // ИС. Авторское право и смежные права. 2019. № 3. С. 5–22.

2. Искусственный интеллект не заменит работу человека. URL: https://www.kommersant.ru/doc/5798187

3. Как я написал диплом с помощью ChatGPT и оказался в центре спора о нейросетях в образовании. URL: https://journal.tinkoff.ru/neuro-diploma

4. Коданева С. И. Трансформация авторского права под влиянием развития цифровых технологий // Право и цифровая экономика. 2021. № 4. С. 31–38.

5. Положение о проведении государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры (новая редакция). URL: https://clck.ru/36oJJB

6. Синельникова В. Н., Ревинский О. В. Права на результаты искусственного интеллекта // Копирайт. 2017. № 4. С. 24–27.

7. Студенту РГГУ, который написал выпускную работу с нейросетью ChatGPT, вручили диплом. URL: https://msk1.ru/text/world/2023/03/15/72134255

8. Kasap A. Copyright and Creative Artificial Intelligence (AI) Systems: A Twenty-First Century Approach to Authorship of AIGenerated Works in the United States // Wake Forest Journal of Business & Intellectual Property Law. 2019. Vol. 19, № 4. Pp. 335–380.

Г. А. Грищенко,
кандидат юридических наук,
Московский государственный юридический
университет имени О. Е. Кутафина

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ДИПФЕЙКОВЫХ ТЕХНОЛОГИЙ

Аннотация. Целью статьи является проведение анализа законодательства, правоприменительной практики, научной литературы по вопросам использования дипфейковых технологий, и выработка рекомендаций по совершенствованию правового регулирования соответствующих отношений. В условиях цифровизации вопрос о правовых аспектах применения дипфейковых технологий напрямую

связан с институтом персональных данных, что требует выработки новых подходов к установлению допустимых пределов использования личной информации. В статье предпринята попытка обобщить подходы к регулированию дипфейков не только в России, но и в других странах, акцентируя внимание, что подобные технологии могут нести как отрицательный, так и положительный эффект. Делается вывод, что совершенствование законодательства в указанном направлении должно носить комплексный характер и включать как правовые, так организационные и технические меры, связанные, в частности, с необходимостью выработки понятийного аппарата, введения обязательной маркировки дипфейкового контента, разработки свода практик и этического кодекса по применению данных технологий.

Ключевые слова: дипфейковые технологии, дипфейк, персональные данные, дискредитация, честь, достоинство, мошенничество, социальные сети, этический кодекс, правовые проблемы, совершенствование законодательства

PROBLEMS OF LEGAL REGULATION OF DEEPFAKE TECHNOLOGIES

Abstract. The purpose of the article is to analyze legislation, law enforcement practice, scientific literature on the use of deepfake technologies, and develop recommendations for improving the legal regulation of relevant relations. In the context of digitalization, the issue of legal aspects of the use of deepfake technologies is directly related to the institution of personal data, which requires the development of new approaches to establishing acceptable limits for the use of personal information. In this article, the author has attempted to summarize approaches to regulating deepfakes not only in Russia, but also in other countries, emphasizing that such technologies can have both negative and positive effects. It is concluded that improving legislation in this direction should be comprehensive and include both legal, organizational and technical measures related, in particular, to the need to develop a conceptual framework, introduce mandatory labeling of deepfake content, develop a set of practices and a code of ethics for the use of data technologies.

Keywords: deepfake technologies, deepfake, personal data, discredit, honor, dignity, fraud, social networks, code of ethics, legal problems, improvement of legislation

Развитие цифровых технологий, в частности, искусственного интеллекта, нейротехнологий, больших данных, отражается на всех сферах общественной жизни. Возможности современных цифровых технологий используются в различных процессах принятия управленческих решений, оказания государственных (муниципальных) услуг, коммуникации в сети Интернет, что зачастую связано с обработкой персональных данных, например, для идентификации и поиска физических лиц, распознавания фото-, аудио- и видеоизображений и т. д.

Особо следует отметить достижения нейросетей, которые способны копировать тембр, мимику, черты лица человека и обучаться на оригинальных интервью, фильмах, клипах, создавая новый контент, где в фокусе внимания оказываются личные данные. Уже не требуется обладание какими-то специальными навыками, чтобы заменить лицо и (или) голос абсолютно любого человека на видео или

фото и отграничить достоверную информацию от фейковой порой сложно даже специалистам в этой сфере. Многие социальные сети и иные Интернет-ресурсы предоставляют возможность путем несложных манипуляций заменить изображение (или голос) человека на лицо любой знаменитости.

В последние несколько лет одну из актуальных тем для обсуждений представляет вопрос о правовых аспектах применения дипфейковых технологий и допустимых пределах использования персональных данных.

В настоящее время в российском законодательстве определение дипфейков отсутствует. Можно отметить единственный документ, упоминающий о дипфейках применительно к возможности использования таких технологий при совершении преступлений (Приказ Генпрокуратуры России от 9 декабря 2022 г. № 746 «О государственном едином статистическом учете данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре»). При этом ни признаки дипфейков, ни требования и условия их применения в данном документе не раскрываются.

Конечно, определенные аспекты, связанные с обработкой персональных данных, распространением фейковой информации, в том числе в сети Интернет, и способами восстановления нарушенных прав, в настоящее время регулируются Уголовным кодексом Российской Федерации, Гражданским кодексом Российской Федерации (далее – ГК РФ), Кодексом Российской Федерации об административных правонарушениях, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ «Об информации»), Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Законом Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» и др. При этом очевидно, что в существующих реалиях указанные документы не способны в текущей редакции охватить всевозможные аспекты применения именно дипфейковых технологий, а неоднозначная правоприменительная практика указывает на необходимость выработки новых механизмов по защите прав граждан в цифровой среде, особенно в части использования их персональных данных.

Осенью 2023 г. в Государственной Думе Федерального Собрания Российской Федерации планируется рассмотрение соответствующей законотворческой инициативы, связанной с введением в нормативные правовые акты положений, направленных на регулирование применения дипфейковых технологий.

Сразу хотелось бы отметить, что дипфейки могут применяться как в мошеннических целях (и именно на борьбу с мошенничеством направлена государственная политика по законодательному регулированию данного явления), так и вполне в законных и благоприятных, например, в сфере кинематографа, искусства, рекламы. Известны случаи «сдачи» своего лица в аренду для создания новых персонажей, озвученных искусственным интеллектом, которые используются в рекламных или образовательных целях; многие режиссеры рассматривают возможность применения дипфейков для создания цифровых образов актеров, что особенно актуально для воспроизводства исторических фильмов, «оживления» умерших людей (разнообразные онлайн-выставки и виртуальные концерты известных художников, музыкантов).

Но все же дипфейки как воплощение новых технологических возможностей несут в себе серьезные риски и спектр этих рисков весьма широк и продолжает увеличиваться. Дипфейки могут представлять опасность как для отдельного человека или группы людей, так и создавать более серьезные угрозы в информационном пространстве, затрагивая государственные интересы и создавая угрозы национальной безопасности [5. С. 54–64; 8].

Повсеместный сбор биометрических персональных данных создает дополнительные риски: фейковое изображение можно будет использовать вместе с фейковыми отпечатками пальцев или следами ДНК. Биометрические атаки с технологией дипфейк выходят на новый уровень и используют уязвимость, в частности, государственных информационных систем, когда программный лайвнесс (определение, что перед камерой находится живой человек) не срабатывает. Такая практика вынуждает предъявлять новые требования к системам безопасности, обрабатывающим биометрию.

Сгенерированные изображения на основе чужих персональных данных могут быть использованы в развлекательных и шуточных целях (разнообразные пранки и розыгрыши), но зачастую они применяются в рамках дискредитации известных личностей (политиков, актеров, медийных лиц). Помимо этого, новые возможности нейросетей позволяют сгенерировать портрет несуществующего человека (URL: https://thispersondoesnotexist.com/) или создать аватар по описанию (URL: https://images.ai/), что порождает новые правовые проблемы распознавания фальшивых изображений (создание изображений, схожих до степени смешения с реальными лицами) [8].

Условно угрозы, связанные с применением дипфейковых технологий, можно разделить на следующие группы:

1. Причинение вреда репутации лицам вследствие искажения персональных данных, включая изображение и голос человека (дискредитация личности);

2. Искажение фактов (фейковые новости);

3. Мошенничество (целевой фишинг) [8].

В большинстве стран мира не существует четкого правового регулирования дипфейков. Наиболее активно противодействуют распространению вредоносного ложного контента Индия, КНР, США, Сингапур, Великобритания, Южная Корея, Япония, Австрия и Евросоюз. При этом правовая регламентация может охватывать как общие вопросы распространения дипфейков независимо от сферы регулирования соответствующих отношений, так и специальные отраслевые направления (например, избирательную сферу) [8].

В Китае, например, приняли закон, запрещающий с 1 января 2020 г. публиковать фейковые новости и вводящие в заблуждение «дипфейковые» видео, созданные с помощью искусственного интеллекта [6]. Дипфейки должны быть соответствующим образом маркированы, но при этом не уточняется, каким образом будет осуществляться дифференциация дипфейков от реальной, соответствующей действительности информации. В отношении нарушителей предусматривается уголовная ответственность, которая может быть применена как к производителям дипфейков, так и к интернет-сервисам, где соответствующий контент будет размещен [8].

В конце 2022 г. Администрация киберпространства Китая (CAC) опубликовала правила распространения фейковой информации в Интернет-пространстве (вступили в силу 10 января 2023 г.):

– фейки можно публиковать только с согласия изображаемого на них лица;

– фейки не должны наносить вред национальной безопасности;

– фейки не должны использоваться для обмана или распространения клеветы.

В США (штат Калифорния) приняли закон, запрещающий разрабатывать и распространять дипфейковый контент в пределах 60 дней до выборов; во Франции введены санкции за монтаж речи или изображения человека без его согласия; в Великобритании законодательство в основном нацелено на защиту чести и достоинства человека за распространение дипфейк-контента [8].

В настоящее время наблюдается курс на внедрение национальных законодательных мер, нацеленных именно на возложение большей ответственности за создание и распространение ложного контента на онлайн-платформы [3. С. 38].

Многие социальные сети уже разрабатывают и применяют политику по защите пользователей от фальшивого контента, и планируется, что в ближайшее время они научатся распознавать лица, сгенерированные с помощью дипфейковых технологий. Представляется, что самоцензура социальных сетей также может принести определенный положительный эффект, но очевидно, что обеспечение подлинности контента в цифровом пространстве должно сопровождаться правовыми методами со стороны государства.

В литературе высказывается мнение о целесообразности разработки и принятия унифицированного этического кодекса по применению дипфейковых технологий в различных сферах деятельности [7].

Разработка подобного этического кодекса будет способствовать установлению правил использования дипфейков, что позволит минимизировать репутационные риски и просчитывать способы, с помощью которых такие технологии могут быть использованы злоумышленниками.

Многие этические вопросы, связанные с технологиями (например, использования образа умершего человека), еще только предстоит оценить в полной мере. Но важно, чтобы принимаемое законодательство, не создав препятствий для развития искусственного интеллекта в творческих индустриях, обеспечило защиту человека, чей образ теперь так легко повторить и использовать [4. С. 87–103].

Распространение дипфейков затрагивает напрямую институт персональных данных, поскольку при создании соответствующих видео- и аудироликов используются изображения людей и (или) голос, что может причинить вред репутации абсолютно любого человека [8].

Участилась практика дискредитации публичных личностей (особенно в период избирательных кампаний), многие случаи распространения в сети Интернет дипфейкового контента сопровождаются судебными разбирательствами.

Все это свидетельствует о необходимости не только правового реагирования на уже существующие общественные отношения, но и разработки соответствующих технических решений, которые позволили бы устанавливать факт использования дипфейковых технологий. Представляется, что это может быть автоматизированный

сервис, который с помощью искусственного интеллекта мог бы выявлять факты генерации дипфейков и соответствующие нарушения законодательства в изображениях и видеоматериалах (по аналогии с разработанной информационной системой «Окулус», с января 2023 г. поэтапно внедряемой в мониторинговые программы Роскомнадзора и выявляющей в сети Интернет запрещенный контент). По сути, речь идет о механизме фактчекинга, когда любой пользователь Интернета может проверить сомнительный контент на факт применения дипфейк-технологий [8].

Подобные сервисы разрабатываются и в зарубежных странах. Например, в США внедрена программа экспертизы содержания (семантического анализа) мультимедийных материалов SemaFor, которая способна также определять манипуляции с фото и видео, созданные человеком, которые могут казаться семантически согласованными, но передавать ложную информацию [8].

Как отмечалось выше, распознать фейк зачастую сложно даже специалистам, хотя в целом можно выделить определенные моменты, на которые стоит обратить внимание при критической оценке контента (разница в качестве отрисовки элементов лица и остальных частей тела, явные пиксели в изображении, частота моргания, плохая синхронизация движений и т. д.).

Несмотря на правовое регулирование отношений, связанных с распространением «фейков» в России (ФЗ «Об информации» (ст. 15.3), УК РФ (ст. 207.1 – 207.3), КоАП РФ (ч. 9, 10, 10.1, 10.2 ст. 13.15), своевременный и хорошо реализованный дипфейк может пошатнуть всю политическую систему страны (например, в случае публикации речи главы государства с призывом к насилию или началу военных действий) [8].

Отдельно стоит отметить случаи так называемого целевого фишинга, когда дипфейк направлен на обман сотрудников определенной компании, чтобы заставить их выполнить какую-нибудь операцию (рассылка сообщений с корпоративной почты, дача поручений голосом руководителя) [8]. Известны случаи, когда дипфейки используются для подачи заявок на удаленную работу от имени несуществующих людей и «исчезают», получив аванс, или пытаются завладеть коммерческой информацией о компании изнутри.

Одной из серьезных проблем, способных нанести угрозу правам человека, является способность дипфейк-технологий с невероятной точностью имитировать интонацию, характерные паузы между словами, акцент, корректировать эмоции при произношении слов (голосовые дипфейки). И здесь возникают сложности, связанные с возможностью распространения авторского права на голос. Представляется, что дипфейки сто́ит рассматривать через призму производного произведения, при котором использование исходного произведения без согласия его правообладателя будет незаконно [2. С. 116; 8].

Очевидно, что в дальнейшем дипфейки будут разрабатываться на более высоком уровне, учитывая быстрое и качественное развитие возможностей нейросетей, в связи с чем могут увеличиться случаи фальсификации и дискредитации, однако преимуществ у данной технологии намного больше [8].

Способы защиты прав субъектов персональных данных при использовании дипфейковых технологий сводятся ко всем возможным формам защиты прав, но преимущественно касаются вопросов защиты чести, достоинства и деловой

репутации, защиты от недостоверной информации, включая возможность возмещения морального вреда в рамках гражданского судопроизводства (ст. 152 ГК РФ). При этом нельзя забывать и о возможности привлечения виновных к административной (например, при рассмотрении дел об оскорблении по ст. 5.61 КоАП РФ) и даже уголовной ответственности (например, в рамках рассмотрения дел о клевете по ст. 128.1 УК РФ).

Что касается использования, например, образов актеров или иных известных лиц для создания пародийного контента (популярных в настоящее время пранков), то нужно понимать, что само по себе использование дипфейковых технологий действующее российское законодательство не нарушает. Вместе с тем копирование образов реально существующих людей для создания подобных видео незаконно. Обнародование и использование изображения гражданина допускается только с его согласия (ст. 152.1 ГК РФ). В противном случае актер может обратиться в суд с требованием изъятия и удаления сгенерированной информации, но при этом потребуется доказать сходство внешности истца с изображенным на видео лицом, что можно сделать с помощью соответствующей экспертизы.

В целях совершенствования правового регулирования дипфейковых технологий в России весьма целесообразным является проработка вопросов о необходимости:

– введения в законодательство определения дипфейков (представляется, что подобная категория может быть отражена в понятийном аппарате ФЗ «Об информации»);

– разработки новых механизмов защиты, например, высших должностных лиц государства (по аналогии с государственной символикой и государственным флагом России) [1];

– разработки унифицированного этического кодекса (правил) по применению дипфейковых технологий в различных сферах деятельности;

– классификации дипфейков по видам угроз и последствиям с целью выработки эффективных механизмов по защите прав субъектов персональных данных (представляется, что подобная классификация должна отражать методы создания дипфейков (синтез изображения и (или) голоса), субъектов их создания (политические оппоненты, средства массовой информации), их цели (полезные или преступные), наносимый ущерб (от психологического воздействия до угроз национальной безопасности);

– создания экспертной комиссии, в которую следует включить специалистов различных направлений (от технических до юридических), в компетенцию которой входило бы изучение зарубежного опыта правового регулирования дипфейк-технологий, ведение свода практик применения таких технологий, оценка рисков и внедрение успешного опыта в национальные нормативные правовые акты;

– обязательной маркировки контента, созданного с помощью дипфейковых технологий, и привлечения к ответственности в случае ее отсутствия;

– разработки и внедрения технических решений (программ/сервисов), способных выявлять контент, созданный на базе дипфейков;

– популяризации применения дипфейковых технологий в целях положительного воздействия на сферы развлечения, образования, искусства, рекламы;

– повышения цифровой грамотности населения и разработки алгоритма действий в случае выявления подозрительного (сомнительного) контента [8].

При этом совершенствование законодательства следует осуществлять не только в отношении дипфейков как таковых, а в отношении использования технологий искусственного интеллекта в целом. Принципы использования искусственного интеллекта, указанные в Стратегии развития искусственного интеллекта в Российской Федерации, утвержденной Указом Президента Российской Федерации от 10 октября 2019 г. № 490, во многом должны определять и принципы применения дипфейков.

Одним из основных принципов правового регулирования допустимости применения дипфейковых технологий должно стать обеспечение безопасности, основанной на недопустимости использования данных технологий в целях умышленного причинения вреда гражданам и юридическим лицам, а также предупреждение и минимизация рисков возникновения негативных последствий их использования, прежде всего, в сфере обеспечения защиты персональных данных. Представляется, что вышерассмотренные предложения могут быть учтены при внесении соответствующих изменений в российское законодательство, прежде всего, регулирующее информационные правоотношения и вопросы привлечения к уголовной и административной ответственности за правонарушения в цифровой среде [8].

Список литературы

1. Алискеров М. Р. Угрозы и риски применения технологии «Deepfake» в противоправных целях // Информационная безопасность. 2022 № 2(72). С. 38–41.

2. Добробаба М. Б. Дипфейки как угроза правам человека // Lex russica. – 2022. Т. 75, № 11. С. 112–119.

3. Игнатьев А. Г., Курбатова Т. А. Аналитический обзор «Дипфейки в цифровом пространстве: основные международные подходы к исследованию и регулированию». Москва, 2023.

4. Калятин В. О. Дипфейк как правовая проблема: новые угрозы или новые возможности? // Закон. 2022. № 7. С. 87–103.

5. Киселев А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник Московского государственного областного университета. Серия «Юриспруденция». 2021. № 3. С. 54–64.

6. Мун Д. В., Попета В. В. «From fake to deepfake»: угрозы и риски развития и распространения технологий искажения реальности в глобальном информационном пространстве. URL: https://cyberleninka.ru/article/n/from-fake-to-deepfake-ugrozy-i-riski-razvitiya-i-rasprostraneniya-tehnologiy-iskazheniya-realnosti-v-globalnom-informatsionnom

7. Bart van der Sloot, Yvette Wagensveld. Deepfakes: regulatory challenges for the synthetic society // Computer Law & Security Review. 2022. № 46. Art. 105716.

8. Грищенко Г. А. Обеспечение защиты персональных данных в условиях применения дипфейковых технологий // Устойчивое развитие России: правовое измерение: сборник докладов X Московского юридического форума. В 3-х частях. М., 2023. С. 197–202.

П. С. Гуляева,
младший научный сотрудник,
Казанский инновационный университет
имени В. Г. Тимирясова

ЦИФРОВИЗАЦИЯ НОРМОТВОРЧЕСТВА В УСЛОВИЯХ СМЕНЫ ТЕХНОЛОГИЧЕСКОГО УКЛАДА

Аннотация. В рамках исследования рассмотрены теоретико-правовые аспекты применения генеративных языковых моделей в нормотворчестве. В частности, проведен эксперимент по разработке нормативных актов посредством популярных нейронных сетей ChatGPT и YandexLM, а именно: правила поведения на объектах метрополитена, проект акта об административном правонарушении и должностная инструкция младшего научного сотрудника. По итогам эксперимента был сформирован перечень проблем, возникающих при интеграции самообучающихся алгоритмов в нормотворческую деятельность.

Ключевые слова: нормотворчество, цифровизация, нейросеть, генеративная модель, YandexLM, ChatGPT, LLM, большие языковые модели

DIGITIZATION OF RULE-MAKING IN CONDITIONS OF CHANGE OF TECHNOLOGICAL STRUCTURE

Abstract. The study examines the theoretical and legal aspects of the use of generative language models in rule-making. In particular, an experiment was conducted to develop regulations using the popular neural networks ChatGPT and YandexLM, namely: rules of conduct at metro facilities, a draft act on an administrative offense and a job description for a junior researcher. Based on the results of the experiment, a list of problems that arise when integrating self-learning algorithms into rule-making activities was compiled.

Keywords: rule-making, digitalization, neural network, generative model, YandexLM, ChatGPT, LLM, Large Language Models

Изобретение колеса, парового двигателя, использование нефти как источника энергии повлекло не только смену экономической модели, но и серьезные социальные изменения. Технологическая трансформация XXI в. фундаментально отличается от предыдущих: инструментом и продуктом в новых условиях стала информация.

До 2020 г. технологии искусственного интеллекта и машинного обучения продемонстрировали разнообразный функционал с высокой степенью автоматизации, например, робот-поэт, робот-изобретатель, робот-судья. В правовой сфере можно отметить как зарубежные, так и отечественные проекты в рамках legaltech-тренда: Dashboard legal, Immediation, Jus Mundi, Botman.one и другие. Экспертные системы, чат-боты и конструкторы документов полностью или частично продублировали компетенции низкоквалифицированных юристов. При этом в правовой теории активизировалась дискуссия о базовых концептах, например, о гипотетической правосубъектности искусственного интеллекта и робототехники.

С 2021 г. генеративные языковые модели продемонстрировали принципиально новые подходы к цифровизации деятельности и работе с информацией. Генеративные нейронные сети можно классифицировать по типам следующим образом:

1) нейросети, формирующие по запросу оператора аудиовизуальный контент и способные генерировать и редактировать фото-, видеоматериалы (например, Midjourney, Kandinsky 2.0, Stable Diffusion);

2) нейросети, которые анализируют метаданные и данные, содержащие информационные следы пользователей (например, подбор целевой аудитории в рамках процесса подготовки рекламной компании в социальных сетях);

3) нейронные сети, применяемые в медицине, способны распознавать данные и обучаться на датасетах, собранных в разных городах страны, чтобы спрогнозировать состояние пациента более точно.

Популярность генеративных нейронных сетей обусловлена появлением, так называемых, Больших Языковых Моделей (Large Language Models – LLM), например, ChatGPT. Аналогичные сервисы разработаны компаниями Google, Apple, Yandex. Нейросети обучены подбирать информацию, тексты, формировать ответы на запросы оператора и участвовать в беседе в формате чата.

Генеративные нейронные сети обучены на огромных объемах данных, а LLM содержат, как правило, от 100 до 200 миллиардов параметров.

В процессе подготовки диссертационного исследования автора статьи был проведен эксперимент, в рамках которого была протестирована возможность применения сервисов ChatGPT и Yandex LM для автоматизации процесса нормотворческой деятельности. Были подготовлены несколько документов, а именно:

– правила поведения на объектах метрополитена;

– должностная инструкция младшего научного сотрудника;

– проект постановления об административном правонарушении.

Отечественный сервис Yandex LM уступает зарубежному ChatGPT по количеству параметров (100 миллиардов и 175 миллиардов соответственно). При этом нейросеть подходит для подготовки фрагментов текстов и характеризуется следующими параметрами:

– ограниченный объем итогового текста, который подходит для работы с короткими заметками либо при подготовке текста по частям;

– отсутствие понимания системой связи между запросами, а следовательно невозможность уточнить задачу после обращения;

– осмысленность результата приемлемая, но не превосходная;

– не подходит для работы в рамках высокой степени автоматизации;

– требуется не просто контроль результата, но и постоянное участие оператора.

В настоящее время специалисты Яндекс разрабатывают новую версию системы, которая обладает более совершенными техническими характеристиками.

Популярная зарубежная нейронная сеть продемонстрировала хорошие результаты, в частности:

– взаимосвязь запросов между собой;

– возможность уточнить параметры задачи как до запуска генерации, так и после него, возможность «подсказывать» системе и обращать внимание на логику посредством таких обращений, как «думай последовательно» и подобных;

– сравнительно больший объем выдачи;

– понимание контекста достаточное для подготовки типовых документов на высоком уровне;

– качество работы приемлемое для тестирования высокоавтоматизированных сервисов, включая машиноисполняемые опции;

– к недостаткам нейросети можно отнести спонтанный переход с русского языка на иностранный.

Важно отметить, что указанные сервисы не обучены специально для выполнения правовых задач, но возможно подготовить нейронную сеть, адаптированную к работе с юридическими текстами.

В итоге к основным характеристикам генеративных языковых моделей можно отнести следующие признаки:

1) количество символов в итоговой выдаче ограничено возможностями конкретной генеративной языковой модели;

2) нейронная сеть функционирует на базе принципов и целей, заложенных разработчиками;

3) процесс принятия решения сервисом не прозрачен и неподконтролен – данный феномен называется проблемой «черного ящика»;

4) различаются системы с открытым и закрытым датасетом – в первом случае сервис учится на запросах пользователей по всему миру, во втором случае может учиться на обращениях только в рамках одной сессии, после завершения которой все удаляется;

5) генеративная модель не занимается поиском информации о конкретных людях, кроме сведений об общеизвестных личностях, которые были специально внесены в базу данных, например, ученый Стивен Хоакинг;

6) уровень оригинальности текстов неодинаков;

7) в практике применения нейросетей в юриспруденции существуют кейсы, когда система «придумала» факты, например, по запросу судебного юриста сделала подборку выдуманных прецедентов, представив их как реальные – в итоге юрист был лишен права практиковать;

8) в зависимости от качества обучения нейронная сеть способна генерировать полноценные тексты, однако контроль человека, по мнению автора статьи, не только необходим, но и обязателен на современном этапе.

В процессе подготовки эксперимента были выявлены не только прикладные, но и фундаментальные противоречия:

1) понятийно-категориальный аспект связан с отсутствием терминологического аппарата, необходимого для разработки правового механизма и методологии применения нейросетей в нормотворческой деятельности;

2) проблема субъекта подразумевает сложности с формированием правового статуса нейросети и результатов ее деятельности, особенно в условиях высокой степени автоматизации нормотворчества на базе LLM;

3) деликтная проблема связана с предыдущей и характеризуется противоречиями при распределении ответственности за неблагоприятные последствия.

Помимо перечисленных противоречий можно отметить риски в сфере безопасности, а также этические, коммуникативные и методологические.

На основании вышеизложенного можно заключить, что в условиях развития цифровизации и, в частности, технологий машиночитаемого и машиноисполняемого права, эксперимент по интеграции инструментария больших языковых моделей в нормотворческую практику можно считать не только возможным, но и желательным. Применение генеративных нейронных сетей представляется верным в условиях цифровой трансформации и технологизации публичного и корпоративного управления. Самообучающиеся алгоритмы безусловно открывают новые горизонты в сфере цифровизации права, при этом провоцируют серьезные риски для правовой теории и практики.

Смена технологического уклада является объективным процессом и оказывает непосредственное влияние на правовую реальность, а также на индивида, общество в целом и государство. Разработка механизма применения самообучающихся алгоритмов в нормотворческой практике является в таком контексте естественным продолжением развития права в новых условиях цифровой трансформации всех сфер жизни. По мнению автора, игнорирование данных технологий и отказ от их применения в правовой сфере противоречит глобальным трендам и ведет к существенному отставанию в развитии цифровой экономики и социальных институтов.

Список литературы

1. Гуляева П. С. Медицинские нанороботы в фокусе права // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 89–122. EDN: WNRAOE.

2. Пашенцев Д. А., Залоило М. В., Дорская А. А. Смена технологических укладов и правовое развитие России. Москва: ИЗиСП: Норма: ИНФРА-М, 2021. 224 с.

3. Пономарева Е. В. Феномен квазисубъекта права: вопросы теории: монография / под редакцией С. И. Архипова. М.: Юрлитинформ, 2020. 154 с.

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

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

6. Alice Witt, Anna Huggins, Guido Governatori, and Joshua Buckley. Converting Copyright Legislation into Machine-Executable Code: Interpretation, Coding Validation and Legal Alignment. Proceedings of the 18 International Conference on Artificial Intelligence and Law. June 21–25, 2021. São Paulo, Brazil. Pp. 139–148.

7. Naman Jain, Arun Iyer, Suresh Parthasarathy, Sriram Rajamani, Rahul Sharma. Jigsaw: Large Language Models meet Program Synthesis. Proceedings of the 44th International Conference on Software Engineering, 2022. Pp. 1219–1231.

А. С. Даниелян,
кандидат юридических наук,
Центр правовой поддержки “Веритас»

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СУДЕ: ПОМОЩНИК ИЛИ СУДЬЯ?

Аннотация. В исследовании рассматривается использование искусственного интеллекта в отечественном судопроизводстве. Отмечается, что технологии искусственного интеллекта могут ускорить принятие решений, повысить точность и объективность, а также улучшить доступность правосудия. Однако также отмечается, что есть некоторые потенциальные риски, такие как нарушение конфиденциальности данных и возможность ошибок в алгоритмах. Итоговый вывод исследования заключается в том, что использование информационных технологий и системы искусственного интеллекта необходимо рассматривать не в качестве самоцели, а как одно из первостепенных задач в срезе стратегии совершенствования правовой системы и повышения эффективности защиты и восстановления прав участников правоотношений с учетом социальных и этических аспектов судопроизводства.

Ключевые слова: искусственный интеллект, судопроизводство, правосудие, судебная система, правовая аналитика, электронное правосудие, цифровизация, машинное обучение, цифровые технологии

ARTIFICIAL INTELLIGENCE IN COURT: ASSISTANT OR JUDGE?

Abstract. The study examines the use of artificial intelligence in domestic civil proceedings. It is noted that artificial intelligence technologies can speed up decision-making, increase accuracy and objectivity, and improve access to justice. However, it also notes that there are some potential risks, such as data privacy violations and the possibility of algorithmic errors. The final conclusion of the study is that the use of information technology and artificial intelligence systems should not be considered an end in itself but should be introduced as part of a strategy to improve the legal system and increase the effectiveness of the protection and restoration of the rights of subjects of legal relations, taking into account the social and ethical aspects of legal proceedings.

Keywords: artificial intelligence, legal proceedings, justice, judicial system, legal analytics, e-justice, digitalization, machine learning, digital technologies

В последнее время решения на основе искусственного интеллекта (далее – ИИ) все чаще используются в различных сферах деятельности, включая судопроизводство. Эти системы могут применяться для протоколирования хода судебных разбирательств, систематизации процессуальных документов и даже для категоризации подсудимых [9].

Основными причинами внедрения систем ИИ в судопроизводство являются:

– сокращение расходов и времени на судопроизводство;

– устранение субъективных факторов при принятии судебных решений;

– содействие в более эффективной реализации принципов судопроизводства.

Однако использование систем ИИ в судопроизводстве сопряжено с определенными рисками, в том числе:

1. Формирование эффекта объективности. Люди склонны считать решения, принятые автоматизированной системой, более объективными, чем решения, принятые человеком. Это может привести к тому, что решения системы будут подвергаться меньшему сомнению и критике.

2. Стереотипизация. Системы ИИ могут усиливать стереотипы, присутствующие в данных, на которых они обучаются. Это может привести к тому, что решения системы будут дискриминационными в отношении определенных групп людей.

В некоторых отраслях, включая судопроизводство, компьютерные системы и системы ИИ могут заменять людей на рабочих местах, например, для систематизации информации по делу в заданных критериях и внесения предложений или советов на основе имеющихся данных. При этом для адекватного применения систем с поддержкой ИИ судьям необходимо понимать, как они работают [18].

Вдобавок, существует точка зрения, что ни одна автоматизированная система не может функционировать без человеческого сопровождения [11]. Считаем, что в настоящий момент компьютерные системы и системы ИИ преимущественно дополняют людей на рабочих местах, упрощая выполнение отдельных операций и сокращая время на выполнение других. Это вариант этичного применения ИИ на рабочем месте, который следует поощрять.

В качестве примера применения ИИ можно привести сервис Google Scholar, в котором встроенный ИИ помогает быстро находить и систематизировать материалы. Это существенно упрощает работу исследователей и уменьшает уровень их нагрузки [13].

Вот несколько возможных способов использования системы ИИ в правовой сфере:

1. Организация информации о судебных делах. Система ИИ может использоваться для распознавания шаблонов в текстовых документах и файлах при сортировке большого количества дел или в сложных делах, содержащих большой объем информации. Это может ускорить поиск и анализ информации, необходимой для принятия решений.

2. Консультативный ИИ. Система ИИ может анализировать информацию и предоставлять рекомендации в режиме «вопрос-ответ». Это может быть полезно судьям и участникам судебного процесса для принятия решений.

3. Юридическая аналитика. Система ИИ может предоставлять данные из судебной практики, которые юристы могут использовать при подготовке к текущим судебным процессам. Это может повысить эффективность и точность юридических исследований.

4. Автоматизация документооборота. Система ИИ может использоваться для автоматического составления и подачи юридических документов. Это может сэкономить время и усилия юристов.

5. Интеллектуальная собственность. Система ИИ может использоваться для поиска и регистрации товарных знаков, патентов, авторских прав и других объектов интеллектуальной собственности. Это может упростить и ускорить процесс регистрации интеллектуальной собственности.

ИИ все чаще используется в судопроизводстве во всем мире [1, 2, 7, 14]. В Китае, например, с 2014 г. разрабатывается система умного суда, которая к 2025 г. должна охватить все суды страны. Главные цели этой системы – ускорить рассмотрение дел, повысить доверие к судам и сделать процессы более удобными [3].

В Индии в марте 2023 г. суд одного из штатов использовал чат-бот с ИИ при принятии решения по делу об освобождении под залог [17].

В России полномасштабное применение ИИ планируется посредством введения суперсервиса «Правосудие онлайн». Основная задача ИИ в этом сервисе будет заключаться в автоматизированном составлении проектов судебных актов, расшифровке аудиопротоколов и создании интеллектуальной поисковой системы [5].

Использование ИИ в организационной деятельности суда позволяет уменьшить рутинную работу судей и работников аппарата суда. Уже сейчас с помощью ИИ можно автоматизировать ввод и обработку информации при осуществлении делопроизводства, рассмотрение поступающих в суд процессуальных документов, идентификацию личности и полномочий для участия в судебном разбирательстве.

В Колумбии судья использовал нейросеть ChatGPT для консультации перед вынесением приговора. Решение суда совпало с ответом чат-бота, но окончательное решение принял судья самостоятельно. Отметим, что в 2022 г. в Колумбии приняли закон, который обязывает государственных юристов использовать современные технологии для более эффективной работы [10].

Применение технологии слабого искусственного интеллекта в организационной деятельности суда позволит уменьшить рутинную работу судей и работников аппарата суда. Уже сейчас с помощью данной технологии можно решать задачи по автоматизированному вводу и обработке информации при осуществлении делопроизводства, рассмотрению поступающих в суд процессуальных документов с целью выявления их несоответствия требованиям процессуального законодательства, идентификации личности и полномочий для участия в судебном разбирательстве [4].

ИИ может быть использован для рассмотрения гражданских и административных дел по бесспорным требованиям, т. е. там, где принятие решения не связано с анализом правоотношений сторон и в большей степени имеет технический характер. Например, ИИ может быть использован для расчета размера алиментов, компенсации морального вреда или штрафа.

Правоведы отмечают, что для эффективного использования ИИ в судопроизводстве необходимо провести дополнительную работу как в доктринальной, так и в технической областях. Необходимо найти способы имитации юридического мышления с помощью ИИ, а также адаптировать математические расчеты к правовой сфере [16, p. 313].

Бразильскими учеными было проведено исследование, посвященное трудностям обеспечения справедливости и отсутствия предубеждений при принятии решений моделями ИИ. В исследовании были использованы различные методы, техники и инструменты для обнаружения и устранения алгоритмической несправедливости и предубеждений.

Авторы исследования рассмотрели три основных формы предвзятостей:

1. Предвзятость данных: Предвзятость в обучающих данных может привести к тому, что модель будет выдавать несправедливые или предвзятые решения.

2. Предвзятость алгоритмов: Предвзятость в алгоритмах может привести к тому, что модель будет выдавать несправедливые или предвзятые решения, даже если обучающие данные не являются предвзятыми.

3. Предвзятость пользователей: Предвзятость пользователей может привести к тому, что люди будут злоупотреблять моделями ИИ или использовать их для принятия несправедливых или предвзятых решений.

Для устранения предвзятостей в моделях ИИ авторы исследования предлагают использовать следующие подходы:

1. Предобработка данных: Предобработка данных может помочь устранить предвзятость в обучающих данных, например, путем удаления чувствительных атрибутов.

2. Внутренняя обработка: Внутренняя обработка может помочь устранить предвзятость в алгоритмах, например, путем использования алгоритмов машинного обучения, устойчивых к предвзятости.

3. Постобработка: Постобработка может помочь устранить предвзятость в решениях модели, например, путем корректировки результатов модели с учетом известных предубеждений.

Авторы исследования отмечают, что текущие исследования в области устранения предвзятости в моделях ИИ имеют ряд ограничений. Во-первых, многие исследования сосредоточены на одноклассовых задачах, тогда как в реальном мире часто требуется решать многоклассовые задачи. Во-вторых, результаты различных метрик справедливости могут быть неоднородными для одного и того же случая. В-третьих, необходимо проводить более широкие исследования с использованием различных архитектур моделей и различных метрик, чтобы стандартизировать подходы и определить, какие метрики являются более подходящими в конкретных контекстах.

В заключение авторы исследования отмечают, что внедрение решений на основе ИИ в судопроизводство может существенно сэкономить время и средства на рассмотрение и разрешение дела. Однако внедрение таких решений несет с собой существенные риски, связанные с предвзятостью моделей ИИ.

Люди склонны доверять решениям ИИ, даже если они ошибочны. Это связано с тем, что люди часто не понимают, как работают алгоритмы ИИ и как они могут быть предвзятыми [9]. Однако алгоритмы ИИ часто отражают предубеждения, которые присутствуют в обучающих данных. Это может привести к тому, что ИИ принимает несправедливые решения, например, на основании расовой или этнической принадлежности. Это особенно опасно в сфере правосудия, где ошибки могут иметь серьезные последствия.

Типичную модель машинного обучения можно образно представить в виде «плохого отличника» – заучивает то, что ей демонстрируют в источнике информации (обучающие данные) и при этом ничего не понимает.

Алгоритмы машинного обучения часто отражают существующие предубеждения в обществе. Это может привести к тому, что они принимают несправедливые решения, например, на основании расы или этнической принадлежности. В качестве примера можно привести алгоритмы прогнозирования арестов. Такие алгоритмы часто обучаются на данных, которые отражают расовую дискриминацию в системе правосудия. В результате эти алгоритмы могут предсказывать, что чернокожие люди более склонны к совершению преступлений, чем белые, даже если это не так [12]. Данный пример показывает, что важно учитывать предвзятость данных при разработке и использовании алгоритмов машинного обучения. Необходимо использовать методы, которые помогают выявлять и устранять предвзятость в данных.

В настоящее время существует несколько методов для обнаружения предвзятости в обучающих данных. Один из таких методов заключается в использовании метрик, которые измеряют разницу в предсказаниях, сделанных на основе данных, отражающих существующие предубеждения, и данных, отражающих идеализированный мир [19]. Однако этот метод не является универсальным, так как он может давать ложные результаты в случае наличия ошибок в тестовых данных.

Другой подход заключается в использовании метода предсказания следующего действия. Этот метод позволяет выявлять аномалии в данных, которые могут указывать на наличие предвзятости [15]. Например, если система предсказывает, что следующий документ в деле будет иск, но вместо этого поступает ходатайство, это может указывать на то, что данные были предвзяты в пользу исков.

Помимо того, для минимизации предвзятости в алгоритмах машинного обучения можно использовать концепцию групповой справедливости. Эта концепция предполагает, что решения, принимаемые алгоритмом, должны быть справедливыми для всех групп населения. Для этого алгоритм может быть модифицирован таким образом, чтобы он учитывал статистические данные о различных группах населения [8].

Важно также уделять внимание этическим аспектам использования машинного обучения в судопроизводстве. К этим аспектам относятся: прозрачность, объективность, недискриминация, защита персональных данных и отслеживаемость принимаемых алгоритмом решений. В контексте судопроизводства эти проблемы могут быть особенно актуальными, так как правильность и справедливость принимаемых судом решений зависят от того, какие данные используются для принятия этих решений и как они интерпретируются алгоритмами машинного обучения. Поэтому важно обеспечить прозрачность и объективность принимаемых алгоритмом решений, а также учитывать факторы групповой справедливости при работе с данными и принятии решений.

Проанализировав способы использования системы ИИ в правовой сфере и потенциальные риски внедрения решений на его основе, предлагаем методологические принципы для внедрения решений на основе ИИ в судопроизводство. Эти принципы основаны на трехэтапном подходе:

Этап 1. Ручной процесс. На этом этапе решение на основе ИИ используется в качестве ассистента, а окончательные решения принимаются участниками

судебного процесса. Это позволяет выявить и устранить потенциальные ошибки в алгоритме.

Этап 2. Ограниченное развертывание. На этом этапе решение на основе ИИ используется для принятия решений самостоятельно, но только в ограниченном масштабе. Это позволяет выявить ошибки в системе, которые могут возникнуть в результате увеличения масштаба применения.

Этап 3. Постепенное расширение. На этом этапе решение на основе ИИ используется в полном масштабе. Однако участникам судебного процесса предоставляется возможность обжаловать решения системы [6].

Эти принципы позволяют снизить риски, связанные с внедрением решений на основе ИИ в судопроизводство. Они также обеспечивают прозрачность и подотчетность системы, что важно для обеспечения справедливого правосудия.

Резюмируем, что применение ИИ в судопроизводстве может ускорить процесс принятия решений и повысить их объективность, но также несет с собой риски, такие как предвзятость алгоритмов и нарушение конфиденциальности данных. Чтобы снизить эти риски, необходимо соблюдать следующие принципы:

– системы ИИ должны быть прозрачными и подотчетными;

– их алгоритмы должны быть разработаны с учетом социальных и этических норм;

– данные, на которых обучаются системы, должны быть репрезентативными и непредвзятыми.

Кроме того, необходимо учитывать, что качество работы систем ИИ зависит от архитектуры данных и качества обучающей выборки.

Список литературы

1. Бирюков П. Н. Искусственный интеллект и «предсказанное правосудие»: зарубежный опыт // Lex russica. 2019. № 11. С. 79–87.

2. Бирюков П. Н. Цифровизация правосудия по гражданским делам: опыт ЕС // Арбитражный и гражданский процесс. 2022. № 2. С. 3–7.

3. Интернет-суд: новый проект в действии. URL: https://www.obwbip.com/04D540/assets/files/News/Internet-Court-On-the-Fly-RU.pdf

4. Крисько В. С. К вопросу о реализации принципа доступности правосудия и создания единого информационного пространства судебной системы // Администратор суда. 2019. № 1. С. 54–56.

5. Момотов В. В. Искусственный интеллект в судопроизводстве: состояние, перспективы использования // Вестник университета имени О. Е. Кутафина (МГЮА). 2021. № 5. С. 188–191.

6. Ховард Д., Гуггер С. Глубокое обучение с fastai и PyTorch: минимум формул, минимум кода, максимум эффективности. СПб., 2022.

7. Чудиновская Н. А. Некоторые направления цифровизации правосудия в России и странах Евросоюза // Арбитражный и гражданский процесс. 2022. № 7. С. 7–9.

8. Araujo M., Pagano T. P., Loureiro R., Lisboa F, Peixoto R. M., Guimarães G., Cruz G., Santos L., Cruz M., Oliveira E., Winkler I., Nascimento E. Bias and Unfairness

in Machine Learning Models: A Systematic Review on Datasets, Tools, Fairness Metrics, and Identification and Mitigation Methods // Big Data and Cognitive Computing. 2023. № 7(1). P. 15.

9. Bogert E., Schecter A. & Watson R. T. Humans rely more on algorithms than social influence as a task becomes more difficult // Science Reports. 2021. № 11. P. 8028.

10. Colombian judge says he used ChatGPT in ruling. URL: https://www.theguardian.com/technology/2023/feb/03/colombia-judge-chatgpt-ruling

11. Godwin J. Position of Artificial Intelligence in Justice System: Justice of the Future. URL: https://nji.gov.ng/wp-content/uploads/2021/12/Position-of-Artificial-Intelligence-in-Justice-System-Justice-of-the-Future-by-Joel-Gogwim.pdf

12. Heaven W. D. Predictive policing algorithms are racist. They need to be dismantled // MIT Technology Review. 2020. № 3.

13. Jones N. AI science search engines expand their reach [Электронный ресурс] // Nature News. 2016. № 11.

14. Khan A. AI-powered Indian judiciary: A step forward or cause for concern? URL: https://www.barandbench.com/columns/litigation-columns/ai-powered-indian-judiciary-a-step-forward-cause-concern

15. Lee S., Lu X., Reijers Hajo A. The Analysis of Online Event Streams: Predicting the Next Activity for Anomaly Detection // arXiv. 2022. № 03. Pp. 1–10.

16. Lim S. Judicial Decision-Making and Explainable Artificial Intelligence // Singapore Academy of Law Journal. 2021. № 33. P. 280–314.

17. Punjab and Haryana High Court uses ChatGPT in bail order. URL: https://www.barandbench.com/news/litigation/punjab-haryana-high-court-uses-chatgpt-bailorder

18. Reiling A. D. Courts and Artificial Intelligence // International Journal for Court Administration. 2020. № 11. Pp. 1–8.

19. Yu Z., Xi X. A Pilot Study on Detecting Unfairness in Human Decisions with Machine Learning Algorithmic Bias Detection // arXiv. 2021. № 12. Pp. 1–9.

Д. Э. Демин,
студент,
Сибирский федеральный университет
Н. В. Шапран,
старший преподаватель,
Сибирский федеральный университет

ГРАЖДАНСКО-ПРАВОВАЯ ДИФФАМАЦИЯ ДЕЛОВОЙ РЕПУТАЦИИ МЕДИЦИНСКИХ РАБОТНИКОВ В ЦИФРОВОМ ПРОСТРАНСТВЕ

Аннотация. Целью исследования выступает анализ деликта в цифровом пространстве на примере гражданско-правовой диффамации деловой репутации медицинских работников. Раскрываются правовая природа и особенности

диффамации деловой репутации медицинских работников. Рассматриваются существующие меры охраны деловой репутации медицинских работников в рамках цифровой платформы «ПроДокторов». Анализируются нарушения положений законодательства и правил публикации материалов в аспекте защиты деловой репутации со стороны пользователей и модераторов цифровой платформы. Предлагаются новеллы по охране деловой репутации медицинских работников в цифровом пространстве.

Ключевые слова: право, цифровизация, цифровые технологии, гражданское правонарушение, гражданско-правовая диффамация, охрана деловой репутации, медицинские работники, пользователи цифровых технологий

CIVIL LEGAL DEFAMATION OF THE BUSINESS REPUTATION OF MEDICAL WORKERS IN THE DIGITAL SPACE

Abstract. The aim of the study is to analyze the tort in the digital space on the example of civil defamation of the business reputation of medical workers. The legal nature and features of defamation of the business reputation of medical workers are revealed. Existing measures to protect the business reputation of medical workers within the «ProDoctorov» digital platform are considered. Violations of the provisions of the law and the rules for publishing materials are analyzed in the aspect of protecting business reputation on the part of users and moderators of the digital platform. Novels are proposed to protect the business reputation of medical workers in the digital space.

Keywords: law, digitalization, digital technologies, tort, civil defamation, protection of business reputation, medical workers, users of digital technologies

Одной из тенденций современного общества выступает цифровизация – активное внедрение цифровых технологий во все сферы деятельности человека. Проявлением данной тенденции в сфере оказания медицинских услуг выступает создание специальных интернет-ресурсов, на которых пациенты и лица, желающие получить медицинскую помощь, могут в форме отзывов обменяться информацией о медицинской услуге и ее исполнителе- медицинском работнике.

Несмотря на положительную роль указанных цифровых платформ для гражданского оборота и повышения уровня здравоохранения, они являются полем для противоправных действий пользователей и модераторов сайта.

Одним из актуальных видов правонарушения в данной области выступает диффамация деловой репутации медицинских работников. Гражданско-правовая диффамация – деликт, «состоящий в распространении не соответствующих действительности сведений, порочащих честь, достоинство или деловую репутацию лица» [3. С. 90]. Исходя из анализа гражданского законодательства, диффамация деловой репутации должна соответствовать таким критериям, как: факт распространения сведений, связанных с профессиональной деятельностью лица; порочащий характер сведений, не соответствие данных сведений действительности, распространение сведений третьим лицом [4].

Согласно позиции А. Л. Анисимова, предметом деловой репутации является «оценка социальной значимости отдельно взятого лица, которая определяется уровнем его квалификации и характеристикой профессиональной деятельности» [1. С. 9].

Медицинский работник как субъект, осуществляющий профессиональную деятельность, обладает субъективным правом на защиту деловой репутации от диффамации. Исходя из положений ст. 152 ГК РФ, данное субъективное право реализуется через такие способы защиты, как: опровержение недостоверных и порочащих деловую репутацию сведений, возмещение убытков и компенсация морального вреда [2].

Интернет-ресурсы для охраны деловой репутации медицинских работников от диффамации применяют локальные правила размещения материалов. Например, модераторы сайта отзывов «ПроДокторов» не допускают к публикации отзывы, содержащие: нарушение законодательства РФ и призывающие к его нарушению; антирекламу медицинских услуг определенных медицинских работников; ненормативную лексику и оскорбления в отношении медицинских работников [6].

Анализируя судебную практику по делам о защите деловой репутации медицинских работников от порочащих сведений, распространенных в интернет-ресурсе «ПроДокторов» [7], необходимо отметить следующее.

Пользователи сайта умышленно предлагают для публикации сведения, умаляющие репутацию медицинских работников, что является нарушением локальных правил размещения материалов сайта «ПроДокторов».

Модераторы сайта не осуществляют проверку и допускают для публикации указанные сведения, что приводит к их распространению в отношении индивидуально-неопределенного круга лиц. Действия модераторов нарушают гражданское законодательство, законодательство РФ о СМИ и локальные правила размещения материалов [5].

Однако медицинские работники в полной мере реализуют свое субъективное право на защиту деловой репутации, взыскивая моральный вред и опровергая порочащие и не соответствующие действительности сведения.

Таким образом, проблема диффамации медицинских работников в цифровом пространстве заключается не в защите деловой репутации, а в ее охране. Предлагается усилить меры по охране деловой репутации медицинских работников в цифровом пространстве.

Во-первых, необходимо ввести в локальные правила публикации материалов сайта-отзывов условие о предоставлении пользователем данных, подтверждающих предлагаемые для публикации сведения. Такими данными могут выступать аудио и видеозаписи, фотографии, письменные доказательства, заключение эксперта. В случае отказа от предоставления указанных данных, модераторам сайта необходимо отказывать пользователям в публикации сведений.

Во-вторых, надлежит ввести в локальные правила публикации материалов сайта условие о блокировке пользователя, который неоднократно предлагал к публикации порочащие и не соответствующие действительности сведения или

был привлечен по решению суда к гражданской правовой ответственности в связи с распространением в интернет-ресурсах сведений, умаляющих деловую репутацию медицинских работников.

В-третьих, предлагается обязать модераторов цифровых платформ осуществлять публикацию не только отзывов пользователей, но также и иную информацию, которая соответствует действительности и характеризует деловую репутацию медицинского работника. Указанная информация может заключаться в результатах контрольно-надзорных мероприятий уполномоченных органов и достижениях в учебной, научной и профессиональной деятельности медицинского работника. Такая мера позволит сформировать объективный образ медицинского работника у пользователей сайта.

В заключение отметим то, что проблема диффамации деловой репутации медицинских работников в цифровом пространстве остается открытой и требует дальнейшего нормативного урегулирования в области мер по охране деловой репутации медицинских работников.

Список литературы

1. Анисимов А. Л. Честь, достоинство, деловая репутация под защитой закона. М.: ВЛАДОС-ПРЕСС, 2004. 88 с.

2. Гражданский кодекс Российской Федерации (часть первая): федеральный закон 30.11.1994 № 51-ФЗ // Справочная правовая система «КонсультантПлюс».

3. Невзгодина Е. Л., Парыгина Н. Н. Диффамация как правовая категория // Вестник Омского университета. 2016. № 2. С. 86–94.

4. О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц: Постановление Пленума Верховного Суда РФ от 24.02.2005 № 3 // Справочная правовая система «КонсультантПлюс».

5. По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона «О персональных данных» в связи с жалобой общества с ограниченной ответственностью «Медрейтинг»: Постановление Конституционного суда РФ от 25.04.2021 № 22-П // Справочная правовая система «КонсультантПлюс».

6. Правила публикации материалов интернет-ресурса «ПроДокторов». URL: https://prodoctorov.ru/info/publishing-policy/#publication

7. Решение № 2-2756/2019 от 27 мая 2020 г. по делу № 2-2756/2019 Октябрьского районного суда г. Новороссийска; Решение № 2-8294/2017 от 1 сентября 2017 г. по делу № 2-8294/2017 Ленинского районного суда г. Краснодара. URL: https://sudact.ru

Р. Ю. Демина,
кандидат технических наук, доцент,
Астраханский государственный университет
имени В. Н. Татищева
Д. Э. Шукралиева,
аспирант, старший преподаватель,
Астраханский государственный университет
имени В. Н. Татищева

ПРАВОВАЯ БАЗА ЗАЩИТЫ WEB-РЕСУРСОВ ОТ ВРЕДОНОСНОГО ПАРСИНГА

Аннотация. В последнее время наблюдается тенденция постоянного увеличения создаваемого пользователями мировой сети контента и его нелегитимного заимствования с целью получения личной выгоды. В связи с этим становится актуальным вопрос защиты общедоступной информации от несанкционированного копирования. Проанализировано законодательство Российской Федерации в данной сфере, на основании чего предложено техническое решение по защите web-ресурсов от вредоносного парсинга.

Ключевые слова: парсер, дезинформация, пользовательское соглашение

LEGAL FRAMEWORK FOR PROTECTING WEB RESOURCES FROM HARMFUL PARSING

Abstract. Recently, there has been a trend of constant development of digital technologies, which has led to the simplification of unauthorized borrowing of information resources. In this regard, the issue of protecting publicly available information from unauthorized copying becomes urgent. A technical solution has been proposed that would not contradict the legislation of the Russian Federation.

Keywords: parser, imposition, user agreement

Введение. В цифровом обществе информационный контент является объектом рыночных отношений. Стоимость различной информации может варьироваться в неограниченно широком диапазоне. Злоумышленники или мошенники используют информацию для совершения различных преступлений. Для сбора информации применяются различные технологии такие как: промышленный шпионаж, подкуп сотрудников или автоматизированный сбор общедоступных сведений, так называемый парсинг. Автоматизированный сбор информации с указанных интернет-ресурсов возможно осуществить с помощью специального программного обеспечения, онлайн-сервиса или скрипта. Парсеры копируют необходимые данные с заранее перечисленных веб-ресурсов и формируют выходные данные в нужном формате.

Основная часть. Основным направлением деятельности вредоносных парсеров является автоматизированный сбор персональных данных пользователей, интеллектуальной собственности, финансово-значимого контента. Собранная информация может быть использована как для перепродажи или собственного

несанкционированного использования, так и для совершения компьютерного преступления.

Так, например, в августе 2023 г. сервис мониторинга внешних цифровых угроз компании Solar AURA [1] зафиксировал массовую фишинговую рассылку от лица следственных органов с требованием ознакомиться с материалами уголовного дела.

При рассмотрении полученного электронного письма были отмечены следующие признаки, которые у обычного пользователя обычно не вызывают подозрений:

– домены максимально похожи на настоящие;

– при обращении к адресату рассылки указаны персональные данные: ФИО, паспортные данные и адрес регистрации;

– в электронном письме указан номер уголовного дела, полученный из открытых источников.

Такого рода данные могут быть получены путем парсинга соответствующих сайтов, на которых размещена общедоступная информация о материалах уголовных дел.

Злоумышленники не использовали для передачи материалов уголовного дела вредоносный ZIP-файл, так как существует вероятность, что письмо с таким вложением сервис электронной почты распознает как «СПАМ». Поэтому для передачи информации был использован файлообменник. Предполагалось, что при получении будет осуществлен переход по указанной ссылке и загрузка содержимого. Вредоносное программное обеспечение было замаскировано под программу распознавания текста.

Парсинг считается относительно безобидным явлением в сфере информационных технологий. Но приведенный выше пример наглядно демонстрирует негативные последствия от применения парсеров мошенниками.

В связи с этим становится актуальным вопрос защиты общедоступной информации от несанкционированного копирования. Для эффективного противодействия вредоносным парсерам необходимо разрабатывать современные правовые и технические решения. Для этого необходимо проанализировать существующие нормативно-правовые акты с различных точек зрения.

В нормативно-правовых актах Российской Федерации по защите информации отсутствует определение технического термина «парсинг», поэтому рассмотрение вопроса правовой защиты web-ресурсов от вредоносного парсинга необходимо начать с Конституции Российской Федерации. В статье 29 Конституции Российской Федерации упомянуто, что каждый гражданин Российской Федерации вправе свободно осуществлять поиск и получение информации любым законным способом [2]. В Федеральном законе «Об информации, информационных технологиях и о защите информации» № 149 от 27 июля 2006 года также подтверждено: «Информация, размещаемая ее обладателями в сети «Интернет» в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в форме открытых данных» [3].

В примечании к статье 272 Уголовного кодекса Российской Федерации дается определение компьютерной информации. Компьютерной информацией считаются сообщения, данные, сведения, которые представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Анализ указанных нормативно-правовых актов показывает, что данные, выложенные правообладателем без ограничений в сети «Интернет», являются общедоступными и могут автоматизировано собраны.

Однако если парсер был разработан и использован злоумышленниками при атаках на web-ресурсы и собранные сведения в дальнейшем были использованы для совершения противоправных действий, то может быть применена статья 273 Уголовного кодекса Российской Федерации «Создание, использование и распространение вредоносных компьютерных программ». Использование парсеров для умышленного нанесения ущерба или несанкционированного копирования информации влечет за собой риск уголовной ответственности [4].

Из приведенного выше анализа можно сделать вывод, что парсинг общедоступной информации сам по себе не является преступлением. Но практика показывает, что данный процесс очень часто предшествует совершению преступления. Необходимо рассмотреть возможность защиты пользователей и владельцев информации от несанкционированного автоматизированного копирования.

Правовые меры от несанкционированного автоматизированного копирования. При посещении некоторых web-ресурсов и изучении их структуры можно отметить, что владельцы размещают условия использования или пользовательские соглашения. Указанные документы регулируют отношения между владельцами и пользователями web-ресурсов, фиксируют права, обязанности и ответственность сторон, а также правила использования ресурса и контента. В случае, если в пользовательском соглашении имеется пункт, который запрещает автоматизированное копирование, то тот, кто осуществляет процесс парсинга нарушает правила пользования данным ресурсом.

Для пользователей web-ресурсов не понятно подписано ли пользовательское соглашение и необходимо ли это, если он планирует посетить сайт для чтения, просмотра.

Следует учитывать, что большинство сайтов не привязаны к персональным данным физического лица, что затрудняет идентификацию заключившего с владельцем web-ресурса пользовательское соглашение [5].

Существует различие между зарегистрированными и незарегистрированными пользователями ресурсов. Если парсинг осуществляется зарегистрированным пользователем, который при регистрации подтвердил свое согласие с условиями пользовательского соглашения, владелец сайта имеет право применить санкции, предусмотренные в договоре. Простейшее наказание – это «бан», который юридически может означать введение ограничения действий пользователя или расторжение договора в одностороннем порядке [6].

Технические меры от несанкционированного автоматизированного копирования. Для предотвращения одной атаки со стороны программного

обеспечения парсера возможно применить несколько вариантов защиты, которые при комплексном воздействии на атаку позволяют дать удовлетворительный результат для владельца информации при защите его сведений.

Для эффективной защиты от атак вредоносного программного обеспечения парсера можно применить несколько методов, которые вместе обеспечат надежную защиту информации. Один из таких методов активно используется в области информационной безопасности – это применение ложной информации для запутывания злоумышленника. Например, внедрение муляжей видеокамер или объектов инфраструктуры, которые будут вводить злоумышленника в заблуждение и отвлекать его от реальных целей.

Для защиты WEB-пространства от парсинга также может быть использован метод навязывания заведомо ложной информации злоумышленникам. Этот подход заключается в том, что WEB-ресурс обнаруживает роботизированный трафик и выводит измененную версию страницы для подозрительных пользователей [7].

Аналогичная стратегия применяется в приложении «Авито», где в объявлениях не указывается достоверный номер телефона продавца или покупателя, но при вызове осуществляется переадресация на правильный номер.

Предлагается расширить данный подход следующим образом:

1. Определить наличие вредоносных парсеров, осуществляющих автоматизированный сбор данных.

2. Создать фальшивые данные по запросу.

3. Передать эти фальшивые данные в ответ на запросы.

При этом необходимо учесть, что вывод фальшивых данных не должен повлиять на внешний вид страницы. Кроме того, желательно, чтобы страница была изменена таким образом, чтобы законный пользователь все равно мог просматривать оригинальный контент.

Давайте рассмотрим две ситуации, при которых происходит парсинг:

1. Злоумышленник использует поиск на сайте, и в результате ему предоставляется список информации.

Когда пользователи проводят легальный поиск, результаты будут соответствовать их требованиям, а наиболее подходящая информация будет расположена в начале списка. Однако, если поиск осуществляется вредоносным парсером, результаты могут быть перемешаны, и строки, полностью соответствующие критериям, могут быть опущены. Тем не менее, не исключая возможность получения «ложного списка» легальным пользователем. В этом случае, с помощью анализа правильных результатов, пользователь сможет легко выбрать наиболее подходящую информацию для своего поиска.

2. Злоумышленник производит сканирование WEB-страниц по известным ему адресам, с целью получения подробной информации об объектах – людях, товарах и т. д. При обнаружении вредоносной активности, на HTML-странице создается дополнительное поле, в которое сохраняется оригинальная информация. При этом ложная информация выводится в поле, предназначенное для оригинальных данных. На рис. представлена схема анализа поведения пользователя.

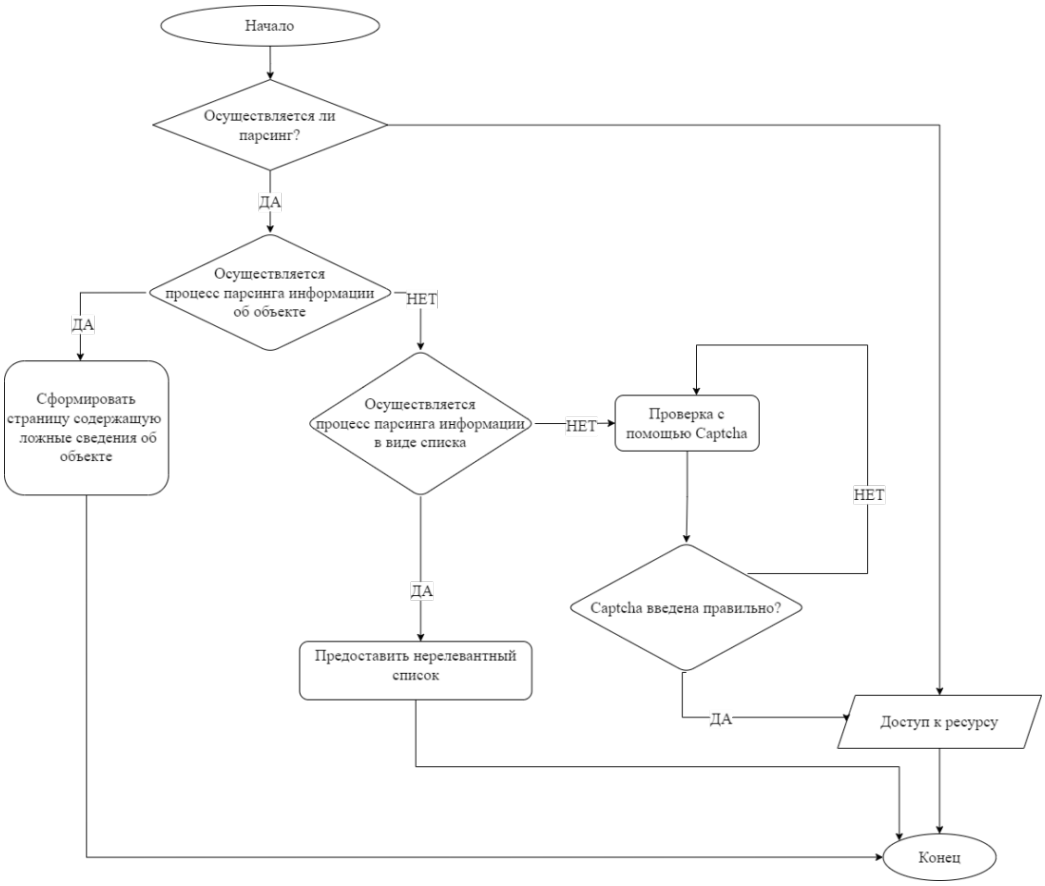

Рис. Анализ поведения пользователя

Применение данного метода позволит компрометировать собранный парсером пакет информации.

Заключение. Основными направлениями использования парсинга злоумышленником являются: автоматизированный сбор персональных данных пользователей, информация об интеллектуальной собственности, финансово-значимый контент.

В статье был проведен анализ нормативно-правовой базы Российской Федерации по защите общедоступной информации и сделан вывод о допустимости навязывания заведомо ложной информации в случае нарушения правил пользовательского соглашения.

В рамках статьи были рассмотрены способы защиты от парсинга и предложен усовершенствованный способ защиты от парсинга – навязывание злоумышленнику заведомо ложной информации. Реализация данного метода позволит сделать собранные данные непригодными для последующего использования.

Список литературы

1. «РТК-Солар»: мошенники пишут россиянам от имени правоохранителей. URL: https://rt-solar.ru/events/news/3665

2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993). URL: https://www.consultant.ru/document/cons_doc_LAW_28399

3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_61798

4. Уголовный кодекс Российской Федерации: федеральный закон от 13.06.1996 № 63-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_10699

5. Демина Р. Ю., Ажмухамедов И. М. Защита web-контента от нелегитимного роботизированного копирования // Вестник ГГНТУ. Технические науки. 2022. Т. 18, № 1. С. 3-4.

6. Демин К. С., Марьенков А. Н. Обнаружение и противодействие вредоносным веб роботам // Проблемы повышения эффективности научной работы в оборонно-промышленном комплексе России: Материалы IV Всероссийской научно-практической конференции. Астраханский государственный университет. Астрахань, 2021. С. 121–127.

7. Демина Р. Ю., Ажмухамедов И. М. Защита web-контента от нелегитимного роботизированного копирования // Вестник ГГНТУ. Технические науки. 2022. Т. 18, № 1. С. 11–17.

Р. Д. Мартинс,
кандидат юридических наук,
частнопрактикующий адвокат в Бразилии
(OAB/RN 15.923)

ЗАЩИТА АВТОРСКИХ ПРАВ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: О НЕПРОЗРАЧНОСТИ АЛГОРИТМОВ ПОСРЕДНИКОВ

Аннотация. Целью исследования является выявление возникающих у автора сложностей в сфере защиты своих авторских прав в условиях цифровизации из-за непрозрачности алгоритмов посредников, таких как «Amazon», «ЛитРес», особенно когда речь идет о чтении книги, взятой у посредника по подписке. Это обусловлено главным образом тем, что у автора практически нет возможности даже установить факт нарушения. Как алгоритмы рассчитывают количество прочитанных страниц и на основании чего решают, сколько получит автор. Эти проблемы требуют немедленного урегулирования, так как без полноценной прозрачности появляется возможность замаскированного пиратства со стороны посредника.

Ключевые слова: алгоритмы, авторское право, цифровизация, датаизм, открытый исходный код, экономика подписок, непрозрачность алгоритмов

COPYRIGHT PROTECTION UNDER THE CONTEXT OF DIGITALIZATION: ON THE OPACITY OF THE ALGORITHMS OF INTERMEDIARIES

Abstract. The purpose of the study is to identify the difficulties for the author to protect their copyrights in the context of digitalization, due to the opacity of intermediary algorithms, such as Amazon, Litres, especially when it comes to reading books taken from

a subscription intermediary. This is mainly due to the fact that it is practically impossible for the author to even verify the fact of a violation. How the algorithms calculate the number of pages read, and based on what the algorithms decide how much the author will receive. These issues require immediate regulation because, without greater transparency, there is the possibility of disguised piracy by an intermediary.

Keywords: algorithms, copyright, digitalization, dataism, open source, subscription economy, opacity of algorithms

С появлением Интернета и ростом его популярности стало понятно, что мировая сеть станет площадкой для усиления оборота имущества. Согласно изданию Forbes, в 2023 году ожидается то, что 20,8 % розничных покупок будут осуществляться по интернету [8]. На этом рынке среди многих других благ встречаются объекты, охраняемые авторским правом, такие как книги. При этом не только печатные, но и цифровые. Продажи цифровых книг превышали долю печатных изданий, купленных на сайте Amazon в 2011 году, но согласно сайту wordsrated.com, специализирующемуся на исследованиях авторов, публикаций и тому подобном, сегодня печатные издания превышают в продажах цифровые в 3 раза [11].

Следует также сказать, что цифровые технологии создали условия для появления экономики подписок. Это важнейшее направление, которое действительно показывает вектор развития будущего потребления [1]. Модель подписок интересна и компаниям, предлагающим услуги, а также подписчикам, так как обычно такие сервисы предоставляют огромное количество доступных материалов по относительно низкой цене.

Развитие технологий всегда вызывало у издателей опасения в том, что их права будут нарушены. Конечно, от этого обычно страдают и авторы. Интернет в этом смысле стал настоящей «бомбой»: контролировать распространение копий в цифровом мире невероятно сложно. Файлы (в которых могут находиться и объекты авторского права) можно копировать так быстро и незатратно, что, казалось, пиратство окончательно воцарится. Несмотря на то, что издателям действительно это наносит ущерб, цифровой мир обнаруживает и другие возможности нарушения авторских прав, о которых пойдет речь дальше. В частности, поговорим о непрозрачности алгоритмов посредников.

Перед тем как перейти к алгоритмам, следует сказать, что и Amazon, и другие платформы (как, например, «ЛитРес» в России) играют важнейшую роль в расширении возможности публикации, особенно авторам, без помощи издательства. Кроме этого, часто стоимость цифровых книг значительно ниже печатных по понятным причинам, что расширяет и доступ общества к культурным благам. Это бесценно, но нужно серьезно анализировать и понимать возможные проблемы, вызываемые этой моделью оборота охраняемых авторским правом объектов. Эти трудности показывают кризис современного правового регулирования, требующий смену парадигмы [2].

Когда мы думаем о пиратстве в Интернете, обычно рассуждаем об этом явлении с точки зрения недобросовестных пользователей. Конечно же, кто-то выкладывает материал в интернет, но вскоре после этого копии распространяются

пользователями. Итак, в Интернете сложно установить контроль копий. Но, если это проблематично сделать в отношении цифровых книг, то как авторам точно знать, сколько копий продалось и сколько страниц прочитали пользователи через платформы Amazon, «ЛитРес» и другие? А что такое вообще страница для алгоритмов? Когда речь идет о контрафактных бумажных копиях, то легче установить факт нарушения прав, но в интернете у автора всего лишь отчет, подготовленный алгоритмом.

Мы, конечно, никого не обвиняем ни в чем, но давайте возьмем в качестве примера Amazon и подумаем о правах авторов. Надо сказать, что относительно цифровых книг алгоритм действительно показывает правильное количество их проданных копий. Есть и другой вопрос – чтение страниц по подписке. Если также брать в расчет оборот книг на сайте Amazon, взятых по подписке (Kindle Unlimited), то доля рынка этой платформы достигает 83 % в США [11]. Итак, нет сомнений в значимости такого направления в современном потреблении. Но, опять же, возникает проблема: что такое страница для алгоритма Kindle Unlimited? Как он поймет, что страница прочитана? В такой модели пользователи платят за подписку и могут читать любые книги, доступные по ней. Оплата подписок образует фонд Kindle Direct Publishing Select (KDP Select), который распределяется между авторами. Мы не знаем точно, как формируется этот фонд, но полагаем, что часть денег остается у Amazon.

На сайте Amazon есть страница с информацией по этой теме, где заявлено, что алгоритм KENPC вышел уже в третьей версии и продолжается его усовершенствование для достижения большей справедливости в распределении глобального фонда KDP Select [6]. Ответа на вопрос, что такое прочитанная страница, однако, по-прежнему нет. Как же автору защитить свои авторские права, если даже нет критерия понимания, что представляет собой прочитанная страница?

Посмотрим пункт 2.3 «Условий и положений» KDP, раздел KDP Select Benefits: «Мы создадим ежемесячный фонд, и вы сможете зарабатывать часть этого фонда от клиентов, читающих ваши цифровые книги, включенные в программы подписки Kindle. Мы будем выделять часть фонда каждому маркетплейсу, где программа доступна, и вы будете получать долю ежемесячного фонда в зависимости от количества вашего контента, прочитанного клиентами на каждом маркетплейсе. Эти доли являются вашим общим роялти за доступ клиентов к вашим цифровым книгам через программы подписки Kindle. Мы будем устанавливать, по нашему собственному усмотрению, критерии для определения того, какая часть вашего контента читается и как пропорционально распределить фонд. Мы можем публично объявить лучшие цифровые книги, включая автора, издателя, количество квалифицированных прочтений и заимствований, а также заработанные гонорары фонда KDP Select» [7].

Другими словами, они сами решают, какая часть фонда KDP Select причитается автору. Конечно же, количество прочитанных страниц имеет значение, но понятно также, что алгоритм весьма непрозрачный, равно как и условия обжалования, так как при решении опубликовать свою книгу автор знает или должен знать, что решение о том, сколько ему заплатить, принимает Amazon. Классификация

договора автора и Amazon – не объект нашего исследования, но сама логика функционирования и терминология, правоотношения между сторонами указывают на то, что это лицензионный договор. Размер вознаграждения в таких договорах весьма важен. По ГК РФ (ст. 1235) договор считается незаключенным, если в возмездном лицензионном договоре отсутствуют условия о размере вознаграждения или порядке его определения [3]. Другими словами, либо размер вознаграждения, либо порядок его определения должны быть установлены в договоре. Конечно, в Amazon это не прописано. Несмотря на то, что Amazon в настоящее время не работает в России, понятно, что приведенные условия должны быть установлены в любом договоре таких правоотношений. Безусловно, сама модель нуждается в регулировании, так как любая компания с подобной бизнес-моделью сталкивается с этим же вопросом.

Итак, непрозрачность алгоритма содействует появлению пиратства со стороны посредника. Мы, опять же, не обвиняем никакую компанию в этом, но, уверены, настало время обсуждать способы исправить ситуацию. Мы не утверждаем, что алгоритм Amazon платит автору неправильно или показывает меньше прочитанных страниц в своем отчете, чем положено. Однако необходимо, чтобы критерии расчета были более прозрачными. Есть довольно обширный перечень литературы о защите авторских прав в интернете, а отдельно можем отметить работу М. Ю. Осипова, который, в свою очередь, упоминает другие работы по этому вопросу и делает общий обзор возможностей по защите авторских прав в интернете. В работе М. Ю. Осипова [5] (и, думаем, по очевидным причинам, ни в каких других научных работах) приведены условия защиты авторских прав в случае, когда автор сам не может фиксировать факт нарушения. Именно это происходит, когда мы публикуем книгу на Amazon и других подобных площадках.

Понимаем, что алгоритм часто является способом усиления экономической эффективности, поэтому бизнес и компании неохотно будут открывать исходный код своих алгоритмов. Однако нам не кажется неразумным с точки зрения права позволять компаниям решать самостоятельно и единолично, сколько выплачивать авторам.

В этом смысле остается под вопросом роль прочитанной страницы в определении размера вознаграждения автора. Дело в том, что Amazon в вышеупомянутых «Условиях и положениях» смело утверждает, что оставляет за собой право определять, какие части контента автора считаются прочитанными. Достаточно загадочное заявление: количество прочитанных страниц будет определено на усмотрение Amazon (а не по действительному прочтению). Это значит, что и критерии определения прочитанных страниц на усмотрении компании? В любом случае непрозрачность системы в целом и необходимость ее регулирования очевидны. Несмотря на то, что часто алгоритмы принадлежат частным компаниям, они затрагивают и общественные интересы, влияя на них [10]. Социологи тоже прилагают усилия, чтобы решить вопрос неравенства, который часто создают алгоритмы [4]. Это важно упомянуть, так как и алгоритм Amazon, по всей видимости, также определяет размер вознаграждения авторов на основании неравных условий,

поскольку расчет оплаты ведется не только на основании прочитанных страниц, а исходя из собственного мнения.

В качестве вывода можно предложить разные варианты решения проблемы. Один из них – просто принудить компании работать с алгоритмами с открытым исходным кодом или же установить общий алгоритм для определения количества прочитанных страниц – как в случае, о котором говорили в этой работе. Это может снизить экономическую эффективность бизнеса, но решение проблемы часто бывает затратным, поэтому может оказаться допустимым. Без прозрачности алгоритмов нет возможности поддерживать правовые отношения на доверии и добросовестности [9].

Самый серьезный вопрос даже не юридического характера. Дело в том, что отсутствие литературы по этой тематике показывает не что иное, как рост веры в датаизм. В обсуждаемом нами случае, даже если есть нарушения прав любого характера посредниками, ситуация выглядит следующим образом: глаза не видят – сердце не чувствует.

Список литературы

1. Беликова К. М. Экономика подписок: право собственности и будущее потребления // Вопросы российского и международного права. 2021. Т. 11, № 4–1. С. 60–72.

2. Войниканис Е. А. Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. Издательский дом «Юриспруденция», 2016.

3. Гражданский кодекс Российской Федерации (часть четвертая) [Текст]: от 18.12.2006 № 230-ФЗ // СПС Консультант Плюс.

4. Мартыненко Т. С., Добринская Д. Е. Социальное неравенство в эпоху искусственного интеллекта: от цифрового к алгоритмическому разрыву // Мониторинг. 2021. № 1.

5. Осипов М. Ю. Защита авторских прав в сети Интернет: основные особенности и проблемы //Актуальные проблемы российского права. 2018. №. 12 (97). С. 116–122.

6. Amazon KDP: Royalties in Kindle Unlimited. URL: https://kdp.amazon.com/en_US/help/topic/G201541130

7. Amazon: Kindle Direct Publishing Terms and Conditions. URL: https://kdp.amazon.com/en_US/terms-and-conditions?ref_=FOOT_tac

8. FORBES: 38 E-Commerce Statistics OF 2023. URL: https://www.forbes.com/advisor/business/ecommerce-statistics

9. Ouyang W. Research on the Role of Algorithm Transparency in Algorithm Accountability // 2019 3rd International Conference on Education, Economics and Management Research (ICEEMR 2019). Atlantis Press, 2020. Pp. 234–237.

10. Ryan M. J. Secret Algorithms, IP Rights, and the Public Interest // Nev. LJ. 2020. Т. 21. Pp. 61–81.

11. WORDSRATED: Amazon Publishing Statistics. URL: https://www.forbes.com/advisor/business/ecommerce-statistics

М. Б. Добробаба,
доктор юридических наук, доцент,
Московский государственный юридический
университет имени О. Е. Кутафина

ЦИФРОВИЗАЦИЯ ГОСУДАРСТВЕННОЙ СЛУЖБЫ: ПРОБЛЕМЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ

Аннотация. Статья посвящена анализу основных направлений цифровизации государственной службы, реализация которых направлена на обеспечение цифровой трансформации государственного управления. Делается вывод, что, поскольку кадровая система государственной службы детально регламентирована и лишена гибкости, это не позволяет ей быстро реагировать на динамичные изменения, связанные с цифровизацией. В этих условиях многие направления применения цифровых технологий в государственном управлении реализуются в экспериментальном режиме, по итогам применения которого будет оценена их эффективность, проведена доработка правового обеспечения применения цифровых технологий на государственной службе. Учитывая, что использование цифровых технологий в системе государственной службы создает и новые риски правам человека, новые угрозы, в том числе коррупционной направленности, что требует соблюдения баланса между правовым регулированием и внедрением цифровых инноваций.

Ключевые слова: цифровые технологии, цифровая трансформация, государственная служба, цифровизация, искусственный интеллект, цифровой контроль, цифровое профилирование, цифровые компетенции, информационная система, противодействие коррупции, автоматизация, экспериментальный режим

DIGITALIZATION OF PUBLIC SERVICE: PROBLEMS OF LEGAL SUPPORT

Abstract. This article is devoted to the analysis of the main directions of digitalization of the public service, the implementation of which is aimed at ensuring the digital transformation of public administration. It is concluded that since the personnel system of the civil service is regulated in detail and lacks flexibility, this does not allow it to quickly respond to dynamic changes associated with digitalization. In these conditions, many areas of the use of digital technologies in public administration are being implemented in an experimental mode, based on the results of which their effectiveness will be assessed, and the legal framework for the use of digital technologies in the public service will be finalized. Considering that the use of digital technologies in the public service system also creates new risks to human rights, new threats, including corruption, which requires maintaining a balance between legal regulation and the introduction of digital innovations.

Keywords: digital technologies, digital transformation, public service, digitalization, artificial intelligence, digital control, digital profiling, digital competencies, information system, anti-corruption, automation, experimental mode

Введение. В последние годы цифровизация стремительно проникает во все сферы государственного управления, что сопровождается его цифровой трансформацией [8]. Одной из проблем текущего состояния государственного управления, решаемых при цифровизации, является наличие недостаточного уровня цифровизации кадровой работы государственной службы.

К числу задач достижения Национальной цели развития «Обеспечение ускоренного внедрения цифровых технологий в экономике и социальной сфере» относится внедрение цифровых технологий и платформенных решений в сферах государственного управления и оказания государственных услуг [9], реализация которых осуществляется, в том числе, посредством обеспечения цифровой трансформации государственной (муниципальной) службы.

Основная часть. Можно выделить несколько направлений осуществления цифровизации государственной службы, реализация которых направлена на обеспечение цифровой трансформации государственного управления, построение устойчивых отношения общества и государства. К их числу следует отнести:

1) функционирование российской государственной информационной системы в области гражданской службы;

2) отбор сотрудников на государственную службу с помощью искусственного интеллекта;

3) цифровая трансформация рабочих мест на государственной службе;

4) экспериментальное использование электронных документов в кадровой работе;

5) цифровой контроль деятельности государственных служащих;

6) применение цифровых технологий в целях противодействии коррупции в системе государственной службы;

7) цифровое профилирование государственных гражданских служащих и должностей государственной гражданской службы.

8) правовое оформление и развитие у государственных гражданских служащих новых цифровых компетенций.

Функционирование российской государственной информационной системы в области гражданской службы. Единая информационная система управления кадровым составом государственной гражданской службы РФ (далее – ЕИСУКС) является базовым государственным информационным ресурсом в отношении информации о кадровом составе государственных органов [12], с помощью которого автоматизировано большинство аспектов кадровой работы на гражданской службе. Прежде всего, ЕИСУКС позволяет в общей базе объединять вакансии в области государственной службы, обеспечивая взаимодействие граждан, претендующих на замещение вакансий гражданской службы с потенциальным представителем нанимателя; ЕИСУКС объединяет возможности по прохождению профессионального развития государственных служащих [5].

Правовые основы функционирования ЕИСУКС установлены в Постановлении Правительства РФ от 03.03.2017 № 256 «О федеральной государственной информационной системе «Единая информационная система управления кадровым составом государственной гражданской службы Российской Федерации» [4].

В научной литературе указывается на необходимость предусмотреть расширение функционала работы с представителями, вошедшими в федеральный резерв управленческих кадров. С точки зрения комплексного предложения по совершенствованию и развитию ЕИСУКС предлагается модель, позволяющая повысить эффективность и вовлеченность служащих, построить среду для инициатив и привлекательности для кандидатов, развивать лидерство и формировать эффективный резерв кадров. Отдельно необходимо предусмотреть функционал, связанный с оценкой кадровых рисков, позволяющий выявлять риски при планировании, обороте персонала, его оценки, развития, мотивацией и связанные с организационной культурой [15]. Представляется, что расширение имеющегося функционала ЕИСУКС позволит оптимизировать кадровые процессы, предоставляя новые возможности для осуществления кадровой работы.

Отбор сотрудников на государственную службу с помощью искусственного интеллекта. Как известно, поступление на государственную гражданскую службу осуществляется по результатам конкурса [1]. При этом сама процедура отбора – довольно сложный процесс, требующий учета множества требований и критериев, дифференцируемых применительно к отдельным государственным органам. В свою очередь, от правильности отбора кандидатов зависит формирование эффективной и грамотной системы государственного управления.

Учитывая необходимость повышения качества отбора персонала, с 1 сентября 2023 года по 1 ноября 2024 года на платформе «Государственные кадры», созданной на базе «Гостеха», Правительством РФ запланирован эксперимент по найму чиновников с помощью искусственного интеллекта, который позволит автоматизировать как процесс отбора, так и профессионального развития, мотивации, оценки чиновников, формирования профессиональной культуры и противодействия коррупции [10].

Следует отметить, что искусственный интеллект уже давно применяется, как российскими, так и зарубежными кадровыми агентствами при отборе персонала, в том числе, с использованием чат-бота для взаимодействия с претендентами на вакантную должность. Его применение позволяет анализировать резюме большого количества потенциальных сотрудников, анализировать их социальные сети, проводить с ними первичное собеседование, что значительно сокращает время поиска сотрудников.

На государственной гражданской службе эксперимент продлится с целью «апробацию методов осуществления кадровой работы с использованием информационно-коммуникационных технологий». В свою очередь, после запуска платформы «Государственные кадры», ее интегрируют в состав уже существующей Единой информационной системы управления кадровым составом государственной гражданской службы (ЕИСУКС). Как сказано в Пояснительной записке, «к 2030 году должна быть создана и внедрена на всех уровнях государственной службы новая информационная HR-система развития госслужащих, предусматривающая использование технологий искусственного интеллекта».

Вместе с тем следует учитывать, что искусственный интеллект может анализировать и недостоверные источники, а значит, не исключена ошибка при принятии решения. Искусственный интеллект должен применяться как вспомогательный

инструмент при осуществлении рутинных и наиболее трудоемких процессов в подборе персонала. Одновременно можно предусмотреть возможность расширения границ поиска: применение искусственного интеллекта позволит анализировать данные кандидатов, которые не подавали заявки на государственную службу, но подходят под вакансию, с последующим инициированием представителем нанимателя приглашения потенциального кандидата участвовать в конкурсе.

Цифровая трансформация рабочих мест на государственной службе. В 2023 году запланировано осуществление перехода на единую систему коммуникаций на базе типового автоматизированного рабочего места для государственных служащих (далее – АРМ ГС), а также утверждение единой политики работы с данными управления России.

Контракт на выполнение одного из этапов проекта по переводу чиновников с Telegram на российские коммуникационные сервисы получила Структура VK ООО «ВК Цифровые технологии». В свою очередь, АРМ ГС включает в себя защищенный мессенджер, разработанный VK и объединяющий переписки, видеозвонки, почту, календарь, облачное хранилище и «внутренний портал» [16].

Другим направлением цифровизации государственной службы является введение с июня 2023 года в порядке эксперимента электронного документооборота в кадровой работе ряда федеральных государственных органов исполнительной власти [6]. В настоящее время такая возможность на гражданской службе нормативно не закреплена, а оформление кадровых документов осуществляется на бумажных носителях [18, С. 12–16].

Вместе с тем в соответствии с Указом Президента РФ от 31.08.2020 № 536 «Об утверждении Положения о порядке организации экспериментов, направленных на развитие федеральной государственной гражданской службы» [2] в целях апробации и внедрения новых методов осуществления кадровой работы с использованием информационно-коммуникационных технологий проводится эксперимент по введению электронного документооборота на государственной гражданской службе.

Эксперимент проводится с использованием ФГИС «Единая информационная система управления кадровым составом государственной гражданской службы Российской Федерации». Участниками эксперимента стали: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации; Федеральное казначейство; Федеральная налоговая служба; федеральные государственные гражданские служащие указанных органов (на добровольной основе); граждане Российской Федерации, претендующие на замещение должностей федеральной государственной гражданской службы или поступающие на федеральную государственную гражданскую службу в указанные органы (на добровольной основе).

Электронный документооборот имеет несомненные преимущества: его применение позволяет обеспечить скорость и надежность обработки и передачи информации. По результатам проведения эксперимента по его реализации будет оценена его эффективность, проведена доработка, предшествующая широкомасштабному внедрению электронного кадрового документооборота.

Цифровой контроль за деятельностью публичных чиновников. Перспективным направлением цифровой трансформации государственного управления является цифровой контроль, в отношении которого в Государственную Думу РФ внесен законопроект о ежегодной оценке качества работы депутатов всех уровней, руководства регионов и муниципальных образований на портале «Госуслуги» [11].

Встречаются предложения оценивать на сайте «Госуслуги» и государственных служащих, что позволит присваивать им определенный рейтинг, а при рейтинге ниже 50 % – лишать должности [19]. Полагаем, подобный рейтинг может использоваться только в качестве показателя народного доверия в рамках общего рейтингования гражданских служащих. При этом нельзя использовать исключительно его результаты в качестве основания прекращения государственно-служебных отношений.

В отношении государственных гражданских служащих цифровой контроль осуществляется с помощью государственной информационной системе в области противодействия коррупции «Посейдон» [3] (далее – ГИС «Посейдон»), применение которой требует решения ряда проблем [13. С. 25–30]. Так, до сих пор на законодательном уровне не установлена обязательность проведения антикоррупционной проверки по результатам выявления ГИС «Посейдон» фактов коррупционных проявлений, что оставляет простор для злоупотреблений уполномоченных должностных лиц. Не исключены ошибки при принятии решений ИИ, что требует нормативного закрепления возможности пересмотра в ручном режиме результатов проверки, полученных с использованием ГИС «Посейдон».

Следует отметить, что применение ГИС «Посейдон» позволяет сформировать своего рода цифровой профиль проверяемого лица и получить информацию о возможных конфликтах интересов, неформальном общении с представителями подконтрольных граждан и организаций, злоупотреблении полномочиями, сомнительных финансовых операциях и других индикаторах коррупционных рисков [17. С. 126–142].

Формирование цифрового профиля гражданского служащего и цифрового профиля должности гражданской службы осуществляется в соответствие с Распоряжением Правительства РФ от 24 июля 2019 г. № 1646-р [7]. Представляется необходимым включение в цифровой профиль не только официальной, но и неофициальной информации о гражданских служащих, что позволит прогнозировать их служебное поведение, а при необходимости корректировать его [14. С. 32–36].

Цифровая трансформация государственной службы предполагает не только управления кадровым составом, но и развитие у государственных гражданских служащих новых цифровых компетенций, освоение которых позволит оптимизировать организационную работу государственных органов. При этом в состав квалификационных требований к должностям государственной службы должны быть включены цифровые компетенции, дифференцированные с учетом категорий и групп должностей государственной гражданской службы и функциональным обязанностям государственных служащих.

Заключение. Подводя итог, можно констатировать поступательное развитие процесса цифровизации государственной службы, при котором внедрение цифровых технологий в государственно-служебную деятельность значительно опережает развитие правовой базы в данной сфере. Вместе с тем говорить об осуществлении цифровой трансформации государственной службы пока рано: кадровая система государственной службы регламентирована и лишена гибкости, это не позволяет ей быстро реагировать на динамичные изменения. В этих условиях многие направления применения цифровых технологий в государственном управлении реализуются в экспериментальном режиме, по итогам применения которого будет оценена их эффективность, проведена доработка правового обеспечения применения цифровых технологий на государственной службе.

Нельзя забывать о том, что использование цифровых технологий в системе государственной службы создает и новые риски правам человека, новые угрозы, в том числе коррупционной направленности, что требует соблюдения баланса между правовым регулированием и внедрением цифровых инноваций. Кроме того, эффективность государственно-служебной деятельности зависит не только от применения цифровых технологий, не менее важное значение по-прежнему имеют правовая политика, идеология и правовая культура.

Список литературы

1. Указ Президента РФ от 01.02.2005 № 112 «О конкурсе на замещение вакантной должности государственной гражданской службы Российской Федерации» // Собрание законодательства РФ. 2005. № 6. Ст. 439; 2023. № 18. Ст. 3297.

2. Указ Президента РФ от 31.08.2020 № 536 «Об утверждении Положения о порядке организации экспериментов, направленных на развитие федеральной государственной гражданской службы» // Собрание законодательства РФ. 2020. № 35. Ст. 5555.

3. Указ Президента РФ от 25.04.2022 № 232 «О государственной информационной системе в области противодействия коррупции «Посейдон» и внесении изменений в некоторые акты Президента Российской Федерации» // Собрание законодательства РФ. 2022. № 18. Ст. 3053; 2023. № 27. Ст. 4980.

4. Постановление Правительства РФ от 03.03.2017 № 256 «О федеральной государственной информационной системе «Единая информационная система управления кадровым составом государственной гражданской службы Российской Федерации» // Собрание законодательства РФ. 2017. № 11. Ст. 1573.

5. Постановление Правительства РФ от 15.08.2019 № 1056 «О едином специализированном информационном ресурсе, предназначенном для профессионального развития государственных гражданских служащих Российской Федерации» // Собрание законодательства РФ. 2019. № 34. Ст. 4890.

6. Постановление Правительства РФ от 18.03.2023 № 413 «О проведении эксперимента по использованию электронных документов в кадровой работе отдельных федеральных органов исполнительной власти» // Собрание законодательства РФ. 2023. № 13. Ст. 2270.

7. Дорожная карта по реализации основных направлений развития государственной гражданской службы Российской Федерации на 2019–2021 гг., утв. Распоряжением Правительства РФ от 24 июля 2019 г. № 1646-р // Собрание законодательства РФ. 2019. № 31. Ст. 4669.

8. Распоряжение Правительства РФ от 22.10.2021 № 2998-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления» // Собрание законодательства РФ. 2021. № 44 (ч. 3). Ст. 7467.

9. Единый план по достижению национальных целей развития Российской Федерации на период до 2024 года, утв. Правительством РФ 07.05.2019 № 4043п-П13.

10. Проект Постановления Правительства РФ «О проведении эксперимента по применению федеральными государственными гражданскими служащими и работниками, замещающими должности, не являющиеся должностями федеральной государственной гражданской службы, федеральных органов исполнительной власти и работниками государственных внебюджетных фондов Российской Федерации, федеральных государственных учреждений цифровых кадровых сервисов с использованием платформы «Государственные кадры» и внесении изменений в некоторые акты Правительства Российской Федерации» (по состоянию на 21.08.2023) (подготовлен Минцифры России, ID проекта 01/01/08-23/00141122).

11. Пояснительная записка к проекту Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации». URL: https://sozd.duma.gov.ru/bill/314667-8#bh_note

12. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://digital.gov.ru/ru/activity/govservices/infosystems/7/?utm_referrer=URL: https%3a%2f%2fya.ru%2f

13. Добробаба М. Б., Чаннов С. Е. Применение цифровых технологий в целях противодействия совершения дисциплинарных коррупционных правонарушений в системе государственной службы // Информационное право. 2022. № 3 (73). С. 25–30.

14. Добробаба М. Б., Чаннов С. Е. Цифровое профилирование гражданских служащих как способ повышения эффективности дисциплинарной ответственности в системе государственной службы // Юридический мир. 2022. № 11. С. 32–36.

15. Состояние и перспективы развития единой информационной системы управления кадровым составом государственной гражданской службы Российской Федерации / Т. Б. Лаврова, С. А. Еварович, А. Г. Полякова, А. А. Колесников, Л. Ю. Красивская. М., 2020. С. 84–85.

16. Филоненко В. Чиновники станут летать в гособлаках. URL: https://www.pnp.ru/politics/chinovniki-stanut-letat-v-gosoblakakh.html

17. Цирин А. М., Артеменко Е. А. Цифровые технологии и искусственный интеллект как средства профилактики проявлений коррупции в контрольной (надзорной) деятельности: отечественный и зарубежный опыт // Журнал российского права. 2023. № 3. С. 126–142.

18. Шадрина Т. В. Эксперимент по ЭКДО в органах исполнительной власти // Отдел кадров государственного (муниципального) учреждения. 2023. № 5. С. 12–16.

19. Цифровой профиль чиновника и депутата. URL: https://pred-pensioner.ru/2019/12/09/цифровой-профиль-чиновника-и-депутат

Д. А. Доротенко,
руководитель направления по международному,
партнерскому и ИТ сопровождению,
Общество с ограниченной ответственностью
«Старт.Ру»

СТАТИСТИКА ДОМЕННЫХ СПОРОВ В РОССИИ

Аннотация. Доменные споры знакомы российским арбитражным судам уже более 20 лет. За это время судам удалось разрешить много важных споров, выработать общие подходы по различным аспектам, а экономическим субъектам – заметить тенденции, научиться учитывать различные факторы в своих спорах. Несмотря на то, что российским судам пока далеко до того количества дел, которые рассматривает Центр ВОИС по арбитражу и посредничеству, тем не менее уже сейчас можно говорить, что судебные дела по такой категории споров уже представляют собой ценный объект изучения для статистики, эконометрики и юридического анализа.

Ключевые слова: доменные споры, судебная статистика, арбитражное судопроизводство, цифровые технологии, базы данных, Kardamon

STATISTICS OF DOMAIN DISPUTES IN RUSSIA

Abstract. Domain disputes have been familiar to Russian arbitration courts for more than 20 years. During this time, the courts have resolved many important disputes, developed common approaches on various aspects, whereas economic entities have managed to notice trends, learn to take into account various factors relevant to their disputes. Despite the fact that Russian courts are still far from the number of cases that resolved by the WIPO Arbitration and Mediation Center, nevertheless, it can be said that court cases of domain disputes already represent a valuable object of study for statistics, econometrics and legal analysis.

Keywords: domain disputes, trademarks, judicial statistics, arbitration proceedings, digital technologies, databases, Kardamon

Введение. Доменные споры знакомы российским арбитражным судам уже более 20 лет. Так, относительно недавно мы с интересом узнавали о деталях рассмотрения спора Высшим Арбитражным Судом Российской Федерации в отношении доменного имени kodak.ru. Однако этому «недавно» уже 22 года [10]. За это время количество доменных споров в России, рассматриваемых арбитражными судами, уверенно вышло на уровень десятков дел ежегодно (рис. 1, период 2011–2019 гг.). За эти два десятилетия мы успели понять, что доменное имя не является результатом интеллектуальной деятельности и средством индивидуализации [8], но при этом выполняет функцию своеобразного средства индивидуализации [13] (которое интеллектуальной собственностью все же является [2]). Такие вот они, противоречивые и непростые доменные споры.

Очевидно то, что доменные споры в рамках системы арбитражных судов России – это одна из надводных частей айсберга доменных споров, связанных с российскими экономическими субъектами. Так, к иным его частям относимы, например, судебные споры в рамках системы российских судов общей юрисдикции; споры, рассмотренные Центром ВОИС по арбитражу и посредничеству [1]; многочисленные иные претензии и споры, которые были урегулированы сторонами конфликтов в рамках досудебного урегулирования.

За эти два десятилетия мы с вами непрестанно наблюдаем, в частности, за попытками привлечь к ответственности регистраторов доменных имен (которые, при этом, не выполняют одновременно услуги хостинга для своих клиентов) в качестве соответчиков, которые, при этом, не завершаются успехом для истцов (если считать критерием успеха взыскание компенсаций с регистраторов) [11, 12].

Доменные споры как категория судебных споров представляет собой особый интерес и для экономических субъектов, и для профессионального юридического сообщества, свидетельством чего являются различные обзоры дел [3, 5. С. 68–72], сообщения в СМИ [10], исследования [4. С. 192–206, 7].

Автор статьи, интересуясь данной категорией споров, разработал собственную базу данных доменных споров в России (“Kardamon”), благодаря чему открывается путь к статистическому и более полноценному юридическому анализу таких споров (и не только к этому). Пускай это лишь часть вышеупомянутого айсберга, но весомая часть.

Цель настоящей статьи – обратить внимание на данную категорию судебных споров в России, привлечь к дискуссии представителей экономических субъектов и представителей профессионального сообщества, а также поделиться некоторыми наблюдениями и выводами, которые удалось сделать автору в ходе разработки вышеуказанной базы данных.

Хронология доменных споров. Вышеупомянутый спор по домену kodak.ru является одним из знаковых доменных споров начального периода таких дел в России. Автор предлагает выделить всего три таких периода:

1) первый период – до 01.01.2008 года (даты вступления в силу Гражданского Кодекса (части четвертой)) [19],

2) второй период – с 01.01.2008 до 31.12.2017 (десятилетний период),

3) третий период – с 01.01.2018 по настоящее время.

Автору не удалось к моменту публикации настоящей статьи обнаружить в открытом доступе официальную статистику по доменным спорам в России, разрешенных арбитражными судами. Поэтому нижеследующие статистические сведения позволяют говорить именно о минимальных значениях и числах, относимых к доменным спорам за все три вышеуказанных периода.

Общее количество доменных споров. За весь период наблюдения за доменными спорами удалось установить, что всего в России с 2001 по 2021 годы арбитражными судами было рассмотрено 430 судебных дел. Если обратить внимание на статистику дел в хронологическом порядке (беря за основу подсчета количество дел по доменным спорам за каждый календарный год, в который было инициировано судопроизводство по таким делам), то картина видится следующей (рис. 1):

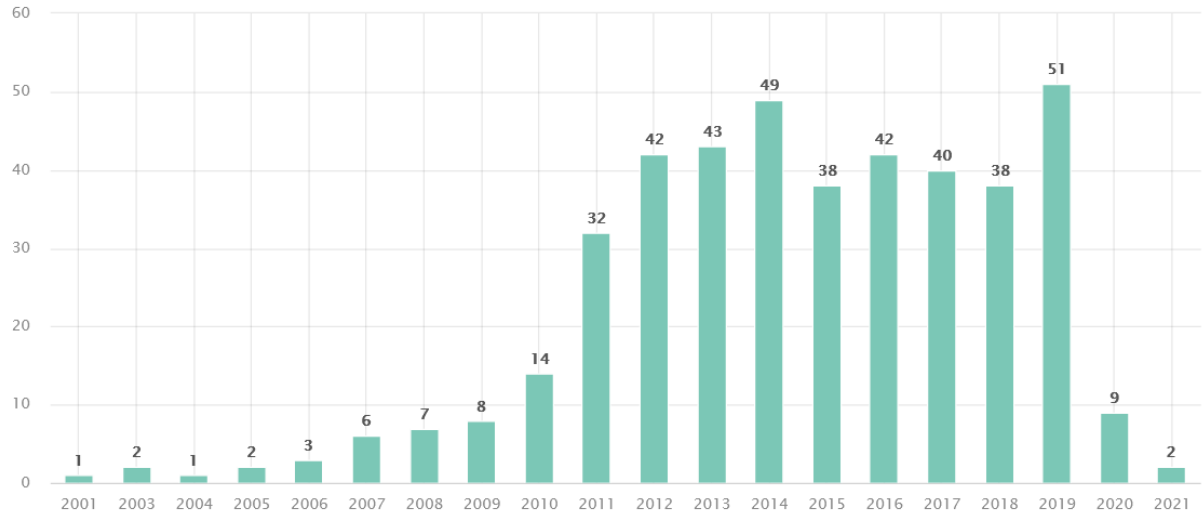

Рис. 1. Общее количество доменных споров (по годам начала судопроизводств по ним)

Если мы желаем узнать в таком же, хронологическом, порядке сведения о количестве завершенных доменных споров (с любым решением суда по делам), то такие сведения мы можем получить из следующей иллюстрации (рис. 2):

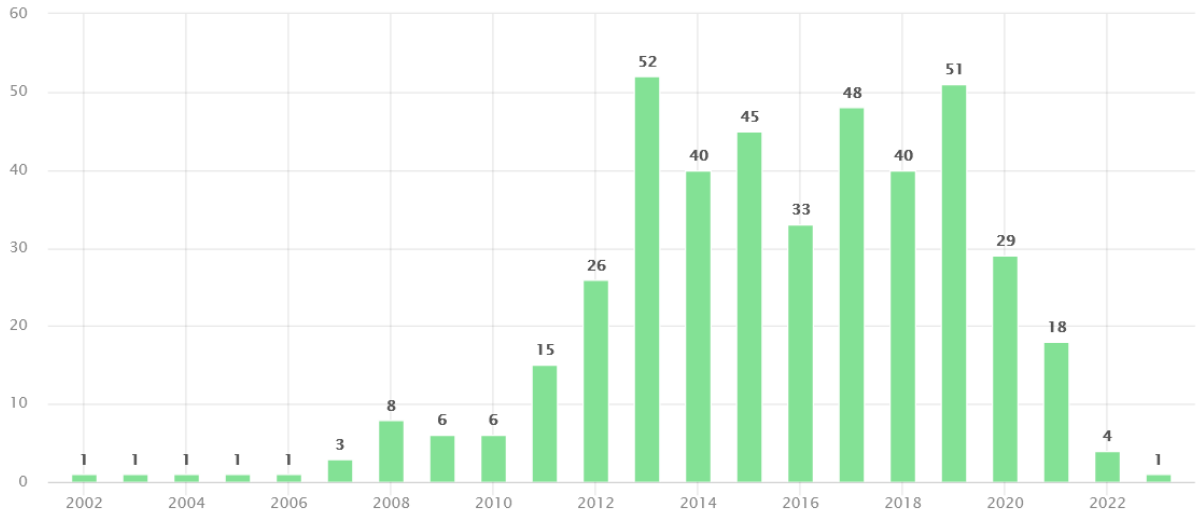

Рис. 2. Общее количество доменных споров (по годам завершения судопроизводств по ним)

Из этих двух графиков автор предлагает сделать следующие выводы:

1. Это не абсолютное количество всех дел, рассмотренные судами в РФ по доменным спорам в виду ряда причин (в частности, насколько это известно автору, отсутствие официальной судебной статистики по доменным спорам в России). Но это минимальное количество известных дел.

2. Зафиксирован уверенный рост количества судебных дел по доменным спорам в России с 2004 по 2014 гг. На спад количества дел в 2020-х гг. автор предлагает

не обращать внимание, так как далеко не все дела за этот период исследованы автором к моменту публикации статьи.

3. Больше всего судебных делопроизводств по доменным спорам было начато в 2013, 2014 и 2019 гг. (43, 49 и 51 соответственно) (рис. 1), в то время как больше всего споров было разрешено арбитражными судами в 2017, 2019, 2013 гг. (48, 51 и 52 соответственно) (рис. 2).

4. На протяжении 9 лет (с 2011 по 2019 гг.) суды рассматривали не менее тридцати судебных дел по доменным спорам ежегодно.

В первый период было инициировано 15 доменных споров, во второй период – 315 споров, в третий период – (пока что) 140 споров.

Количество спорных доменных имен. За тот же период наблюдения за доменными спорами в России удалось определить, что в указанных 430 судебных делах по доменным спорам 557 доменных имен стали объектами споров. При этом, если смотреть статистику о среднем количестве доменных имен в одном иске (в том же хронологическом порядке), она будет следующей (рис. 3):

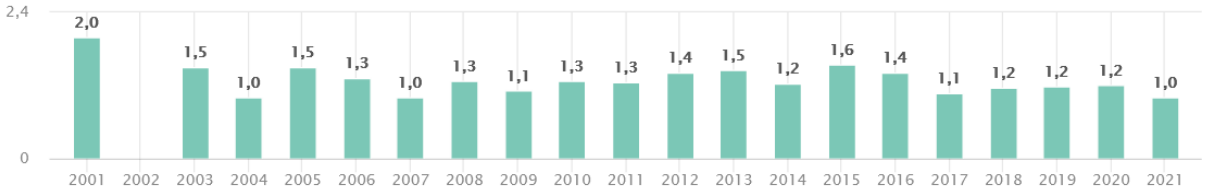

Рис. 3. Среднее количество доменных имен в одном иске (по годам начала судопроизводств по доменным спорам)

Более интересным видятся сведения о том, какое количество доменных имен (объектов споров) было максимальным в исках по такой категории дел. Такие сведения у автора имеются, они представлены ниже в том же хронологическом порядке на следующей иллюстрации (рис. 4):

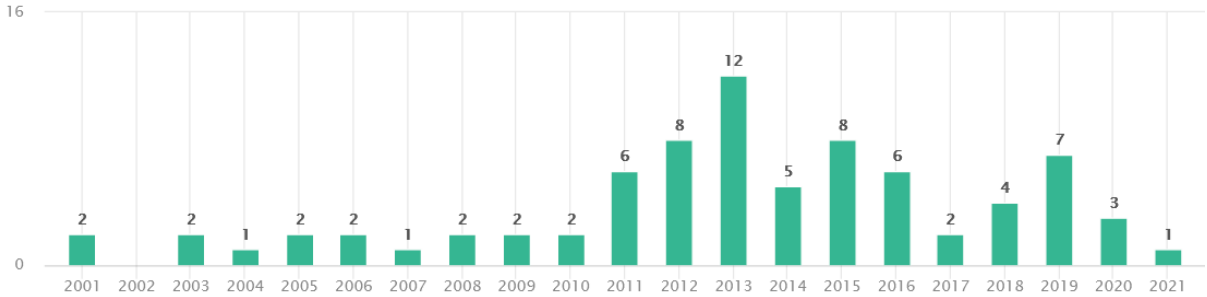

Рис. 4. Максимальное количество доменных имен в одном иске (по годам начала судопроизводств по доменным спорам)

На этом графике по каждому году (столбцу) указано максимальное количество доменных имен (ставших объектами спора), которое каждый истец указывал в своем иске. Если в конкретный год было более одного дела, в котором было

равное (максимальное) количество спорных доменных имен, то в графике такое количество доменных имен не суммируется (а показывается такое максимальное количество, без учета того, в каком количестве исков оно было за соответствующий год).

Из этой пары графиков автор предлагает сделать следующие выводы:

1. Сведений за 2002 год графики не содержат, так как в базе данных автора отсутствуют судебные дела, рассмотрение которых было инициировано в 2002 году (рис. 1).

2. Несмотря на то, что наибольшее значение среднего количества доменных имен зафиксировано в 2001 году (2,0), это нивелируется тем, что общее количество доменных споров, начатых в 2001 году и исследованных автором – всего одно дело [6]. Поэтому будет нагляднее отметить, что чаще всего средним количеством доменных имен (объектов споров) является значение в 1,2 шт., указанных в одном иске – так было 4 раза, в 2014, 2018-2020 гг. (рис. 3). При том, что в 2019 году всего было инициировано более 50 судопроизводств по доменным спорам (рис. 1).

3. Если максимальное количество доменных имен, указанных в исковых требованиях, в годы первого периода не превышали 3 шт., то второй период отметился ростом такого количества (более половины лет этого периода максимальное значение превышало 5 шт.).

Доменные зоны спорных доменных имен. Говоря о доменных спорах, некоторые читатели могут полагать, что в России суды рассматривают доменные споры только по доменным именам, зарегистрированным в доменной зоне .RU. Однако это не так. Российская судебная практика знает доменные споры по доменным именам и в иных доменных зонах. Ниже предлагаются на рассмотрение примеры, позволяющие развеять такое заблуждение (табл. 1):

Таблица 1

Примеры спорных доменных имен различных доменных зон, ставших объектами доменных споров в России

Спорные доменные имена	Их доменные зоны	Реквизиты судебных дел
тиссан.рф	РФ	№ А65-26240/2015
ombrello.me	ME	№ А41-17765/12
bonduelle.ru	RU	№ А40-131093/2013
sberbank.org, sberbank.biz	ORG, BIZ	№ А40-140236/10-51-1189
burgerking.su, burger-king.su	SU	№ А40-154813/12

Более того, в распоряжении автора имеется расширенная статистика по доменным зонам спорных доменных имен. Так, за все три периода самыми популярными доменными зонами (в которых были зарегистрированы спорные доменные имена), стали следующие (рис. 5):

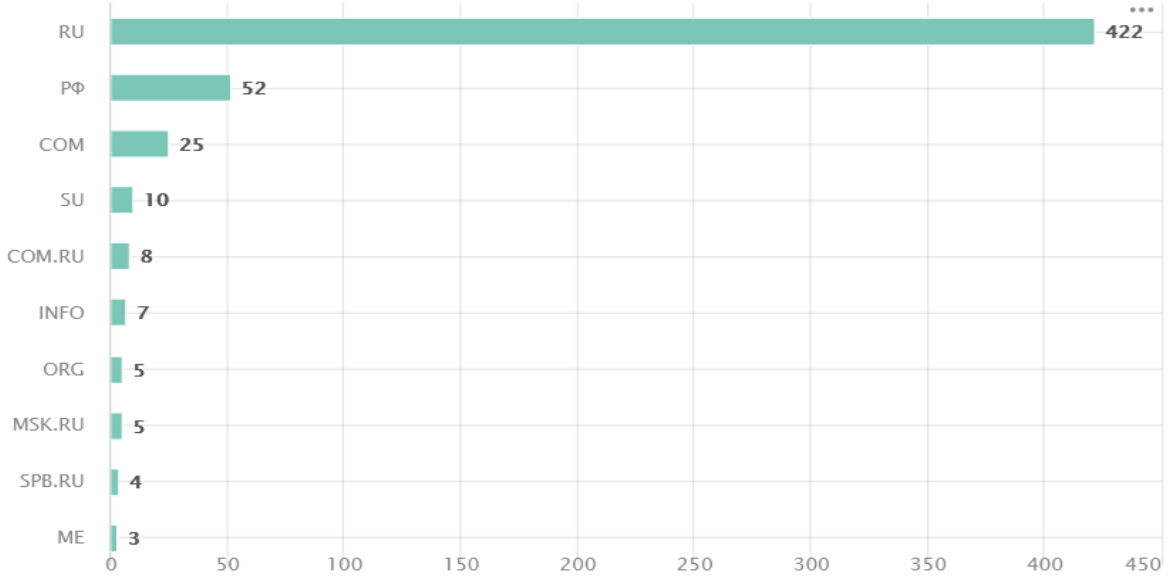

Рис. 5. Доменные зоны спорных доменных имен (по всем исследованным искам, за все периоды)

На этом графике нижняя ось (числовые значения) отображает количество доменных имен, зарегистрированных в соответствующей доменной зоне, которые стали объектами доменных споров в тех делах, которые были исследованы автором. Так, например, если в доменной зоне .ME стоит значение «3», это значит, что за весь период наблюдения (с 2001 по 2021 гг.) автору удалось идентифицировать три доменных имени в этой зоне, которые стали объектами доменных споров (сведения об одном из них – доменному имени ombrello.me – см. выше, табл. 1).

Эта иллюстрация позволяет нам сделать следующие выводы:

1. Абсолютное большинство объектов споров – более 75 % от общего количества – составляют доменные имена, зарегистрированные в доменной зоне .RU. Эта зона остается неизменным лидером в этом аспекте, совокупное количество доменных имен (спорных объектов) в которой превышает совокупное количество спорных доменных имен во всех других доменных зонах (вместе взятых) в несколько раз. Таким образом, каждые 3 из 4 спорных доменных имен, в отношении которых есть судебное делопроизводство – это доменные имена, зарегистрированные в зоне .RU.

2. На втором месте (с отрывом от лидера этого рейтинга более, чем в 8 раз) – кириллическая доменная зона .РФ. Несмотря на то, что открытая регистрация доменных имен в этой зоне началась 11.11.2010 [18] – ближе к середине второго периода исследования, немногим больше, чем за 10 лет, она по количеству спорных доменных имен сумела обойти интернациональную доменную зону .COM (третье место), которая остается самой популярной у владельцев доменных имен во всем мире. [14] Такой статистический факт может косвенно подтверждать популярность этой доменной зоны в России и интерес к ней экономических субъектов.

3. Еще одна российская доменная зона – .SU [9] – также в топ-5 доменных зон, где зарегистрированы наибольшее количество спорных доменных имен.

Примеры доменных имен, зарегистрированных в этой доменной зоне, также есть выше (табл. 1).

4. Примечательно, что общее количество доменных имен (не объектов спора, а всего зарегистрированных) в зоне .РФ [15] приблизительно в 6 раз больше, чем в зоне .SU [17] – и количество спорных доменных имен в той же первой зоне больше, чем во второй зоне примерно в том же соотношении. Примерно такая же картина и с соотношением доменных имен в зонах .RU и .РФ: в зоне .RU доменных имен больше в 7,2 раза [16], а спорных доменных имен – примерно в 8 раз.

5. Российская судебная практика решает доменные споры не только в отношении доменных имен второго уровня (например, тиссан.рф, bonduelle.ru – табл. 1), но и в отношении доменных имен третьего уровня. Об этом свидетельствуют доменные зоны .COM.RU, .MSK.RU, .SPB.RU, вошедшие в число доменных зон с наибольшим количеством выявленных в них спорных доменных имен.

Говоря о вышеуказанном выводе (5), стоит отметить, что по собственным сведениям автора, доля доменных споров по доменным именам 3-го уровня (по отношению к общему количеству исследованных автором доменных споров) составляет 4,7 %. То есть, примерно каждое двадцатое спорное доменное имя – это доменное имя третьего уровня (например, условное domain.msk.ru).

Автор подготовил следующую статистику по вышеуказанным параметрам с группировкой по указанным временным периодам исследования (табл. 2).

Таблица 2

Совокупная статистика по вышеуказанным параметрам доменных споров в России (по периодам)

Параметр Первый (до 2008 г.)		**Исследуемые периоды**			**Всего**
		Первый (до 2008 г.)	**Второй (2008-2017 гг.)**	**Третий (2018 – н. в.)**	
Общее количество доменных споров, принятых к рассмотрению судами		15	315	100	430
Общее количество доменных споров, производство по которым судами завершено		8	271	143	430
Среднее количество спорных доменных имен (в одном иске)		1,3	1,3	1,2	
Максимальное количество спорных доменных имен в одном иске)		2	12	7	
Доменные зоны	.RU	20	312	90	422
	.РФ	0	48	4	52
	.COM	0	19	6	25
	.SU	0	8	2	10
	.COM.RU	0	2	6	8

Следует обратить внимание, что значения на рис. 5 и в табл. 2 (по строкам «Доменные зоны», в столбце «Всего») должны совпадать.

Автор также подготовил статистику по вышеуказанным параметрам с группировкой по указанным временным периодам исследования, связанную с деятельностью Суда по интеллектуальным правам и Высшего Арбитражного Суда Российской Федерации (табл. 3).

Таблица 3

Совокупная статистика по вышеуказанным параметрам доменных споров в России (в периоды ВАС РФ, СИП РФ)

Параметр		Исследуемые периоды			
		СИП РФ		ВАС РФ	
		До начала работы	В период работы	В период работы	После упразднения
Общее количество доменных споров, принятых к рассмотрению судами		99	331	148	274
Общее количество доменных споров, производство по которым судами завершено		99	331	189	241
Среднее количество спорных доменных имен (в одном иске)		1,2	1,3	1,3	1,3
Максимальное количество спорных доменных имен (в одном иске)		2	12	12	8
Доменные зоны	.RU	88	334	151	271
	.РФ	15	37	19	33
	.COM	1	24	8	17
	.SU	2	8	4	6
	.COM.RU	0	8	0	8

Следует обратить внимание, что совокупные значения в табл. 3 (по первым двум строкам табл. 3) определяются только по столбцам одной группы («СИП РФ» и «ВАС РФ» соответственно). Так, например, сумма значений параметра «Общее количество доменных споров, принятых к рассмотрению судами» группы «СИП РФ» равна 430 (что соответствует соответствующему значению в столбце «Всего» таблицы 2).

Также следует обратить внимание, что в табл. 3 отражены не сведения о делах, которые рассмотрены исключительно Судом по интеллектуальным правам или Высшим Арбитражным Судом Российской Федерации, но всеми судами в рамках системы арбитражных судов Российской Федерации (судебные дела которых стали предметом исследования автором).

Таким образом, судя по данным табл. 3, в период работы СИП РФ (по настоящее время) российские арбитражные суды рассмотрели доменных споров в 3,3 раза

больше, чем до его начала работы; и в 1,3 раза больше, чем во время работы ВАС РФ.

Также примечательно, что доменные споры в отношении доменных имен доменной зоны .COM.RU, становились объектами споров уже после упразднения ВАС РФ.

Заключение. Приведенные выше данные позволяют говорить о том, что доменные споры – вполне активная категория споров на протяжении многих лет в России, хорошо знакомая арбитражным судам (как до начала работы СИП РФ, так и после упразднения ВАС РФ). Эта категория споров была в стадии активного роста их количества более, чем 10 лет (с 2004 по 2014 гг., рис. 1). При этом, автор не наблюдает спад общего количества таких дел в последние годы – снижение количества дел в 2015–2018, 2020–2021 гг. (рис. 1) можно объяснить тем, что многие споры пока еще не исследованы (и не занесены в вышеуказанную базу данных автора, фрагменты сведений из которой приведены в настоящей статье).

Автор надеется на то, что вышеприведенные сведения помогут взглянуть по-новому на доменные споры и узнать дополнительные сведения о них, неизвестные ранее. Дополнительную аналитику по доменным спорам в России автор планирует предоставить в последующих публикациях.

Список литературы

1. Альтернативное урегулирование споров. URL: https://www.wipo.int/amc/ru
2. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ. URL: https://www.consultant.ru
3. Доротенко Д. «Культурные» доменные споры. URL: https://dorotenko.pro/ru/domain-disputes-theatres
4. Доротенко Д. А. Такие разные доменные споры. О компенсациях // Вестник экономического правосудия Российской Федерации. 2019. № 10. С. 192–206.
5. Малахов Б. А., Власов Р. Б. Изменение критериев подведомственности доменных споров Верховным Судом // Журнал Суда по интеллектуальным правам. 2019. № 23. С. 68-72.
6. Определение Федерального арбитражного суда Московского округа от 01 апреля 2002 г. по делу № Ф05-1288/2002. URL: https://kad.arbitr.ru/Card/8a520678-a655-45b8-b47e-59d0d3781dfe
7. Попцов А. В. Правовое регулирование доменного имени в Российской Федерации: автореф. дис. ... канд. юрид. наук. URL: https://search.rsl.ru/ru/record/01003481902
8. Постановление Пленума Верховного Суда Российской Федерации от 23 апреля 2019 г. № 10 «О применении части четвертой Гражданского кодекса Российской Федерации». URL: https://rg.ru/documents/2019/05/06/postanovlenie-dok.html
9. Постановление Пленума Верховного Суда Российской Федерации от 27 июня 2017 г. № 23 «О рассмотрении арбитражными судами дел по экономическим спорам, возникающим из отношений, осложненных иностранным элементом». URL: https://rg.ru/documents/2017/07/04/verhsud2-dok.html

10. Рассмотрение дела о домене Kodak.Ru начинается заново, с учетом рекомендаций ООН. URL: https://lenta.ru/news/2001/01/17/kodak

11. Решение Арбитражного суда города Москвы от 09 декабря 2010 года по делу № А40-19126/10-12-118. URL: https://clck.ru/36ovPP

12. Решение Арбитражного суда города Москвы от 31 мая 2019 года по делу № А40-138291/18-105-733. URL: https://clck.ru/36ovQp

13. Решение Арбитражного суда Чувашской республики – Чувашии от 06 марта 2013 года по делу № А79-10130/2012. URL: https://clck.ru/36ovRo

14. Самые популярные домены и доменные зоны – исследование Serpstat. URL: https://clck.ru/36ovSM

15. Сводный отчет (.РФ). Домены России. URL: https://statdom.ru/tld/рф/report/summary

16. Труханов А. Открылась регистрация доменных имен в зоне «.РФ». URL: https://clck.ru/36ovT2

17. Федеральный закон «О введении в действие части четвертой Гражданского кодекса Российской Федерации». URL: http://pravo.gov.ru

А. К. Дубень,
кандидат юридических наук,
Институт государства и права
Российской академии наук

ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В современных условиях трансформации экономики, цифровизации права изменен подход к развитию промышленности в пользу обеспечения технологического суверенитета, а также правового обеспечения информационной безопасности в рамках межгосударственного сотрудничества. Усиление давления со стороны зарубежных хакерских группировок, увеличение масштаба компьютерных атак на российскую инфраструктуру разработчиков программ и оборудования способствовало актуализации данной темы в доктрине международного и информационного права. По результатам данного исследования автор делает вывод, что укрепление межгосударственного сотрудничества Российской Федерации с иностранными государствами по вопросам, касающимся технологического сотрудничества в области безопасности в информационной сфере, является важным направлением по укреплению международной и национальной безопасности.

Ключевые слова: информационная безопасность, государственная политика, международное право, информационное право, международная информационная безопасность, международные организации, межгосударственное сотрудничество

PRIORITY DIRECTIONS OF LEGAL PROVISION OF INFORMATION SECURITY OF THE RUSSIAN FEDERATION

Abstract. In modern conditions of economic transformation, digitalization of law, the approach to industrial development has been changed in favor of ensuring technological sovereignty, as well as legal provision of information security within the framework of interstate cooperation. Increased pressure from foreign hacker groups, an increase in the scale of computer attacks on the Russian infrastructure of software and equipment developers contributed to the actualization of this topic in the doctrine of international and information law. Based on the results of this study, the author concludes that strengthening interstate cooperation of the Russian Federation with foreign states on issues related to technological cooperation in the field of information security is an important direction for strengthening international and national security.

Keywords: information security, state policy, international law, information law, international information security, international organizations, interstate cooperation

В настоящее время правовое обеспечение информационной безопасности, включая цифровую безопасность Российской Федерации, национальную кибербезопасность и сетевую безопасность, является не просто актуальной, а приоритетной и одной из ключевых, стратегических задач, обеспечиваемой как на национальном, так и международном уровне. Национальная информационная безопасность касается, по сути, каждого человека, личности, устанавливает безопасность функционирования организаций, общественных и иных объединений в социальном, экономическом, организационном плане, а также детерминирует состояние и перспективы развития России, что определяет значение проблем и перспектив правового обеспечения данной сферы. Факторы правового обеспечения безопасности в современном мире – это не только ценности, провозглашенные в международных правовых актах и национальных стратегических и нормативных документах, но и реализация правовых норм, закрепленных в Основном законе государства – Конституции Российской Федерации, в федеральных законах и нормативных правовых актах субъектов России, которые развиваются в подзаконных нормативных правовых актах, а также и детерминанты будущего устройства мирового порядка с учетом происходящих в мире и России изменений [1].

Правовое обеспечение безопасности в информационной сфере имеет значение как ценность человеческого общения, устойчивого и поступательного развития государств, регионов и мира в целом, которая формируется сегодня в непростое время становления многополярного мира и цифровой трансформации государства и общества. Экспоненциальное развитие цифровых, конвергентных, сквозных, прорывных технологий (сегодня их количество и качество активно увеличивается), а по сути – различных видов информационных технологий, приносит нам, несомненно, много полезного и порой жизненно необходимого, но, как было рассмотрено выше, несет и колоссальные риски, угрозы и вызовы [2. С. 158].

В настоящее время стратегически важно обеспечение информационной безопасности правовыми средствами на всех уровнях в рамках информационно-правового

регулирования и правоприменения, что определяет основные векторы исследований, совершенствования законодательства и изменение государственной информационно-правовой политики.

Вместе с тем современная национальная система правового обеспечения информационной безопасности в Российской Федерации, включая правовое регулирование, пока не в полной мере соответствует вызовам и рискам современности, в целом развивается недостаточно системно, без учета особенностей деятельностного характера средств и методов защиты информации, включая и экспериментальные правовые режимы в сфере цифровых инноваций. Это характерно, в том числе для реализации правовых составляющих в национальных проектах и программах, многочисленных концептуальных документах, связанных с информационной сферой.

Следует признать, что внесение изменений и дополнений в законодательство в рассматриваемой сфере происходит в основном пока без учета научно обоснованных концепций. Примерами могут служить и формирование правовых средств достижения цифрового пространства доверия, идентификация и аутентификация в информационно-коммуникационной сфере, юридическая значимость электронных документов, развитие системы «цифрового профиля» и различных государственных учетных систем – регистров реестров, включая и регистр населения, применение в системе государственного управления облачных технологий и цифровых платформ.

В настоящее время имеются определенные сложности регулирования применения облачных технологий, цифровых платформ, включая государственную систему правовой информации, имеющих правовое значение аспектов применения интернета вещей, больших данных, систем распределенного реестра. Особую значимость приобретает правовое регулирование внедрения объектов, использующих в своем функционировании технологии искусственного интеллекта. Значительную сложность представляет правовое обеспечение развития квантовых технологий, включая риски внедрения квантовой криптографии. В каждом случае требуется специальное правовое осмысление в целях обеспечения безопасности внедрения таких технологий и охраны конституционно значимых ценностей при их применении [3. С. 110].

В этой связи отдельное внимание следует обратить на законодательные изменения и усиление роли информационной безопасности во всех сферах жизнедеятельности. Проблема защищенности персональных данных от несанкционированного доступа имеет приоритетное значение, поскольку широкое распространение получили сервисы в сети Интернет, занимающиеся противоправным оборотом персональных данных. Государство реагирует на данные угрозы посредством внесения изменений в законодательство. Так, Федеральный закон от 14 июля 2022 г. № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу ч. 14 ст. 30 Федерального закона «О банках и банковской деятельности» усиливает защиту прав субъектов персональных данных путем введения дополнительной обязанности операторов незамедлительно информировать

уполномоченные государственные органы об инцидентах с принадлежащими им базами персональных данных, а также надлежаще обеспечивать сотрудничество на постоянной основе с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России, в том числе внесены поправки об обязательном уведомлении Роскомнадзора об обработке личной информации работников и контрагентов оператора [4]. Вводится экстерриториальность применения российского законодательства о персональных данных путем возможности вмешательства уполномоченных органов власти в вопросы обработки персональных данных российских граждан на территории других государств.

Активное применение персональных данных в информационном пространстве, специфика их различных видов также представляет серьезные угрозы информационной безопасности личности в части неправомерного их использования. Противодействие таким угрозам является важной не только национальной задачей, заслуживает продолжения фундаментальных исследований. В настоящее время так называемыми недружественными странами ведется активный сбор геномной информации, исследование возможности применения данных о геноме человека в военно-политических целях для осуществления воздействия на определенные этнические группы населения. Это и многое иное в очередной раз актуализирует необходимость усиления защиты персональных данных физических лиц, включая развитие самостоятельного института геномной информации.

В целях обеспечения защиты конституционных прав и свобод граждан в Стратегии национальной безопасности Российской Федерации содержится определение понятия «национальная безопасность», под которой понимается состояние защищенности национальных интересов РФ от внешних и внутренних угроз [5]. Очевидно, что гарантии этих прав и свобод в информационной сфере напрямую связаны с обеспечением информационной безопасности граждан и социальных групп населения. В связи с этим доктринальное понятие «информационная безопасность» в современных условиях развития информационных технологий, повышения требований по защите информации, кибербезопасности не является статичным и уже нуждается в уточнении и модернизации, особенно в связи с новыми задачами обеспечения стратегической стабильности в современных условиях геополитической нестабильности. Между тем, данная редакция Стратегии национальной безопасности Российской Федерации должна коррелироваться со всеми нормативными правовыми актами стратегического планирования как с базовым документом, так и локальными актами. Это касается в первую очередь и Доктрины информационной безопасности Российской Федерации 2016 г. [6].

Согласно п. 2 Доктрины информационной безопасности Российской Федерации безопасность в информационной сфере имеет приоритетный характер в информационной среде посредством правового регулирования в сети Интернет, сетей связи, критически важных объектов, информационных технологий и систем. Кроме этого, информационная безопасность определяет правила поведения для субъектов, деятельность которых связна с получением, хранением и обработкой информации, развитием информационных технологий.

Следует признать, что стратегическое значение правового обеспечения информационной безопасности подтверждается целым рядом документов федерального уровня, утвержденных указами Президента Российской Федерации, имеющих базовое значение на современном этапе развития общества и государства [7]. Эти документы являются базовыми в системе документов стратегического планирования, требуют научного осмысления с позиции информационного права, поскольку сегодня в эпоху активных процессов цифровой трансформации.

В настоящее время в связи с событиями в мире и возможностью удаленного информационного воздействия на правосознание и миропонимание людей значительно актуализировался вопрос обеспечения достоверности информации как основы осуществления деятельности в информационной сфере и формирования системы правомерных действий различных лиц. Сегодня наблюдается использование разнообразных механизмов неправомерного ограничения доступа граждан к социально значимой информации, в том числе в системе официальных взглядов в Российской Федерации на особенности национальных интересов и порядка их обеспечения.

Таким образом, из проведенного исследования следует отметить, что в целях реализации государственной политики в информационной сфере необходимо определить предметную область российского законодательства и выстроить целостную систему в области обеспечения информационной безопасности. Полагаем, что основными направлениями реализации государственной информационной политики являются: гарантия и реализация конституционных прав человека и гражданина; безопасность информационных сетей; недопущение уязвимости информационных систем; развитие и совершенствование информационной инфраструктуры; дальнейшее межгосударственное сотрудничество по вопросам информационной безопасности и защиты информации.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.). URL: https://www.pravo.gov.ru

2. Камалова Г. Г., Полякова Т. А. Развитие системы принципов информационного права в цифровой среде // Право цифровой среды: монография / под ред. Т. П. Подшивалова, Е. В. Титовой, Е. А. Громовой. М.: Проспект, 2022. С. 157–164.

3. Архипов В. В., Наумов В. Б. Теоретико-правовые вопросы охраны прав человека при использовании биометрических данных системами искусственного интеллекта: европейский опыт // Вестник Удмуртского университета. Серия Экономика и право. 2022. Т. 32, № 1. С. 109–118.

4. Федеральный закон от 14.07.2022 г. № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности»» // Собрание законодательства Российской Федерации. 2022. № 29 (ч. 3). Ст. 5233.

5. Указ Президента Российской Федерации от 02.04.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2021. № 27 (ч. 2). Ст. 5351.

6. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

7. Указ Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2022. № 18. Ст. 3058.

Дэн Шэминь,
доктор юридических наук, профессор,
Уханьский университет

ВЫЗОВ И ОТВЕТНЫЕ МЕРЫ АВТОРСТВА ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ СИСТЕМЫ РАЦИОНАЛЬНОГО ИСПОЛЬЗОВАНИЯ

Аннотация. Процесс обучения и создания ИИ требует использования большого количества данных и материалов, в том числе произведений, охраняемых авторским правом, и такое использование противоречит «автоцентризму» и «трехступенчатому тесту» в рамках действующего режима авторского права. В эпоху «после автороцентризма» необходимо пересмотреть соотношение между охраной авторских прав и добросовестным использованием, а также поднять добросовестное использование до того же статуса, что и охрана авторских прав. Сфера добросовестного использования должна быть расширена, чтобы включить использование произведений с целью изучения и создания ИИ в режим добросовестного использования.

Ключевые слова: искусственный интеллект, глубокое обучение, добросовестное использование

CHALLENGES AND RESPONSES OF AI CREATION TO THE RATIONAL USE SYSTEM

Abstract. The learning and creation of Artificial intelligence (AI) uses a large number of data materials including copyrighted works. With the advent of the era of “post-authorism”, copyright protection and fair use should be reconstructed to elevate them to the same status. The use of copyrighted works by AI learning and creation can be included in the scope of fair use by expanding the scope of it.

Keywords: Artificial intelligence (AI), Deep learning, Fair use

Введение. Искусственный интеллект широко используется для написания стихов, песен, картин, а также сценариев и газетных репортажей; различные

технологические компании «обучают» искусственный интеллект языку, новостям и связанным с ними аспектам, вводя большое количество информации в базу данных, чтобы он мог получать новые сведения и улучшать свои «творческие» способности. Системы искусственного интеллекта должны использовать большие объемы данных, включая произведения, защищенные авторским правом, в процессе обучения и творчества. Является ли это использование рациональным?

Основное содержание. Конфликт между созданием искусственного интеллекта и системой рационального использования.

1. «Защиту авторских прав сосредоточить на авторе» ограничения рационального использования. В конце восемнадцатого века во Франции основной идеей «защиты авторских прав, которая должна быть сосредоточена на авторах», было следующее: произведение сочиняется автором, произведение является воплощением и продолжением личности и духа автора, поэтому автор имеет право на полный контроль над произведениями. Классическая философия Иммануила Канта и мышление личности – теоретическая основа «авторско-ориентированной защиты авторских прав». Под влиянием положения «Защита авторских прав сосредоточить на авторе» Бернская конвенция чрезмерно расширила права на воспроизведение, что, в свою очередь, привело к ограничению пространства для системы рационального использования.

1.1. Постоянное расширение права на воспроизведение под влиянием положения «защита авторских прав должна быть сосредоточена на авторах».

Бернская конвенция и последующие законодательные истории «Договора Всемирной организации интеллектуальной собственности об авторском праве» и «Договора Всемирной организации интеллектуальной собственности об исполнениях и фонограммах» показывают, что понятие «воспроизведение» расширяется. Под влиянием положения «защита авторских прав должна быть сосредоточена на авторах» концепция права на воспроизведение в Бернской конвенции была дополнительно расширена и теперь включает «все и любые» и «известные и неизвестные» методы воспроизведения.

1.2. Использование компьютеров для «ввода», «хранения» и «вывода» будет подпадать под широкие права авторов на воспроизведение.

В тысяча девятьсот семидесятых годах с распространением компьютеров «право на копирование» было истолковано как охватывающее «ввод» и «выход» в компьютерах, включая хранение работ в компьютерах. На совещании Исполнительного комитета Бернского союза в тысяча девятьсот восемьдесят втором году было рекомендовано, чтобы хранение произведений на компьютере представляло собой репродукцию. В тысяча девятьсот девяностых годах в ходе обсуждений в рамках Всемирной организации интеллектуальной собственности (ВОИС) Конвенции об авторском праве в Интернете авторы Конвенции заняли экспансионистскую позицию по вопросу о копировании. Право на копирование должно включать в себя права, связанные с размножением документов, включая цифровую форму, передачу, загрузку и создание автономной физической копии; кроме того, временное копирование также считается копией.

2. Принадлежностный статус рационального использования в традиционном законе об авторских правах. В международных конвенциях в тысяча девятьсот шестьдесят седьмом году, после принятия Бернской конвенции, защита и рациональное использование авторских прав регулируются субординацией, рациональное использование – подчиненным положением, а их содержание еще больше сужается и нарушается в результате технических недостатков законодательства и чрезмерно ограничительного толкования «трехэтапного поверочного подхода». «Трехэтапный поверочный подход» означает: (1) рациональное использование ограничивается исключительными случаями; (2) не должно противоречить нормальному использованию произведения; (3) законные интересы правообладателя не могут быть необоснованно ущемлены. Под влиянием положения «Защиты авторских прав сосредоточить на авторе» освещен статус автора, который не только пользуется обширными материальными правами, такими как воспроизведение, адаптация, сетевое сообщение и прокат, но и пользуется духовными правами на публикацию, подпись и защиту целостности произведения. Полный контроль над произведением от материального до духовного. этом контексте искусственный интеллект использует произведение авторского права в творчестве, трудно проверить с помощью трехэтапного поверочного подход.

3. Конфликт между созданием искусственного интеллекта и рациональным использованием.

3.1. Противоречие между ростом создания искусственного интеллекта и положением «Защиту авторских прав сосредоточить на авторе».

В эпоху искусственного интеллекта искусственный интеллект стал важным субъектом творчества, а теоретическая основа положения «Защита авторских прав сосредоточена на авторе» в эпоху искусственного интеллекта пошатнулась. По мере того, как искусственный интеллект будет становиться важным творцом, авторское право автора «будет сходить с алтаря», поэтому должно быть больше ограничений в законе об авторских правах. Условно говоря, следует повысить статус рационального использования и сбалансировать структуру «защиты авторских прав и рациональнного использования».

3.2. Конфликт между использованием создания искусственного интеллекта и «трехэтапным поверочным подходом».

В рамках традиционной системы авторского права использование произведений искусственного интеллекта, будь то на стадии «ввода», «хранения» или «вывода», контролируется авторским правом, который затрудняет прохождение техосмотра «трехэтапного поверочного подход». Поэтому Джервис показал, что действующий закон об авторском праве не отражает потребностей революционных цифровых технологий и является «несовершенной структурой», реформу закона об авторском праве необходимо ускорить.

4. Выбор законотворческой модели рационального использования системы в контексте искусственного интеллекта.

1. Повысить статус рационального использования.

В эпоху, когда защита авторских прав должна была быть сосредоточена на авторах, необходимо перестроить отношения между защитой авторских прав и рациональным использованием и придать разумному использованию такой же статус, как и защите авторских прав.

Во-первых, человечество больше не является единственным творческим субъектом, искусственный интеллект или сочетание модели человек – компьютер, коренным образом расшатывают основы положения «авторских прав защиты, которые должны быть сосредоточены на авторах». Искусственный интеллект при творчестве основывается на больших данных как основном материале, поэтому рациональное использование искусственного интеллекта при создании произведений должно быть признано.

Во-вторых, рациональне использование авторских произведения является важным механизмом поддержания баланса между авторами и пользователями авторского права, а рациональное использование, равно как и защита авторских прав, является одним из двух столпов авторского права.

2. Расширить сферу рационального использования: включить работы, используемые для обучения и создания искусственного интеллекта, в сферу рационального использования.

Во-первых, «входное» использование при создании искусственного интеллекта является «массовым», выходящим за рамки «незначительного использования» в традиционной системе рационального использования; во-вторых, произведение искусственного интеллекта не является «по существу похожей» на оригинальное произведение, а является новым произведением, которая не нарушает авторских прав.

3. Оптимизировать законодательную модель: принять гибкое и открытое рациональное использование.

Во-первых, статья двадцать четвертая действующего закона об авторском праве Китая перечисляет двенадцать ситуаций, что по-прежнему делает «закрытой» структурой. Такие правила все еще не могут удовлетворить потребности разработки новых технологий искусственного интеллекта. Во-вторых, ситуации, перечисленные в статье двадцать четыре закона об авторском праве, не охватывают, необходимое использование искусственного интеллекта для «обучения» и «чтения». Более того, регламентация «воспроизводение небольшого объема опубликованных произведений» полностью исключает реальное требование использования искусственным интеллектом большого количества произведений.

Во-вторых, чтобы улучшить инновационные возможности, надо разрешить работающим с искусственным интеллектом в полной мере использовать существующие материалы, редактировать и создавать больше новых банк данных. Надо содействовать развитию технологий искусственного интеллекта, снижая при этом транзакционные издержки на использование материалов, защищенных авторским правом, содействовать развитию искусственных интеллектуальных техник при одновременном снизить издержеку использования авторских материалов. В процессе оптимизации законодательных моделей рационального использования Китай должен следовать модели «трехэтапного поверочного подхода и конкретного перечисления» системы гражданского права. При пересмотре китайских «Правил реализации Закона об авторском праве» четко оговорить, что «использование для обучения и создания искусственного интеллекта» является рациональным использованием.

Список литературы

1. Васильева А. К. вопросу о наличии авторских прав у искусственного интеллекта // Журнал Суда по интеллектуальным правам. 2023. № 1.

2. Гурко А. Искусственный интеллект и авторское право: взгляд в будущее // Интеллектуальная собственность. Авторское право и смежные права. 2017. № 12. С. 7–18.

3. Ибрагимов Р., Сурагина Е. Гуманитарный подход к регулированию искусственного интеллекта // Право и экономика. 2018. № 4. С. 41.

4. Лин Сюцин. Пересмотр системы разумного использования авторских прав в эпоху искусственного интеллекта // Исследование в области юриспруденции, 2021, № 6. (на кит. яз.) Оригинальный текст: **林秀芹**：**人工智能**时代著作权合理使用制度的重塑，《**法学研究**》2021**年第6期**。

5. Цяо Хэпин. Риски авторских прав на данные и пути их разрешения в процессе создания искусственным интеллектом // Современное юриспруденция, 2022, № 4. (на кит.яз.) Оригинальный текст: **焦和平**：**人工智能**创作中数据获取与利用的著作权风险及化解路径，《当代法学》2022**年第4期**。

6. Сю Сяобэн. О разумном использовании авторских прав в глубоком обучении искусственного интеллекта // Юридические исследования транспортного университета. 2019, № 3. (на кит.яз.) Оригинальный текст: **徐小奔**：论人工智能深度学习中著作权的合理使用，《交大法学》，2019**年第3期**。

И. А. Ерофеева,
учитель,
Средняя общеобразовательная
школа № 2 г. Суздаля

ЦИФРОВАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ ОБРАЗОВАНИЯ

Аннотация. В статье рассматриваются вопросы о возможностях цифрового оборудования, применяемого в образовательных учреждениях, в связи с переходом на обновленные ФГОС (стандарты третьего поколения), о внедрении и использовании инновационных технологий в системе школьного образования, а также освещается проблема информационной безопасности в рамках школьного пространства всех участников образовательного процесса с точки зрения конфиденциальности персональных данных.

Ключевые слова: инновационные технологии, системные преобразования, информационная безопасность, современное образование, цифровые возможности, сетевое общество, компетентность

DIGITAL SECURITY IN THE EDUCATION SYSTEM

Abstract. This article discusses the possibilities of digital equipment used in educational institutions in connection with the transition to the updated Federal

State Educational Standards (third generation standards), the introduction and use of innovative technologies in the school education system, and also highlights the problem of information security within the school space of all participants in the educational process in terms of confidentiality of personal data.

Keywords: innovative technologies, system transformations, information security, modern education, digital opportunities, network society, competence

Бесспорно, наш мир постоянно меняется. Современные технологии все активнее проникают в повседневную жизнь, не обходя стороной и сферу образования. И сегодня уже сложно представить себе традиционную школу без интерактивной доски и электронного журнала, переносного ноутбука или стационарного компьютера с выходом в Интернет. Поэтому, говоря об образовании сегодня, стоит помнить о том, что, где и как, и с какими цифровыми возможностями можно организовать учебный процесс.

Несмотря на все инновации и грандиозные возможности, главной проблемой любого образовательного учреждения на сегодняшний день остается незащищенность школьников от той или иной пропаганды. Именно поэтому система информационной безопасности российских школ должна стоять на первом месте, так как от нее зависит сохранность базы персональных данных всех участников образовательного пространства. ИТ безопасность должна обеспечивать невозможность проникновения в стены учреждения информации незаконного или негативного характера, а также той информации, которая способна оказать неблагоприятное воздействие или любые манипуляции для учащихся на всех ступенях образования.

В последние годы школы переживают процесс серьезных системных преобразований, связанных с переходом на обновленные ФГОС (ФГОС третьего поколения), а значит, изменения коснутся целей, задач, результатов образования и воспитания гражданина сетевого общества. Как известно, ни один современный школьник не может сегодня обойтись без какого-либо гаджета с выходом в сеть Интернет. И еще бы, ведь 21 век – век информационных технологий с невероятными возможностями, которые стали неотъемлемой частью жизни каждого человека. Цифровые возможности раздвигают границы, помогают в познании мира, открывают все новые и новые горизонты, поэтому традиционная система образования теряет свою актуальность, уступая место всему современному. Отсюда и встает новая задача для каждого образовательного учреждения – внедрение, апробация и реализация государственных стандартов, в основе которого лежит не только системно-деятельностный подход, но и возможность создания единого сетевого пространства с учетом всех вопросов безопасности [1. С. 94].

Учебно-методическое сопровождение, модель флеш-наставничества, электронное оборудование и прочие нововведения повышают компетентность всех участников образовательного пространства, а также способствуют повышению уровня и качества образованности современных школьников, обеспечивая всестороннее развитие и воспитание будущего поколения нашей страны. Именно инновационные возможности позволяют реструктурировать весь учебный процесс. Однако, внедряя все новые и новее цифровые технологии в образовательную

среду, особое внимание стоит уделить такому факту, как цифровая безопасность. Именно ребенок, школьник, на первый взгляд, активный пользователь сети, оказывается подвержен воздействию и влиянию Интернет-ресурсов. Осваивая те или иные приложения, переходя с ссылки на ссылку, посещая подозрительные сайты, неподготовленный пользователь рискует поймать вирусный файл, потерять личные данные или поддаться красивой рекламе в гонке за современными возможностями. Самыми уязвимыми по-прежнему остаются сегодняшние школьники [5. С. 109].

Несмотря на все отрицательные стороны цифровых технологий, Интернет и его возможности – это бессменные помощники в процессе обучения, особенно при саморазвитии и самореализации. Однозначными плюсами были и остаются:

– легкость и доступность необходимой информации;

– возможность самостоятельно изучить какую-либо тему или непонятный вопрос;

– углубить свои знания по тому или иному предмету;

– найти свое место и предназначение в сетевом пространстве.

Прежде всего, такие ресурсы помогают обеспечивать непрерывность образовательного процесса, способствуют развитию памяти, абстрактного и логического мышления, выстраиванию ассоциативных рядов и многому др., что значительно улучшает и облегчает процесс обучения заинтересованного школьника [2. С. 204].

Интернет-возможности – это актуальное поле раскрытия потенциала личности обучающегося, где отдельным звеном стоит вопрос о безопасности.

Следуя определенному алгоритму правил, который должен носить комплексный характер, есть огромная вероятность повышения уровня защиты персональных данных участников образовательного процесса:

Выделим пять основных способов защиты информационной безопасности:

1. Нормативно-правовой: образовательные законы, на основе которых нет доступа к конфиденциальной информации [5. С. 91].

2. Морально-этические средства – система мер, направленная на защиту подростка от любой информации негативного или плохо воздействующего характера [4. С. 52].

3. Административно-организационные меры – это определенные правила и нормы по работе с информацией и ее носителями [4. С. 52].

4. Физические меры – это организованные меры защиты в образовательном учреждении (пропускная система, организация контроля доступа посетителей и т. д.) [4. С. 53].

5. Технические меры – это программные меры комплексной системы защиты всего периметра компьютерной сети [4. С. 54].

Только комплексное использование всех перечисленных мер способно обеспечит цифровую безопасность в образовательном пространстве. Не только школьник, но и его родители являются участниками образовательного процесса, поэтому на каждом лежит определенная степень ответственности по ограничению и фильтрации информации.

Цель современной школы – воспитание и обучение гармоничной личности, способной найти свое место в жизни. И именно современные интерактивные

технологии призваны обеспечить реализацию учебных программ, раскрывая творческую природу каждого обучающегося [3. С. 14].

Инновационные (цифровые) технологии в образовании – это организация всего образовательного процесса, с такими принципами, как:

– ситуация диалога;

– воспитательное пространство;

– социокультурная деятельность и ее продукт;

– психолого-педагогическое воздействие.

Чтобы достичь успеха в реализации безопасности при использовании инновационных (цифровых) технологий в образовании необходимо:

– установить взаимосвязь всех участников образовательной среды через совместную деятельность;

– обеспечить активное и продуктивное взаимодействие всех участников учебной деятельности;

– нести индивидуальную ответственность за свои действия и действия в работе группы;

– развивать навыки совместной работы;

– уметь давать оценку своей деятельности и деятельности других участников образовательного пространства [1. С. 96].

Для недопущения угроз и утечки персональных данных образовательное учреждение создает комплекс мер и правил, которые являются обязательными для исполнения всеми участниками образовательного процесса. Такая система направлена на защиту информационного пространства от случайного или намеренного проникновения в конфигурацию системы.

Обеспечение информационной безопасности обучающихся ложится, прежде всего, на плечи учителей, главными из которых остаются преподаватели информатики и специалисты в области компьютерных технологий. Однако любой педагог – предметник должен знать:

– формы и способы воздействия ИКТ, их негативное воздействие, а также методы защиты от утечки информации или же нежелательного воздействия;

– правила и нормы сетевого этикета в пространстве сети Интернет;

– виды и формы отклоняющегося, зависимого поведения школьников;

– методы работы по профилактике, предупреждению и устранению нежелательного воздействия.

Система информационной безопасности – это процесс обучения ребенка адекватному восприятию и оценке информации, ее критическому осмыслению на основе нравственных и культурных ценностей. Каждому участнику образовательного пространства следует помнить ряд правил и законов виртуального сообщества как при обучении, так и общении. Незнание основ сетевого мира способно привести к демонстрации асоциального поведения школьника или правонарушения в сфере ИКТ [6. С. 74].

Таким образом, инновационная система образовательной среды ставит перед собой цель – создать наиболее благоприятную атмосферу обучения, которая способствовала бы продуктивному взаимодействию по системе: ученик – учитель; ученик – ученик; ученик – родитель; учитель – родитель. При наличии обратной

связи субъектно-объектных отношений происходит обмен коммуникативными ролями, что повышает эффективность обмена информации и улучшает ее усваивание, помогая избежать негативного влияния со стороны интернет-ресурсов.

Организуя образовательное пространство с использованием инновационных (цифровых) форм обучения, стоит делать акцент на моделирование жизненных ситуаций, совместное решение проблем на основе анализа обстоятельств и ситуации, тогда это принесет положительный результат и будет способствовать развитию гармоничной личности, способной искать пути и возможности решения той или иной ситуации, проблемы. Процесс же обеспечения цифровой безопасности основывается на умениях личности увидеть и нейтрализовать угрозу, исходящую от информационного воздействия [2. С. 209].

Формирование информационной безопасности – процесс, требующий детальной проработки, ответственность за который несет каждый участник образовательной среды. Воспитание разносторонней интеллектуальной личности – гарантия ее информационной безопасности в виртуальном пространстве.

Список литературы

1. Агальцов В. П. Контроль знаний – доминирующая составляющая образовательного процесса // Информатика и образование. 2019. № 2.

2. Воронов Р. В., Гусев О. В., Поляков В. В. О проблеме обеспечения безопасного взаимодействия с сетевыми образовательными ресурсами // Открытое образование. 2008. № 3. 234 с.

3. Информационная безопасность в образовательной организации. URL: https://www.smartsoft.ru/blog/informatsionnaja_bezopasnost_v_obrazovateljnoj_organizatsii

4. Кудрявцева О. С. Информационная безопасность детей в образовательной организации: проблемы и пути их решения. URL: https://nsportal.ru/shkola/administrirovanie-shkoly/library/2021/05/11/informatsionnaya-bezopasnost-detey-v

5. Малых Т. А. Педагогические условия развития информационной безопасности младшего школьника: автореф. дис. ... канд. пед. наук. Иркутск, 2018. 56 с.

6. Сыренский В. И. Психофизиология информационной безопасности школьника // Материалы научно-практической конференции «Информационная безопасность школьников: состояние, проблемы, перспективы», 28–30 апреля 2003 г. СПб., 2003. 95 с.

Д. В. Замрыга,
старший преподаватель,
Южно-Уральский государственный университет

ОСОБЕННОСТИ МЕР НАЛОГОВОЙ ПОДДЕРЖКИ НАЛОГОПЛАТЕЛЬЩИКОВ, ОСУЩЕСТВЛЯЮЩИХ ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ ЦИФРОВЫХ ИННОВАЦИЙ

Аннотация. Развитие и внедрение цифровых инноваций в отечественную экономику нуждается в государственной поддержке, в том числе посредством

различных механизмов налогообложения. На основании изученных мер налоговой поддержки сформулированы выводы о разноплановости существующих мер поддержки и необходимости их применения. Вместе с тем в целях дальнейшего совершенствования налогового администрирования предлагается разработка и внедрение специального или экспериментального налогового режима, направленного на комплексную поддержку отдельных категорий налогоплательщиков, осуществляющих деятельность в области цифровых инноваций.

Ключевые слова: налоговая система, налоговое администрирование, меры налоговой поддержки, меры налогового стимулирования, цифровые инновации, специальные налоговые режимы, налогоплательщик

FEATURES OF TAX SUPPORT MEASURES FOR TAXPAYERS ENGAGED IN ACTIVITIES IN THE FIELD OF DIGITAL INNOVATION

Abstract. The development and implementation of digital innovations in the domestic economy needs state support, including through various taxation mechanisms. Based on the studied tax support measures, conclusions are formulated about the diversity of existing support measures and the need for their application. At the same time, in order to further improve tax administration, it is proposed to develop and implement a special or experimental tax regime aimed at comprehensive support for certain categories of taxpayers engaged in activities in the field of digital innovations.

Keywords: tax system, tax administration, tax support measures, tax incentive measures, digital innovations, special tax regimes, taxpayer

В современном мире цифровые инновации стали основой для трансформации экономики в связи с массовой информатизацией общества. Развитие экономики на современном этапе требует активного внедрения IT-технологий, что особенно важно в условиях беспрецедентного экономического давления, в которых оказалась Российская Федерация. В связи с этим возникла острая необходимость внесения изменений в действующее законодательство Российской Федерации в кратчайшие сроки. Поскольку механизм поддержки экономики государства был разработан еще в период антироссийских санкций в связи с присоединением Крыма к России и конфликтом на востоке Украины, а затем также в период пандемии новой коронавирусной инфекции, законодатель смог без промедления реализовать отдельные механизмы государственной поддержки, включая меры налоговой поддержки.

В целях достижения необходимых долгосрочных структурных изменений в экономике Правительством Российской Федерации в сентябре 2020 г. был утвержден «Общенациональный план действий, обеспечивающих восстановление занятости и доходов населения, рост экономики и долгосрочные структурные изменения в экономике» [7], «Основные направления бюджетной, налоговой и таможенно-тарифной политики на 2021 год и на плановый период 2022 и 2023 годов» [8], «Основные направления бюджетной, налоговой и таможенно-тарифной политики на 2023 год и на плановый период 2024 и 2025 годов» [9], Национальная

программа «Цифровая экономика Российской Федерации [6], а также иные программные правовые акты.

Существует множество мер государственной поддержки предприятий, граждан и общества в целом. К таким мерам относят: предоставление субсидий и грантов, влияние на ценообразование, налоговое стимулирование и другие. Одной из самых распространенных и успешно действующих мер является налоговое стимулирование. В различных кризисных ситуациях, которые оказывают влияние на предпринимательство, особенно малый и средний бизнес, а также население конкретного государства, вводятся и используются разнообразные меры налогового стимулирования [4. С. 55–58].

С. В. Васильев утверждает: «Налоговое стимулирование – это направленная деятельность органов государственной власти или органов местного самоуправления по установлению такого налогового законодательства, при котором налоговые льготы и другие налоговые меры улучшают имущественный или экономический статус отдельных категорий» [2]. Роль мер налогового стимулирования заключается в следующем: при возникновении кризисных явлений и ситуаций, которые влекут за собой экономический спад, налоговое стимулирование расширяет спрос или предложение, например, за счет снижения налогов, за счет чего происходит увеличение производственных мощностей, наращивание дохода. За счет увеличения собственного производства государства экономика начинает восстанавливаться. Исходя из этого, можно сформулировать задачи налогового стимулирования. Главной задачей является восстановление экономики и поддержание достойного уровня. Посредством, например, увеличения налогов снижается экономическая активность, так как государство забирает большую часть прибыли за счет налоговых отчислений. Предприятия играют большую роль для экономики государства. А поскольку из-за больших налогов страдает предпринимательство, то и экономика страны будет страдать. Особенно, в кризисных ситуациях это будет очень чувствоваться. То есть логично, чтобы повысить экономическую активность, «поднять» экономику, необходимо уменьшить налоги. Так, при помощи мер налогового стимулирования реализуется задача по восстановлению экономики государства. Для достижения основополагающей задачи существуют подзадачи: налоговое стимулирование инвестиций, поддержка модернизации производства, повышение роли налогов в доходах бюджета, совершенствование налогового администрирования и другие.

Для стабильного и успешного функционирования такого института, как меры налогового стимулирования, существуют принципы. Под принципами налогового стимулирования Н. Н. Лайченкова подразумевает: «Выраженные в нормах налогового права основные руководящие положения, которые определяют направленность и содержание государственной политики при выборе различных видов стимулов, оснований и порядка их применения» [5. С. 44]. Можно выделить общие принципы и частные, которые относятся конкретно к данному институту. Прежде всего, к общеправовым принципам относится принцип законности, который предполагает, что все применяемые меры должны соответствовать законам государства. Основой современной налоговой системы является принцип

справедливости. Последний реализуется при введении налоговых льгот с помощью введения необлагаемого минимума для наиболее незащищенных слоев населения или секторов экономики, нуждающихся в поддержки государства. Таким образом, как раз за счет мер налогового стимулирования можно достичь справедливости. Принцип равенства реализуется за счет равенства плательщиков, т. е. недопустимо устанавливать индивидуальные налоги для лица, дискриминация не допускается. Равенство заключается в запрете установления мер налоговой поддержки исходя из расовой принадлежности, религиозных предпочтений, социального положения, национальности и других дискриминационных критериев. Налоговые стимулы не могут носить индивидуального характера, как и налоги, устанавливаются для широкого круга лиц на равных условиях. Принцип федерализма заключается в том, что законодательство о применении налогового стимулирования едино. Такое регулирование осуществляется за счет законодательства Российской Федерации, субъектов, муниципальных образований. Принцип определенности подразумевает, что меры налогового стимулирования должны быть ясны, недвусмысленны и понятны для всех. К частным принципам можно отнести принцип всеобщности. То есть налоговое стимулирование применимо для всех тех лиц, которые подходят под категории, для которых та или иная мера введена. Нет конкретного лица, которое может воспользоваться мерой. Следующим принципом является отсутствие принуждения. Мерами можно пользоваться, а можно от них отказаться и никто не вправе заставить лицо, которому мера положена. Принцип применение налоговых льгот без ущерба для доходов бюджета. Введение и применение мер не должно вредить бюджету государства, субъектов и самих лиц. Льготы наоборот предусмотрены для того, чтобы поддержать как государство, точнее экономику государства, так и членов общества, оказавшихся в затруднительном положении. Поэтому невозможно ввести меру, которая ухудшало бы положение вышеперечисленных субъектов.

Исходя из вышесказанного, меры налоговой поддержки предусмотрены для поддержания уровня экономики государства при возникновении кризисных явлений и ситуаций [10]. К таким явлениям можно отнести пандемию коронавируса, начавшуюся в 2020 году, и начало специальной военной операции в 2022 году. Оба события повлияли на жизнь всего государства. Изменения произошли во всех слоях общества, всех организациях и предприятиях, государственных структурах. Введение разнообразных санкций не могло не отразиться на экономике государства. В той или иной мере экономика пострадала и необходимо время для восстановления.

Для современного периода мобилизационной экономики характерно применение целого ряда мер налоговой поддержки, которые изначально были апробированы в период пандемии. Развитие мобилизационной экономики во многом зависит от эффективности мер государственной, в том числе налоговой поддержки. Применение мер налоговой поддержки позволило увеличить количество аккредитованных IT-компаний и повысить процент создание новых IT-компаний, а также увеличить число специалистов [3].

Автором были проанализированы отдельные меры налоговой поддержки.

Хозяйствующие субъекты отмечают, что наивысшими результатами характеризуются налоговые каникулы. Налоговые каникулы определены законодателем в виде меры поддержки предпринимательства за счет фиксированного срока (условия определяется регионально как по введению в своих границах налоговых каникул, так и по срокам: от 1 до 3 лет), в течение которого у индивидуального предпринимателя, который был зарегистрирован первый раз на упрощенной налоговой системе или патентной налоговой системе возникает возможность использовать нулевые налоговые ставки, которые были установлены в связи с принятием Федерального закона от 29.12.2014 № 477-ФЗ о внесении изменений в ч. 2 НК РФ, если такое правило закреплено в региональном законодательстве субъекта федерации, где индивидуальный предприниматель зарегистрирован. Такая процентная ставка может быть применена предпринимателями, использующими упрощенную и патентную системы налогообложения, а также осуществляющие предпринимательскую деятельность в производственной, социальной и (или) научной сферах и в сфере бытовых услуг. В период с середины 2020-го года причиной продолжения налоговых льгот стала активно распространяющаяся инфекция коронавируса, период самоизоляции и связанный с этим экономический кризис, во многом также обусловленный западными санкциями. Продление налоговых каникул стало одной из мер государственной поддержки малого бизнеса. Вновь зарегистрированные индивидуальные предприниматели могли воспользоваться нулевыми налоговыми ставками до 2024 года. Не менее 70 % от общего дохода должны составлять товары и услуги, к которым применяется нулевая налоговая ставка. Важно отметить, что предприниматели только на упрощенной или патентной налоговой системе могут использовать налоговые каникулы. Другие налоги, например, акцизы, транспортные налоги и другие, платить обязательно. Предпринимателям на налоговых каникулах необходимо платить страховые взносы на обязательное пенсионное страхование за себя и наемных работников. Несмотря на нулевую процентную ставку (освобождение от налога), сдавать отчетность все же необходимо, указывая в отчете по упрощенной системе налогообложения ставку 0 %.

При этом применение данной льготы разрешенного для целого перечня видов деятельности и не связано непосредственно с развитием цифровых технологий.

В настоящее время налоговые каникулы были продлены до конца 2024 года и продолжают действовать в большей части регионов страны.

Еще одной мерой является освобождение от налогообложения субсидий малому и среднему предпринимательству, в том числе: субсидии на карантин, а также субсидии на нерабочие дни (такая субсидия предоставлялась один раз в период с 30.10.2021 до 07.11.2021).

Данная мера оказалась достаточно эффективной и распространенной для представителей малого и среднего предпринимательства, о чем свидетельствует статистика обращений с соответствующими заявлениями [1].

Стоит заметить, что в связи с началом специальной военной операции такая мера не была применена.

Перенос сроков уплаты налогов на полгода субъектам малого и среднего предпринимательства, находящихся на упрощенной налоговой системе, был установлен в апреле 2020 года. Такая ситуация с переносом сроков выплаты налогов, уплачиваемого в связи с применением упрощенной налоговой системы, действовала в 2020 году в период разгара пандемии. Спустя два года в 2022 году, были внесены изменения: предоставление отсрочки по выплате налога не всем, кто находится на упрощенной налоговой системе, а только из сфер деятельности, ОКВЭД по которым представлен в постановлении Правительства Российской Федерации от 30.03.2022 № 512 «Об изменении сроков уплаты налога (авансового платежа по налогу), уплачиваемого в связи с применением упрощенной системы налогообложения в 2022 году». Можно сделать вывод о выявленной положительной динамике применения в пандемию, что стало основанием для повторного применения во время специальной военной операции.

По новым правилам продлевались сроки уплаты налога по упрощенной налоговой системе за 2021 год и аванса соответствующего специального режима за 1 квартал 2022 года (аналогично с предыдущим – на 6 месяцев). Также было предоставлено право налогоплательщикам внесения этих платежей в рассрочку по 1/6 в месяц. Это позволило субъектам малого и среднего бизнеса с соответствующими ОКВЭД перенести на осенний период уплату налогов, освободив денежные активы на развитие бизнеса.

Воспользоваться возможностью переноса уплаты налога могли только те, у кого код из списка был основным в ЕГРЮЛ или ЕГРИП на 01.01.2022.

Еще одной мерой было введение ФНС России моратория на налоговые санкции за непредставление документов и на выездные налоговые проверки после начала пандемии. Были продлены сроки сдачи бухгалтерской, налоговой отчетности, отчетности по страховым взносам (при этом сроки уплаты налогов остались прежними). Также были продлены сроки реагирования налогоплательщиков на требования налоговых органов (20 рабочих дней – по срокам, установленным в ст. 93, 93.1 НК РФ; 10 рабочих дней – по срокам, установленным п. 3 ст. 88 НК РФ).

Постановлением Правительства Российской Федерации от 01.10.2022 № 1743 «О внесении изменений в постановление Правительства Российской Федерации от 10 марта 2022 г. № 336», согласно которому мораторий продлился на весь период 2023-го года (для представителей малого и среднего предпринимательства), т. е. уже на период специальной военной операции, за исключением ряда организаций с высокими производственными рисками. Мораторий распространяется на плановые проверки Роскомнадзора, Ростехнадзора, МЧС, трудовой инспекции и других ведомств. Мера действует на документарные и выездные мероприятия. Были сохранены и внеплановые проверки сохранили, но с некоторыми оговорками (например, по наличию жалоб, указанию федерального органа или прокуратуры). Также мораторий ограничивает проведение контрольных и мониторинговых закупок, выборочного контроля, рейдового осмотра.

Также стоит остановиться на такой мере, как снижение страховых взносов. Субъекты малого и среднего предпринимательства в части выплат, которые

превышают размер минимальной оплаты труда, могут использовать пониженные тарифы на страховые взносы (платеж снизился с 30 до 15 %):

– на обязательное пенсионное страхование 10 %. Тариф распространяется как на выплаты в рамках предельной базы, так и сверх нее.

– на обязательное социальное страхование на случай временной нетрудоспособности и в связи с материнством – в размере 0,0 процента;

– на обязательное медицинское страхование – в размере 5,0 процентов.

Также некоторые бизнесмены в 2020 году были освобождены от уплаты страховых взносов. Нулевую ставку, согласно Федеральному закону № 172-ФЗ от 8 июня 2020 г., вправе применять компании и индивидуальные предприниматели, чья деятельность входит в список наиболее пострадавших от пандемии отраслей, а также некоммерческие организации и религиозные организации.

Отсрочка касалась только взносов, срок уплаты которых приходилось на 2020 год. Получить такую отсрочка на уплату страховых взносов могли не все предприниматели, а только некоторые, деятельность которых упоминается в перечне Правительства, как деятельность, наиболее пострадавшая.

После начала специальной военной операции были внесены поправки для ряда категорий плательщиков страховых взносов, распространяющиеся на правоотношения с 1 января 2022 года. Так, Федеральным законом от 21.11.2022 № 443-ФЗ внесены дополнения к ст. 422 НК РФ и ст. 20.2 Федерального закона от 24.07.1998 №125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний», устанавливающие перечень выплат в пользу работников, не подлежащих обложению страховыми взносами. Речь как о страховых взносах на обязательное пенсионное, социальное страхование на случай временной нетрудоспособности и в связи с материнством, так и о страховых взносах «на травматизм».

С 1 января 2022 года не облагаются указанными страховыми взносами:

– безвозмездно переданные работникам, призванным на военную службу по мобилизации, денежные средства и иное имущество;

– денежные средства и иное имущество, безвозмездно переданные работникам, проходящим военную службу по заключенному контракту либо по контракту о пребывании в добровольческом формировании.

– Вышеперечисленные меры налоговой поддержки в целом были направлены на стабилизацию экономики. Однако были разработаны и меры исключительно для IT-компаний.

Развитие IT-технологий является одним из важнейших факторов прогресса не только в сфере отдельных специализированных отраслей науки, но и на прямую касается законодательства Российской Федерации, и повышения качества уровня жизни граждан. IT-компании осуществляющие разработку технологий, серьезно пострадали во время пандемии короновирусной инфекции, и для их поддержки государством были приняты меры поддержки и налоговые льготы, такие как: льготы по налогу на прибыль, льготы по НДС, снижение ставки по страховым взносам и налога на прибыль.

Также и во время специальной военной операции IT-компании понесли убытки. Были предоставлены следующие льготы: льготные кредиты со ставкой, не более 3 процентов; для аккредитованных организаций налоговая ставка по налогу на прибыль организаций устанавливалась в размере 0 процентов до 31 декабря 2024 года; упрощается процедура устройства на работу для иностранных граждан в аккредитованную, которые способствуют развитию технологий в Российской Федерации; возможность получения отсрочки гражданам Российской Федерации от призыва на военную службу; аккредитованные организации освобождаются от налогового контроля, валютного контроля и других видов государственного контроля (надзора) и муниципального контроля на срок до трех лет и другие меры поддержки.

Для того чтобы воспользоваться льготами, IT-компаниям необходимо получить аккредитацию в Минцифры и соответствовать определенным критериям: иметь подходящий ОКВЭД, необходимое число сотрудников не менее 7 человек, доля выручки от IT-деятельности должна занимать не менее 90 % от всех ее доходов.

Наиболее эффективной мерой налоговой поддержки для IT-компаний является установление нулевого налога на прибыль в соответствии с Федеральным законом от 14 июля 2022 г. № 321-ФЗ «О внесении изменений в часть вторую Налогового кодекса Российской Федерации». Примечательно, что сроки действия данной льготы установлены с 1 января 2022 года.

Стоит отметить, что нулевым налогом могут облагаться IT-компании при таких условиях как: аккредитованность, количество сотрудников, а также доля доходов от передачи прав на компьютерные программы и базы данных и от отказа услуг по установке тестирования и сопровождения этого программного обеспечения должна составлять не менее 90 % от общей прибыли предприятия.

Данная мера налоговой поддержки оказалось привлекательной для многих IT-компаний ввиду того, что прежняя ставка составляла 3 % налога на прибыль.

В то же время не все регионы смогли адекватно отреагировать на изменения законодательства. Так, например, в Челябинской области в соответствии с Законом Челябинской области от 03.06.2022 № 587-ЗО «О внесении изменения в статью 1 Закона Челябинской области «Об установлении налоговых ставок при применении упрощенной системы налогообложения на территории Челябинской области» налоговая ставка не была «обнулена», а только снижена до 13,5 %.

Приведенные выше примеры мер налоговой поддержки позволяют сделать вывод о многообразии и их разноплановости, а также о необходимости классификации. По-нашему мнению, существующие меры налоговой поддержки можно классифицировать по следующим основаниям.

Первая группа также включает меры, направленные на снижение страховых взносов. Освобождение от налогообложения субсидий малому и среднему предпринимательству и другие виды освобождений также включаются в первую группу исследуемых мер.

Ко второй исследуемой группы мер налоговой поддержки следует отнести введение мораториев на налоговые проверки и иные способы налогового контроля.

К третьей группе мер следует отнести создание новых налоговых режимов, сокращения сроков возмещения НДС и применение новых оснований для налоговой логистики в виде отсрочки.

Перечисленные меры поддержки создают особый правовой режим для отдельных категорий налогоплательщиков, но не представляют собой отдельный специальный или экспериментальный налоговый режим.

Особенностями развития информационных технологий является возможность реализации отдельных проектов силами микропредприятий для которых многообразие мер поддержки может стать может стать одновременно проблемой, так как учредителям и руководителям таких организаций будет сложно разобраться с применением всего предлагаемого спектра мер налоговой поддержки. В связи с чем, читаем наиболее эффективным создание отдельного специального или экспериментального налогового режима для компаний, осуществляющих деятельность в области цифровых инноваций. Создание такого режима направлено на совершенствование налогового администрирования в данной сфере за счет объединения разноплановых мер налоговой поддержки (стимулирования).

Проведенный анализ отдельных меры налоговой поддержки (стимулирования) позволяет сделать вывод об их эффективности. Однако современная ситуация в экономике ставит новые задачи в том числе перед юридической наукой, направленные на осуществление мониторинга влияния применяемых мер налоговой поддержки (стимулирования) и своевременную коррекцию для достижения желаемых результатов.

Список литературы

1. В налоговые органы области представлено более 2 тыс. заявлений на получение субсидии. URL: https://www.nalog.gov.ru/rn53/news/activities_fts/9791059/

2. Понятие и методология налогового стимулирования / В. С. Володченко, Д. С. Ланцова, Т. А. Миронова, К. А. Бышок, Е. В. Сапунова // Вопросы науки и образования. 2020. № 3 (87).

3. Выступление Дмитрия Чернышенко на рабочей встрече с Президентом РФ В. В. Путиным. URL: http://www.kremlin.ru/events/president/news/69665

4. Карпов В. В., Кораблева А. А. Методико-методологические основы моделирования государственной поддержки предпринимательства // Двадцатые Апрельские экономические чтения: материалы Междунар. науч.-практ. конф. / под ред. д. э. н., проф. В. В. Карпова и д. э. н., проф. А. И. Ковалева. Омск: РОФ «ФРСР». 2014. С. 55–58.

5. Лайченкова Н. Н Стимулы в налоговом праве: дис…. канд. юрид. наук. Саратов. 2007.

6. Национальная программа «Цифровая экономика Российской Федерации // СПС «Консультант Плюс».

7. Общенациональный план действий, обеспечивающих восстановление занятости и доходов населения, рост экономики и долгосрочные структурные изменения в экономике // СПС «Консультант Плюс».

8. Основные направления бюджетной, налоговой и таможенно-тарифной политики на 2021 год и на плановый период 2022 и 2023 годов СПС «Консультант Плюс» // СПС «Консультант Плюс».

9. Основные направления бюджетной, налоговой и таможенно-тарифной политики на 2023 год и на плановый период 2024 и 2025 годов // СПС «Консультант Плюс».

10. Правовое управление в кризисных ситуациях: монография / отв. ред. Ю.А. Тихомиров. Проспект, 2022.

Д. А. Зубрик,
магистр юридических наук,
Гродненский государственный университет
имени Янки Купалы

ПРИЗНАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КАЧЕСТВЕ СУБЪЕКТА ПРАВОНАРУШЕНИЯ: ПРОБЛЕМАТИКА И ПЕРСПЕКТИВЫ

Аннотация. Применение искусственного интеллекта в повседневной жизни является неотъемлемым атрибутом современного общества. Продукты искусственного интеллекта становятся все более качественными. Однако в доктрине существуют споры относительно того, кто несет ответственность, если деятельностью искусственного интеллекта будет причинен вред. В связи с этим были проанализированы понятия «субъект правонарушения» и «искусственный интеллект». Также наличие основных законов робототехники позволяют установить правила, которые искусственный интеллект должен учитывать при своей работе. Выявлено, что искусственный интеллект не попадает под признаки субъекта правонарушения. Однако в рамках гражданско-правовой ответственности можем говорить о частичном признании вины роботозированной системы, но с некоторыми оговорками. Проведенный анализ концепции «электронного лица» выявил невозможность внедрения нового субъекта правонарушения в силу своей специфики. С учетом проведенного анализа сделан вывод, что признание искусственного интеллекта в качестве субъекта правонарушения невозможно на современном этапе. Ответственность должно нести то лицо, по ошибке которого робот причинил вред общественным отношениям.

Ключевые слова: искусственный интеллект, субъект правонарушения, ответственность, общественные отношения, нейросеть, chat gpt-4, электронное лицо

RECOGNITION OF ARTIFICIAL INTELLIGENCE AS A SUBJECT OF OFFENSE: PROBLEMS AND PERSPECTIVES

Abstract. The use of artificial intelligence in everyday life is an integral attribute of modern society. Artificial intelligence products are getting better and better. However, there are disputes in the doctrine as to who is responsible if harm is caused by the activities of artificial intelligence. In this scientific article, the concepts of “subject of the offense” and “artificial intelligence” were analyzed. Also, the presence of the basic

laws of robotics allows you to establish the rules that artificial intelligence must take into account in its work. It was revealed that artificial intelligence does not fall under the signs of the subject of the offense. However, within the framework of civil liability, we can talk about a partial recognition of the guilt of the robotic system, but with some reservations. Also, the analysis of the concept of "electronic person" revealed the impossibility of introducing a new subject of the offense due to its specificity. Taking into account the analyzed material, we came to the conclusion that the recognition of artificial intelligence as a subject of an offense is impossible at the present stage. Responsibility should be borne by the person by whose mistake the robot caused harm to public relations.

Keywords: artificial intelligence, subject of offenses, responsibility, public relations, neural network, chat gpt-4, electronic person

Имплементация информационных технологий в повседневную жизнь происходит очень быстро. Ярким примером является создание Chat GPT-4, которая была презентована 14 марта 2023 года. Данная нейросеть способна понимать естественный язык и выполнять задачи на всех языках мира, что делает ее гораздо умнее остальных нейросетей. Кроме этого, данная нейросеть сдала экзамен на адвоката, при этом набрав 297 баллов из 300, что является наивысшим результатом. То есть, можно сказать, что Chat GPT-4 обошел человека по силе интеллектуальных возможностей. Однако уже сейчас ведутся разговоры о создании GPT-5, но Сэм Альтман, глава компании OpenAI, заявляет, что пока что обучение данной нейросети не началось, так как требуется проработать большой пласт технических ошибок. Более того, необходимо отметить, что уже сейчас на просторах сети Интернет существуют каталоги нейросетей. Абсолютно любой пользователь может зарегистрировать в таком каталоге и выбрать ту нейросеть, которая соответствует его требованиям. Наличие систематизированного сайта позволит значительно упростить поиск необходимого сервиса.

Но смоделируем ситуацию, в которой искусственный интеллект причинил вред общественным отношениям. Кто будет нести ответственность: человек или роботизированная система? Кто является субъектом правонарушения?

Прежде чем приступить к установлению проблемных аспектов, необходимо разобрать такие понятия как: «субъект правонарушения» и «искусственный интеллект».

Разберем понятие «субъект правонарушения». Под субъектом правонарушения подразумевается лицо, совершившее общественно вредное деяние [10]. Более того, в рамках статьи мы будем рассматривать данное понятие в широком понимании, затрагивающее те отрасли права, которые регламентируют ответственность. Также для того, чтобы лицо признавалось в качестве субъекта правонарушения, необходимо наличие следующих признаков:

1) физическое или юридическое лицо;

2) вменяемое или обладающего правоспособностью (для юридического лица);

3) достижение возраста несения ответственности (для физического лица).

Что касается терминологии «искусственного интеллекта», то данное понятие ввел Джон Маккарти, в котором закреплялось, что искусственный интеллект – это наука и технология создания интеллектуальных машин, особенно интеллектуальных компьютерных программ. Это связано с аналогичной задачей использования компьютеров для понимания человеческого интеллекта, но ИИ не должен ограничиваться биологически наблюдаемыми методами [4]. Кроме того, искусственный интеллект должен обладать следующими признаками:

1) наличие технического устройства;

2) способность к принятию, обработке и передаче информации;

3) способность к автономной работе;

4) самообучение на основе анализа информации и приобретенного опыта;

5) способность к принятию самостоятельных решений.

В своей работе О. Н. Толочко определяет, что искусственный интеллект – это способность компьютерных систем (аппаратно-программных комплексов) выполнять когнитивные функции, обычно присущие человеку. Более того, искусственный интеллект снабжается информационной базой, блоком, способным находить решения благодаря встроенной в него программе, и интерфейсом для взаимодействия с человеком. Данные технические устройства позволяют искусственному интеллекту самообучаться и выполнять поставленные задачи [2].

Необходимо отметить, что Айзеком Азимовым были выделены законы робототехники:

1) Робот не может причинить вред человеку или своим бездействием допустить, чтобы человеку был причинен вред;

2) робот должен повиноваться всем приказам, которые дает человек, кроме тех случаев, когда эти приказы противоречат первому закону;

3) робот должен заботиться о своей безопасности в той мере, в которой это не противоречит первому или второму законам [8].

Если сопоставить современное развитие искусственного интеллекта и данные законы, то возникает вопрос: можем ли мы говорить о том, что в случае причинения вреда конкретным общественным отношениям, искусственный интеллект признается субъектом правонарушения и несет полную ответственность?

Ранее в данной статье мы выделили признаки, по которым лицо признается субъектом правонарушения. Сопоставим их с признаками искусственного интеллекта. Первый признак – физическое или юридическое лицо. Искусственный интеллект является техническим устройством, соответственно, мы не можем говорить о том, что он [искусственный интеллект] является субъектом права в классическом понимании. Однако в доктрине рассматриваются вопросы о признании искусственного интеллекта в качестве электронного лица.

В своей работе П. М. Морхат отмечает, что наделение правовым статусом «электронного лица» приведет к созданию нового правового института. Данный институт будет предусматривать в себе контроль и управление роботов отдельно от физического или юридического лица, разграничение правоотношений между роботом и третьей стороной, а также между роботом и его владельцем. Сам автор считает, что концепция «электронного лица» может иметь место, однако на

данной стадии развития технологий должна применяться в ограниченных случаях [5. С. 73].

С. С. Горохова отмечает, что концепция «электронного лица» применима к концепции коллективного субъекта права, так как данная концепция не предполагает наделение правосубъектностью физического лица искусственный интеллект. Более того, данная концепция должна быть направлена не на признание самостоятельности искусственного интеллекта и исключения ответственности физических и юридических лиц, а на закрепление порядка идентификации юнитов искусственного интеллекта и людей, ими управляющими [3. С. 30].

С нашей точки зрения, концепция «электронного лица» имеет место быть. Однако ее применение может использоваться только в рамках гражданско-правовой ответственности. Такого же мнения придерживается Н. Н. Апостолова. Автор аргументирует свою позицию тем, что в рамках гражданско-правовых отношений искусственный интеллект может принимать решение самостоятельно без вмешательства человека. Более того, Н. Н. Апостолова делает оговорку о том, что такое применение возможно только в отношении сильного искусственного интеллекта [2. С. 114]. Мы также согласны с позицией автора.

Если говорить про административную и уголовную ответственность, то при определении степени ответственности учитывается волевой признак и психическое отношение к совершенному деянию, т. е. вина.

В теории уголовного и административно-деликтного права существует 2 категории вины: 1) умышленная; 2) неосторожная. Умышленная вина характеризуется тем, что лицо осознает опасность совершенного деяния, предвидит возникновение последствий и желает их наступление. Можем ли мы говорить о том, что искусственный интеллект умышленно совершает противоправное деяние? Если рассматривать искусственный интеллект с точки зрения техники, то роботизированная система может предвидеть определенные последствия. Однако в силу того, что робот не оснащен интеллектуально-волевыми качествами, то он не понимает, что совершает общественно опасное деяние. Более того, у искусственного интеллекта отсутствует желание о наступлении последствий. Соответственно, умышленная вина исключается.

Касательно неосторожной вины, то в данном случае имеется в виду, что лицо не желает наступления общественно опасных последствий, но сознательно допускает или относится к этому легкомысленно. Исходя из теории неосторожной вины, можно сделать вывод, что искусственный интеллект при совершении деяния попадает под ее действие. Но так ли это? Действительно, искусственный интеллект может предвидеть наступления определенных последствий, но в силу отсутствия когнитивно-психологических качеств не способен осознавать, что именно такие действия ведут к наступлению последствий, которые человек расценивает как общественно опасные.

Конечно же, применение концепции электронного лица в уголовном и административно-деликтном праве имеет место быть. Но такое использование возможно при создании сильного искусственного интеллекта, способного не только выполнять поставленные задачи, но и чувствовать, как человек. На сегодняшний

день такое использование повлекло бы за собой полный пересмотр теории о субъективной стороне правонарушения и преступления, что не представляется возможным. При этом, если говорить об использовании концепции «электронного лица», то возникает вопрос: какую именно ответственность будет нести искусственный интеллект?

С нашей точки зрения, применение института ответственности в отношении искусственного лица на современный этап развития невозможно. Это можно объяснить тем, что применение ответственности в отношении конкретного лица является способом порицания и воспитания. Искусственный интеллект в силу своей специфики не способен понимать сущность примененного наказания. Однако наказание в виде уничтожения потенциально опасного робота имеет место быть, но оно не влечет за собой морального порицания к нему.

Следующий признак, который свойственен субъекту правонарушения – вменяемость (правоспособность).

Вменяемость является способностью лица осознавать общественную опасность совершенного деяния и руководить своими действиями. Необходимо отметить, что способность руководить своими действиями характерна для искусственного интеллекта. В данном случае имеется в виду, что искусственный интеллект, запрограммированный на совершение конкретных задач, выполняет поставленные цели на основе собственной работы и самообучения. Однако, как уже было сказано ранее, искусственный интеллект не может давать морально-этическую оценку совершенного деяния. Соответственно, мы не можем говорить о том, что искусственный интеллект попадает под действие признака вменяемости. Более того, нельзя говорить о том, что искусственный интеллект, имеющий статут «электронного лица» обладает вменяемостью, поскольку данный признак характерен для человека, так как в данном случае имеются в виду биологические процессы, проходящие в организме.

Что касается правоспособности в рамках признаков субъекта правонарушения, то в данном случае имеется в виду способность юридического лица иметь гражданские права и обязанности и нести ответственность. Как мы определили ранее, искусственный интеллект не способен нести ответственность. Однако можем ли мы говорить о том, что робот обладает правами и обязанностями?

В теории развития робототехники, в будущем, когда роботизированная система будет приравнена к человеку, создание гражданских прав искусственного интеллекта будет являться необходимым условием. К таким правам можно перечислить: право на качественное техническое обслуживание (аналог права на медицинское обслуживание), право на самообучение (аналог права на образование), право на неприкосновенность.

Если говорить об обязанностях, в целом, можно сказать, что обязанности были отражены в законах робототехники Айзенка Азимова. То есть, мы можем говорить о том, что уже сейчас искусственный интеллект несет обязанности, однако не имеет прав.

Следующий признак – это наступление возраста несения ответственности. В данном случае проблематичным является определение, с какого момента

искусственный интеллект способен нести ответственность. С нашей точки зрения, момент, с которого искусственный интеллект несет ответственность, возникает тогда, когда будет окончено формирование программной кодировки, и робот будет готов к выполнению всех поставленных задач.

Подводя промежуточный итог, можно сказать, что искусственный интеллект на современном этапе развития нельзя признавать в качестве субъекта правонарушения.

Однако возникает вопрос: кто несет ответственность, если был причинен вред общественным отношениям искусственным интеллектом? [9].

В своей работе Е. Н. Агибалова выделяет семь моделей ответственности за деяние робота: 1) действия искусственного интеллекта признаются обстоятельством непреодолимой силы, и, соответственно, ответственность исключается; 2) назначение пострадавшему лицу компенсации из средств страхового фонда или за счет владельца робота, т. е., частичное освобождение от ответственности; 3) Определение причин по которым роботом был совершен вред. То есть, речь идет о том, что если будет выяснено, что деяние было вызвано дефектами конструкции, то ответственность должен нести производитель. Если ответственность была вызвана ошибкой в кодировке, то ответственность должен нести разработчик; 4) ограниченная безвиновная ответственность; 5) полная безвиновная ответственность, т. е. какое-то конкретное лицо несет всю ответственность за действия искусственного интеллекта; 6) личная ответственность самого робота; 7) смешанный тип ответственности, при котором применяются те методы ответственности, более подходящие в соответствии со степенью опасности робота [1. С. 18]. С нашей точки зрения, применение безвиновной ответственности по отношению к лицу, за которым закрепляется искусственный интеллект, не совсем верно. Роботизированная система может причинить вред по различным факторам, которые, например, зависели от разработчика или инженера. Поэтому необходимо учитывать не только лицо, за которым закреплен искусственный интеллект, но и других лиц, участвовавших в его разработке.

В своей работе И. Н. Романова отмечает, что если речь идет об административной и уголовной ответственности, то при назначении наказания необходимо учитывать характер наступивших последствий и форму вины причинителя вреда, т. е. лица, определявшего условия и параметры использования искусственного интеллекта. Если говорить про гражданско-правовую ответственность, то проблема признания искусственного интеллекта в качестве правонарушителя можно решить путем признания данной технологии источником повышенной опасности [6. С. 76].

С точки зрения С. С. Гороховой, ответственность должны нести непосредственно разработчики, так как в их обязанности входит принятие шагов, которые могли бы предотвратить причинение вреда [4]. Аналогичного мнения придерживается И. Р. Бегишев [3]. По нашему мнению, возложение полной ответственности на разработчиков также не является верным. Следует разграничивать причины, в силу которых искусственный интеллект причинил вред, и, исходя из этих причин, определить, какой субъект будет нести ответственность.

В своей работе О. Н. Толочко рассматривает возможные варианты ответственности искусственного интеллекта в гражданском праве: 1) возложение ответственности на владельца данной системы; 2) частичное освобождение от ответственности с введением страховых выплат; 3) признание действий робота как обстоятельство непреодолимой силы, т. е. исключение ответственности; 4) разграничить ответственность, а именно, ответственность несет то лицо, в результате действий которого в работе искусственного интеллекта была ошибка; 5) ответственность несет сам робот, поскольку он наделен правосубъектностью как «электронное лицо». Автор утверждает, что самообучающая машина непредсказуема, поэтому в рамках гражданско-правового регулирования необходимо рассматривать все варианты [7]. Мы также солидарны с мнением автора и считаем, что непосредственное использование всех вариантов ответственности достаточно полно и всесторонне позволяет разрешить подобную проблематику.

Таким образом, можно сделать вывод, что искусственный интеллект на современном этапе развития нельзя признавать в качестве субъекта правонарушения. Это обосновано рядом причин: 1) отсутствует нормативное регулирование ответственности в отношении робота-правонарушителя; 2) отсутствие совпадений критериев между искусственным интеллектом и субъектом правонарушения; 3) невозможность применения ответственности в силу отсутствия у робота понимания сущности ответственности.

Ответственность должен нести гражданин, т. е. субъект права, который был указан в качестве лица, отвечающего за контроль деятельности искусственного интеллекта. Однако такое указание не является аксиомой и, соответственно, может изменяться в зависимости от причин, по которым искусственный интеллект причинил вред.

Список литературы

1. Агибалова Е. Н. Юридическая ответственность при применении систем искусственного интеллекта // Государство, право и общество: вопросы теории и практики: материалы второй Всероссийской научно-практической конференции (Сочи, 7–8 февраля 2020 г.) / отв. редактор В. И. Скрябин. Сочи, 2020. С. 15–24.

2. Апостолова Н. Н. Ответственность за вред, причиненный искусственным интеллектом // Северо-Кавказский юридический вестник. 2021. № 1. С. 112–119.

3. Бегишев И. Р. Уголовная ответственность за создание и (или) распространение роботов, предназначенных для целей совершения преступлений // Северо-Кавказский юридический вестник. 2021. № 2. С. 140–148.

4. Горохова С. С. О некоторых аспектах публичной юридической ответственности в сфере использования искусственного интеллекта и автономных роботов // Юридические исследования. 2021. № 5. С. 24–37.

5. Мохрат П. М. Проблемы определения юридической ответственности за действия искусственного интеллекта // Право и государство: теория и практика. 2017. № 9(53). С. 70–74.

6. Романова И. Н. Проблемы юридической ответственности за вред, причиненный при использовании технологий искусственного интеллекта // Человек: преступление и наказание. 2022. Т. 30, № 1. С. 72–77.

7. Толочко О. Н. Теоретические и прикладные проблемы гражданско-правового регулирования технологий искусственного интеллекта // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2023.

8. Три закона Азимова помогли сформировать ИИ. Нам нужно еще четыре. URL: https://habr.com/ru/companies/skillfactory/articles/528236

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

10. Филипова И. А., Коротеев В. Д. Будущее искусственного интеллекта: объект или субъект права? // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 359–386.

П. А. Иллюк,
аспирант,
Институт законодательства и сравнительного правоведения
при Правительстве Российской Федерации

ПРАВО НА ЗАБВЕНИЕ В ИНДОНЕЗИИ: ЮРИДИЧЕСКИЕ АСПЕКТЫ И ПРОБЛЕМЫ

Аннотация. В статье рассматривается вопрос индонезийского права на забвение. Право на забвение позволяет удалять из поисковых систем информацию, распространяемую с нарушением законодательства, или недостоверную информацию. Индонезия стала первой страной в Азии, которая ввела в законодательство «право на забвение», однако в отечественной правоведческой науке данному вопросу было уделено мало внимания, что не умаляет актуальности темы в эпоху технологического развития. В результате исследования была выяснено следующее. У индонезийского права на забвение, помимо Конституции Индонезии, есть два непосредственных источника регулирования: Закона «Об информации и электронных транзакциях» от 2008 г. и Постановление Правительства № 71 от 2019 г. «О внедрении электронных систем и транзакций». В первом Законе указано, что каждый оператор электронной системы обязан удалить нерелевантную электронную информацию, на основании решения суда. Однако в этих нормативно-правовых актах нет ни самого понятия «право на забвение», ни его определении, а также нет разъяснения того, что имеется в виду под нерелевантной информацией.

Ключевые слова: цифровые технологии, цифровизация, цифровое право, индонезийское право, индонезийское цифровое право, право на забвение

RIGHT TO BE FORGOTTEN IN INDONESIA: LEGAL ASPECTS AND PROBLEMS

Abstract. This study addresses the issue of the Indonesian right to be forgotten. The right to be forgotten allows you to remove from search engines information that is distributed in violation of the law, or inaccurate information. Indonesia was the first country in Asia to introduce the "right to be forgotten" into its legislation, but little attention was paid to this issue in domestic jurisprudence, which does not detract from the relevance of the topic in the era of technological development. As a result of the study, the following was found. The Indonesian right to be forgotten, in addition to the Indonesian Constitution, has two direct sources of regulation: the Law on Information and Electronic Transactions of 2008 and Government Decree No. 71 of 2019 on the Implementation of Electronic Systems and Transactions. The first Law states that each operator of an electronic system is obliged to delete irrelevant electronic information, based on a court decision. However, in these legal acts there is neither the very concept of "the right to be forgotten" nor its definition, and there is no clarification of what is meant by irrelevant information. Instead, Government Decree No. 71 contains terms such as "right to erasure" and "right to delist", thus the Indonesian right to be forgotten is divided into two types at the time of the study.

Keywords: digital technologies, digitalization, digital law, Indonesian law, Indonesian digital law, right to be forgotten

Введение. В 2022 г. в Индонезии насчитывалось 204,7 миллиона пользователей интернет-услуг, что превышает половину ее общего населения [9. С. 111]. В результате цифровизации различных сфер общественной жизни, Индонезия, как и весь мир, превратилась в глобальную деревню, где благодаря Сети Интернет каждый пользователь может узнать о другом пользователе практически любую информацию. К сожалению, в Интернете могут оказаться разного рода персональные данные, будь то какие-либо фотографии или материалы из СМИ, которые субъект этих персональных данных хотел бы удалить из общего доступа. Доступ к электронной информации является одним из вызовов цифровизации. Как справедливо отметил Д. А. Пашенцев, «от того, будут ли найдены адекватные ответы на вызовы цифровизации, под которой понимается внедрение цифровых технологий во все сферы государственной и общественной жизни, зависит дальнейшее развитие правовой сферы общества» [5. С. 6]. Ответом на вызов в сложившийся ситуации является введение в законодательный массив такого понятия как «право на забвение»; 2017 г. принял парламент Индонезии, закрепив поправки к Закону № 11 от 2008 г. об информации и электронных транзакциях, на основании положений которых субъектам данных позволено запрашивать удаление их личных данных [11. С. 25].

Основная часть. Е. М. Подрабинок характеризует право на забвение как одно из «личных неимущественных прав гражданина, обеспечивающих его социальное существование в обществе» [6. С. 291]. *Арини Ферья Путри и Тантимин Тантимин полагают, что* право на забвение в Индонезии нельзя отделять от права

на неприкосновенность частной жизни при использовании информационных технологий [7. 168–187]. Более того, в индонезийском законодательстве гарантия права на забвение содержится в пар 1 ст. 28G, в котрой указано, что «Каждый человек имеет право на защиту личных данных…»

На момент 2016 г. Индонезия была единственной азиатской страной, которая обеспечила праву на забвение базу на законодательном уровне [8. С. 25]. В пп. 3-5 ст. 26 Закона № 19 от 2016 года «О внесении изменений в Закон № 11 от 2008 г. «Об информации и электронных сделках» указано, что каждый оператор электронной системы обязан удалить нерелевантную электронную информацию, электронные документы, на основании решения суда; каждый организатор электронной системы должен обеспечить механизм удаления нерелевантной электронной информации, электронных документов на основании статутного законодательства; положения о процедурах удаления электронной информации и электронного документа, регулируются государственными постановлениями» [4]. Данное положение представляет собой воплощение в индонезийском законодательном массиве право на забвение.

До поправок 2016 г. в старой версии Закона «Об информации и электронных транзакциях» от 2008 г. только предусмотрено, что лицо, чьи права нарушены в соответствии с пунктом, может подать иск о возмещении причиненных убытков на основании п. 1 указанного закона. Стоит отметить, что данное положение сохранилось после нововведений после 2016 г. [8].

В первоначальном тексте поправок к Закону от 2008 г. не говорилось о праве на забвение и касались только вопросов, связанных с диффамацией, перехватом сообщений, и т. д. Понятие «право на забвение» было предложено внести фракцией Партии национального мандата [7].

Предложение о поправках изначально не было немедленно принято, оно было отклонено на рабочей встрече I комиссии Совета народных представителей законопроекта о поправках к Закону «Об информации и электронных транзакциях», так как по словам министра связи и информатизации Рудиантары право на забвение имеет много аспектов, включая права человека, поэтому необходимо дальнейшее изучение, однако все же позднее предложение о поправке было принято [8].

Индонезийское право на забвение заключается в следующем. Запрос на удаление информации, принадлежащей субъекту данных, может быть подан только субъектом данных; запросы на удаление информации и электронных документов, принадлежащих субъектам данных, разрешены на основании решение суда; провайдер обязан удалить запрошенную информацию и предоставить механизм для удаления.

На основании ст. 1 Закона «Об информации и электронных транзакциях» от 2008 г стороной, ответственной за удаление информации, является провайдер, т. е. «лицо, государственный администратор, коммерческое предприятие и общество, которое предоставляет, управляет и (или) эксплуатирует электронные системы, индивидуально или коллективно, пользователям электронных системы для их собственной выгоды и (или) нужд других сторон». По мнению А. Рамли поставщики услуг социальных сетей могут быт отнесены к провайдерам, так как поставщики

услуг социальных сетей участвуют в процессе предоставления, управления, а также эксплуатации электронных систем. Помимо этого, поставщики услуг социальных сетей в качестве Провайдеров несут ряд обязательств по соблюдению стандартов безопасности и конфиденциальности своих пользователей, так как право на забвение является производным от права на неприкосновенность частной жизни. Пункт 3 статьи 26 Закона «Об информации и электронных транзакциях» гласит, что «каждый поставщик электронных систем обязан удалить любую электронную информацию и (или) электронные документы, которые больше не релевантны...». Несмотря на то, что в указанном Законе прямо не объясняется значение слова «релевантный» данный термин можно интерпретировать как информацию, которая все еще актуальна [9. С. 115–116]. Однако в Законе «Об информации и электронных транзакциях» от 2008 понятия «право на забвение» не было, а была лишь в ст. 26 отражена его суть.

В 2019 г. было издано Постановление Правительства № 71 от 2019 г. «О внедрении электронных систем и транзакций» (далее Постановление Правительства № 71), в положениях которого содержатся такие понятия как «право на удаление» и «право на делистинг» (право на удаление из поисковой системы), которые является обязательствами провайдеров.

В ст. 16 Постановления Правительства № 71 указано, что к информации, к которой применяется право на удаление, относят персональные данные, которые: получены и обработаны без согласия владельца персональных данных; согласие отозвано владельцем персональных данных; персональные данные были получены и обработаны незаконным путем; персональные данные больше не соответствует цели приобретения, основанной на соглашениях и положениях законов; использование персональных данных превысило время в соответствии с соглашением или положениями законодательства; отображаемые персональные данные наносят ущерб владельцу персональных данных [3].

Право на делистинг регулируется положениями ст. 17 Постановления Правительства № 71, в которой оно интерпретируется как исключение из списка электронной информации, которая больше не является релевантной для получения результатов поисковой системы. На основании решения суда провайдер обязан удалить нерелевантную информацию [9. С. 115–116].

Иными словами, после публикации Постановления Правительства № 71 индонезийский законодатель разделяет право на забвение на «право на удаление» и «право на делистинг» [12. С. 36–38]. Таким образом, в Индонезии существует два вида права на забвение – право на удаление информации и право на удаление из поиска.

Помимо этого, в п. 29 ст. 1 Постановления Правительства № 7 впервые появилось законодательное определение термина «персональные данные»: это любые данные о лице, идентифицированном и (или) идентифицируемом отдельно или в сочетании с другой информацией, прямо или косвенно посредством электронных и (или) неэлектронных Систем [3].

С одной стороны, в Законе «Об информации и электронных транзакциях» с поправками подчеркивается обязанность удалять ненужную электронную

информацию, а с другой стороны подчеркивается важность механизмов удаления на основании двух основных условий, а именно существенных требований и формальных требований, а именно механизма удаления электронной информации, не имеющей отношения к делу [6. С. 189–190].

1. Новая версия Закона «Об информации и электронных транзакциях» имеет важное значение в защите жертв киберпорнографии, так как, как указано выше, провайдер обязан удалить нерелевантную информацию. А. Ф. Путри, полагает, что положения о праве на забвение необходимо применять только в определенных случаях, таких как киберпорнография, и не применять к случаям коррупции или причинения ущерба государству [7. С. 183–185].

Как указано было выше, Индонезия была первой страной, которая в свое законодательство ввела понятие «право на забвение», поэтому у законодателя не было четкого ориентира для определения сферы действия права за забвение. Другой проблемой является наличие в индонезийском законодательном массиве Закона «О раскрытии публичной информации (UU KIP)», на основании которого предоставляется доступ к общедоступной информации. Если некоторые пользователи решат, что их доступ к общедоступной информации заблокирован, они могут подать жалобу в соответствующую инстанцию, в результате чего могут возникнуть конфликты между правами людей на получение информации и правом человека на удаление своей информации. Другой проблемой является судебное решение как необходимое условие для реализации права на забвение. Для успешной реализации права на забвение С. М. Рифки Новаль предлагает создать уполномоченное учреждение по вопросам права на забвение [10. С. 46–47]. Мы согласны с идеей автора, полагая, что создание такого учреждения снизит нагрузку с судов. Следующая проблема заключается в том, что в Законе «Об информации и электронных транзакциях» от 2008 г. нет понятия «право на забвение», а также нет разъяснения того, что имеется в виду под нерелевантной информацией [12. С. 36]. К. Рамадаани и М. Д. Муаалифин, полагают, что слишком общая формулировка этой ст.26 может привести к столкновению с рядом других законов и нормативных актов при ее применении, особенно с теми, которые касаются права общественности на информацию и свободу выражения мнений [8. С. 27].

2. Следующая проблема, заключается в том, что ни в Законе «Об информации и электронных транзакциях», ни в Постановлении Правительства № 71 не было учтено такое важное условие как реализация права на на забвение, которая связана с отсутствием технических регламентов, с помощью которых можно было бы обеспечить соблюдение этого права и не указаны конкретные способы реализации этого права, что порождает правовую неопределенность [12. С. 26–40].

Б. Зеллер указывает, что потенциальная проблема, которая может возникнуть в Индонезии, вероятно, связана с возможностью судьи действовать по своему усмотрению, которую суд может позволить себе в отношении того, когда, где и как следует удалять личные данные, если вообще следует их удалять [11. С. 34–35].

Заключение. Таким образом, у индонезийского права на забвение, помимо Конституции Индонезии, есть два непосредственных источника регулирования: Закон «Об информации и электронных транзакциях» от 2008 г. и Постановление

Правительства № 71 от 2019 г. «О внедрении электронных систем и транзакций». В новой версии от 2016 г. Закона «Об информации и электронных транзакциях» от 2008 г. указывается, что каждый оператор электронной системы обязан удалить нерелевантную электронную информацию, на основании решения суда, таким образом внедрив в законодательный массив право на забвение. Тем не менее в этих нормативно-правовых актах нет ни самого понятия «право на забвение», ни его определении, а также нет разъяснения того, что имеется в виду под нерелевантной информацией. Вместо этого в Постановлении Правительства № 71 содержатся такие термины как «право на удаление» и «право на делистинг», таким образом индонезийское право на забвение разделено на два вида.

Список литературы

1. Пашенцев Д. А. Российская законотворческая традиция перед вызовом цифровизации // Журнал российского права. 2019. № 2 (266). С. 5–13.

2. Подрабинок Е.. Особенности осуществления права на забвение в эпоху цифровизации общества. Пермский юридический альманах. Ежегодный научный журнал. 2019. № 1.

3. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

4. Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

5. Alycia C., Jatiswara. Aspek Hukum Liabilitas Public Figure Dan Upaya Perlindungan Terhadap Nama Dikaitkan Dengan Cancel Culture // Mimbar Hukum. Vol. 37, No. 1. Pp. 290–300.

6. Christianto H., Konsep hak untuk dilupakan sebagai pemenuhan hak korban revenge porn berdasarkan pasal 26 undang-undang informasi dan transaksi elektronik // Mimbar Hukum. 2022. Vol. 32 (2). Pp. 175–192.

7. Putri, A. F., & Tantimin. Tinjauan Yuridis Tindak Pidana Pornografi dan Penerapan Prinsip Right to be Forgotten di Indonesia // Jurnal Ilmu Hukum. 2022. Vol. 7 (1). Pp. 168–187.

8. Ramadaani, K., & Muaalifin, M. D. Analisis Yuridis Pengaturan Hak Untuk Dilupakan (Right To Be Forgotten) Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Legacy // Jurnal Hukum Dan Perundang-Undangan. 2023. Vol. 3(1). Pp. 18–41.

9. Ramli, Ahmad M; Safiranita, Tasya; Olivia, Denindah; and Millaudy, Reihan Ahmad Legal Aspect Of The Right To Be Forgotten (Rtf) On Social Media In Indonesia // Technology and Economics Law Journal. 2023. Vol. 1, No. 2. Pp. 18–41.

10. Rifqi Noval, S. M. The Challenge of Indonesia in Applying the Right to be Forgotten // International Journal of Crime, Law and Social Issues. 2020. Vol. 5(2). Pp. 39–49.

11. Zeller, Bruno and Trakman, Leon and Walters, Robert and Rosadi, Sinta Dewi, The Right to be Forgotten–The EU and Asia Pacific Experience (Australia, Indonesia,

Japan and Singapore) (January 1, 2019). (2019) 1 European Human Rights Law Review 23, UNSW Law Research Paper No. 19-2.

12. Yudiana, T. C., Rosadi, S. D., & Priowirjanto, E. S. The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia // Padjadjaran Jurnal Ilmu Hukum (Journal OF Law). 2022. Vol. 9(1). Pp 24–45.

И. Г. Ильин,
аспирант,
Санкт-Петербургский государственный университет

ПЕРСОНАЛЬНЫЕ ДАННЫЕ В СИСТЕМАХ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ТЕХНОЛОГИЯ ОБРАБОТКИ ЕСТЕСТВЕННОГО ЯЗЫКА

Аннотация. Статья посвящена концептуализации с точки зрения закона о защите персональных данных процесса развития технологии обработки естественного языка. В результате исследования было выявлено, что существующий правопорядок не в полной мере отвечает техническим особенностям развития данной технологии, что может привести или к излишнему регулированию, или же, напротив, оставить без внимания критические области, требующие защиты. В статье представлены основные проблемы и обозначены направления исследований.

Ключевые слова: право, цифровые технологии, персональные данные, искусственный интеллект, интеллектуальный анализ данных, технология обработки естественного языка, биометрические данные

PERSONAL DATA IN ARTIFICIAL INTELLIGENCE SYSTEMS: NATURAL LANGUAGE PROCESSING TECHNOLOGY

Abstract. The report focuses on the research results aimed at conceptualizing the development of natural language processing (NLP) from the perspective of data protection law. As a result of the research, it was identified that the existing legal regime does not fully meet the technical features of the development of NLP, which can lead to excessive regulation or, on the contrary, leave critical areas that require protection unattended. The following lecture notes aim to briefly describe the problems identified during the research and indicate the directions for further analysis.

Keywords: law, digital technologies, personal data, artificial intelligence, data mining, natural language processing technology, biometric data

Технология обработки естественного языка (англ. Natural language processing, NLP) активно используется в цифровых товарах и услугах (цифровых продуктах) для построения коммуникации между человеком и компьютером [2]. Голосовые помощники, сервисы перевода и озвучки текстов, системы интерактивного

ответа – все это примеры продуктов данной отрасли. В основе рассматриваемой технологии находятся генеративные нейросети, для обучения которых используются электронные лингвистические корпуса – базы данных, содержащие в себе множество текстов (книг, текстовых транскрипций, переводов и т. д.) и аудиофайлов (аудиокниг, записей трансляций, подкастов, другого аудиоконтента) [3, 8]. Создание лингвистических корпусов предполагает последовательное прохождение нескольких этапов: оцифровка языка – сбор, обработка и перевод данных в машиночитаемый формат, разметка корпуса и его последующий интеллектуальный анализ (англ. Text and data mining, TDM) [3–6].

В контексте создания лингвистических корпусов и развития технологии отдельную и важную роль приобретает вопрос использования данных, требующих особого режима правовой и технической защиты – персональных данных. В связи с этим принципиальными для разрешения становятся проблемы разграничения и категоризации персональных данных, пределов, до которых режим персональных данных будет влиять на процесс создания и развития названной технологии, а также частные случаи использования персональных данных, применительно к последующему ее распространению (прим. оплата цифровых услуг персональными данными).

Проблемы, связанные с разграничением и категоризацией персональных данных в общем смысле, объясняются необходимостью сначала выделить из объема всех используемых данных – персональные, а затем соотнести их с соответствующей категорией. Вместе с тем на практике это не всегда удается сделать: граница между персональными и другими данными не всегда четкая.

Во-первых, возникает проблема в определении самого понятия «данные». Из соотношения существующих норм можно сделать вывод о том, что данные – это данные, т. е. понятие определяется через само себя. Это создает трудности при попытках определить форму, в которой персональные данные могут быть выражены.

Во-вторых, действующее законодательство исходит из бинарного подхода к определению понятия персональных данных: данные могут быть либо персональными, либо нет. По мнению автора, такой подход не в полной мере учитывает современное состояние цифровизации общества, уровень технологического развития, а также последние социально-экономические изменения. Например, с точки зрения информатики и компьютерных наук выделяют разные уровни возможной идентифицируемости и относят к каждому из уровней определенный набор рисков [8, 9]. Кроме того, такое определение не учитывает, что данные могут быть идентифицируемыми для одного субъекта, например, в сочетании с другими наборами данных, но не для других [10].

В-третьих, статус данных в процессе обработки также может находиться в динамике и не быть статичным [11]. Иными словами, в процессе обработки данные могут становиться персональными и, наоборот, терять этот статус. Например, в процессе создания языковой модели на базе лингвистического корпуса, задействованные персональные данные теряют маркеры идентификации и, следовательно, теряют статус персональных [7].

Таким образом, в практическом смысле, данные в качестве персональных и можно квалифицировать только на определенный момент времени или этапе обработки, что может затруднить соблюдение законности всего процесса обработки.

Другая проблема, требующая решения – это проблема определения предела, до которого обработка данных должна соответствовать требованиям закона. Например, если языковая модель или корпус были созданы с использованием персональных данных, означает ли это, что дальнейшее использование продуктов, построенных на их базе, также попадает под действие закона о защите персональных данных?

Представляется, что пределы в обеспечении законности обработки персональных данных в рассматриваемом случае может быть определено через материальное, временное и территориальное действие правового регулирования в области защиты персональных данных [4]. Например, материальное действие можно определить через различные уровни использования персональных данных в создании соответствующих цифровых продуктов [7], временные пределы – через срок, в течение которого будет действовать право субъекта на защиту данных о нем, территориальные – через юрисдикции стран, в которых создаются или распространяются соответствующие цифровые продукты. Вместе с тем такой подход не может быть универсальным, а его применение влечет за собой ряд трудностей, таких как необходимость соблюдать регулирование в области защиты персональных данных, в том числе в отношении данных умерших людей и без какого-либо ограничения по сроками, необходимость одновременного соблюдения не только национального законодательства в области защиты персональных данных, но и законов других стран, так как цифровые продукты редко сосредоточены на одной стране, а реализуются на рынках разных стран и т. п.

Последней из обозначенных выше проблем является проблема использования персональных данных, применительно к процессу последующего распространения технология обработки естественного языка – оплате цифровых услуг персональными данными. Использование цифровых продуктов на базе описываемой технологии предполагает интенсивный обмен данными между пользователем и поставщиком [1]. Поставщик зачастую заинтересован в использовании этих данных не только для предоставления самого продукта, но и для его разработки, улучшения, а также в коммерческих целях. Например, голосовые данные могут быть использованы для анализа эмоциональной реакции на рекламный контент [12]. Однако возникает вопрос, насколько такое использование соответствует правовому режиму персональных данных? Представляется, что на сегодняшний день такое использование само по себе не запрещено, но должно осуществляться в строгом соответствии с действующим регулированием в области защиты персональных данных [13]. Вместе с тем остается открытым вопрос об определении данных как объекта права собственности [14], а также о характеристике возмездности соответствующих гражданско-правовых договоров.

Список литературы

1. Goldberg Y. Neural Network Methods for Natural Language Processing // Synthesis Lectures on Human Language Technologies. 2017. Vol. 10, № 1. Pp. 1–309.

2. Hirschberg J., Manning C. D. Advances in natural language processing // Science. 2015. Vol. 349, № 6245. Pp. 261–266.

3. Ilin I. Legal Regime of the Language Resources in the Context of the European Language Technology Development // Language and Technology Conference. Cham: Springer International Publishing, 2019. Pp. 367–376.

4. Ilin I. The Voice and Speech Processing within Language Technology Applications: Perspective of the Russian Data Protection Law // Legal Issues in the digital Age. 2020. № 1. Pp. 99–123.

5. Ilin I., Kelli A. The use of human voice and speech for development of language technologies: the EU and Russian data-protection law perspectives // Juridica Int'l. 2020. Vol. 29. Pp. 71–105.

6. Jents L., Kelli A. Legal aspects of processing personal data in development and use of digital language resources: the Estonian perspective // Jurisprudencija. – 2014. Vol. 21, № 1. Pp. C. 164–184.

7. Kelli A. et al. The interplay of legal regimes of personal data, intellectual property and freedom of expression in language research // Proceedings CLARIN annual conference. 2021. Vol. 2021. Pp. 154–159.

8. Kelli A., Tavast A., Pisuke H. Copyright and constitutional aspects of digital language resources // Juridica Int'l. 2012. Vol. 19. Pp. 40–64.

9. Kolain M., Grafenauer C., Ebers M. Anonymity Assessment-A Universal Tool for Measuring Anonymity of Data Sets under the GDPR with a Special Focus on Smart Robotics // Rutgers Computer & Tech. LJ. 2021. Vol. 48. Pp. 174–188.

10. Oostveen M. Identifiability and the applicability of data protection to big data // International Data Privacy Law. 2016. Vol. 6, № 4. Pp. 299–309.

11. Purtova N. The law of everything. Broad concept of personal data and future of EU data protection law // Law, Innovation and Technology. 2018. Vol. 10, № 1. Pp. 40–81.

12. Sartor G. et al. Study: New aspects and challenges in consumer protection. Digital services and artificial intelligence. European Parliament, 2020. Pp. 1–41.

13. Савельев А. И. Гражданско-правовые аспекты регулирования оборота персональных данных // Вестник гражданского права. 2021. Т. 21, № 4. Pp. 104–129.

14. Талапина Э. В. Закон об информации в эпоху больших данных // Вестник Санкт-Петербургского университета. Право. 2020. Т. 11, № 1. С. 4–18.

Д. А. Казанцев,
кандидат юридических наук,
электронная площадка B2B-Center

ПРАВО НЕЙРОСЕТИ: ФИКЦИЯ ИЛИ НЕОБХОДИМОСТЬ?

Аннотация. Статья посвящена специальному регулированию отношений, реализуемых с использованием искусственного интеллекта, и необходимости комплексного междисциплинарного подхода к формулировки соответствующих норм. На примере проблематики определения авторского права при создании результатов интеллектуальной деятельности с использованием нейросети раскрыта проблематика правовой субъектности искусственного интеллекта. Сформулирована идея о том, что даже в условиях отсутствия правовой субъектности результаты деятельности нейросети подлежат правовой охране, целью которой является соблюдение прав человека. Приведены доводы о необходимости специального регулирования отношений с использованием нейросети в рамках существующих отраслей права, сформулированы ключевые особенности такого специального регулирования. Предложен компромиссный подход к правовому регулированию нейросетей, при котором невозможность признания за ними правосубъектности не исключает их включения в правовые отношения, в том числе в части распространения правовой охраны на результаты их деятельности.

Ключевые слова: право, цифровые технологии, нейросеть, искусственный интеллект, правовая субъектность, авторское право, правовая защита

NEURAL NETWORK LAW: FICTION OR NECESSITY?

Abstract. The article is devoted to the regulation of relations implemented using AI. An interdisciplinary approach is required to develop such legislation. Using the example of the problems of determining copyright when creating results of intellectual activity using a neural network, the problems of the legal subjectivity of artificial intelligence are revealed. Even in the absence of legal subjectivity, the results of the neural network's activities are subject to legal protection, the purpose of which is to respect human rights. There is a need for special regulation of relations using a neural network within the framework of existing branches of law, and the key features of such special regulation are formulated. The work proposes a compromise approach to the legal regulation of neural networks, in which the impossibility of recognizing their legal personality does not exclude their inclusion in legal relations, incl. in terms of extending legal protection to the results of their activities.

Keywords: law, digital technologies, neural network, artificial intelligence, legal subjectivity, copyright, legal protection

Введение. Проникновение технологий искусственного интеллекта во все новые сферы жизни человека и общества ставит перед этим обществом вопросы об актуальности и возможности применения регуляторных механизмов к использованию таких технологий. Однако для юридической науки неуместно установление

регулирования ради регулирования. Регуляторные нормы должны быть адекватны как регулируемым отношениями, так и субъектам, реализующим такие отношения.

Этот подход ставит перед нами по меньшей мере два фундаментальных вопроса. Хотя тематика перспектив правового регулирования технологий искусственного интеллекта не ограничивается лишь этими вопросами, но в рамках данной статьи мы сфокусируемся именно на них:

Может ли нейросеть выступать в качестве правового субъекта?

Порождает ли деятельность нейросети отношения, регулирование которых в полной мере невозможно в рамках существующих правовых конструкций?

И хотя эти вопросы очевидным образом взаимосвязаны, они пригодны для обособленного исследования, а ответы на них не являются взаимно детерминированными.

Основная часть. Нейросеть де-факто действует как субъект отношений, демонстрирующий результаты обработки информации на уровне, превосходящем уровень человека, и порождающий собственные результаты интеллектуальной деятельности. И в качестве мыслящего и действующего субъекта она, на первый взгляд, выглядит вполне уместным кандидатом на роль правового субъекта.

Однако важно помнить о двух факторах. Во-первых, право, как институт всегда антропоориентировано. А во-вторых, подобие не означает тождества. Проще говоря, право онтологически ориентировано на регулирование поведения людей и отношений между людьми. И механистическое перенесение этого регулирования на иные формы когнитивной деятельности не просто сомнительно, но и невозможно.

В частности, правовая субъектность базируется на феномене правового сознания. Не отметая объективно существующие факты правового нигилизма, мы все же презюмирует правового субъекта способным к правовому сознания и должным поверять этим сознанием свое поведение. Однако можем ли мы требовать подобного сознания от нейросети? Не так уж сложно разработать алгоритмы, которые позволят нейросети маркировать те или иные решения в качестве противоправных. Однако, как включить в эти алгоритмы осознание виновности поведения?

Применение категорий «сознание» и «мышление» к нейросети означает упрощение ее деятельности путем придания ей антропоморфных черт. Это упрощение является естественной реакцией человека на то, что результаты обработки информации роботом становятся одновременно непредсказуемыми для человека и при этом тем самым все больше напоминают результаты мыслительной деятельности самого человека. Но при этом ни в коем случае не стоит забывать о том, что такая трактовка – именно упрощение.

Международные исследования ставят под вопрос корректность самого именования нейросетей искусственным интеллектом в смысле признания за ней возможности полноценного мышления и решения творческих задач [1]. Это ни в коем случае не означает умаление возможностей нейросети по обработки информации. Это свидетельствует лишь о том, когнитивная деятельность нейросети основана не на мышлении человеческого типа, а на совсем иных принципах. Именно эти принципы, кстати, обеспечивают результаты, в отдельных случаях превосходящие

результаты мышления человека. Но сами эти результаты свидетельствуют о том, что человеческий тип мышления и сознания нейросети не свойственен.

За этим логичным образом следует проблема деликтоспособности нейросети. Ей не только не свойственно чувство вины. К ней неприменимы и наказания, устоявшиеся в человеческих правоотношениях. На нейросеть не возложишь штраф или обязанность компенсировать причиненный ущерб, ее не направишь под арест или на исправительные работы.

Любая мера ответственности, которую гипотетический судья вздумал бы применить к нейросети, в конечном счете станет мерой ответственности для конкретного человека или корпорации. В этих условиях именно вина «посредников искусственного интеллекта (разработчиков и пользователей) в случае нанесения вреда системой искусственного интеллекта может быть вполне вероятной, юридически и экспертно доказуемой» [2. P. 42]. Например, Р. Линес и Ф. Люсиверо прямо говорят о том, что ответственность за вред, причиненный ИИ, несет лицо, его программировавшее, либо лицо, ответственное за его эксплуатацию, в установленных законом рамках [3].

В силу изложенных выше и иных сопряженных с ними особенностей работы нейросети приходится согласиться с выводом о том, что на сегодня нейросеть – да и искусственный интеллект в целом – едва ли могу быть отнесены к субъектам права. С точки зрения достигнутого уровня развития техники на сегодняшний день «очевидна несостоятельность предложения признания за искусственным интеллектом правосубъектности, аналогичной правосубъектности физического лица, и, несмотря на использование принципов работы человеческого мозга для построения системы искусственного интеллекта, принципы правового регулирования статуса физического лица не могут быть применены к искусственному интеллекту» [4. С. 33]. Наделение нейросети самостоятельной правосубъектностью означает лишь механистическую экстраполяцию прав человека на действия ИИ [5. P. 15.]. Остается лишенной внутреннего содержания.

Однако невозможность признания за нейросетью самостоятельной правовой субъектности не означает невозможности включения нейросети в правовые отношения. Ведь даже признавая преждевременным положительное решение вопроса о правосубъектности роботов, нужно согласиться с мыслью «о необходимости сработать на опережение, нормативно закрепить обязанность разработчиков и других уполномоченных лиц предпринимать все необходимые меры, обеспечивающие в процессе функционирования искусственного интеллекта интересы человека, и разработать систему норм, обеспечивающих исполнение этой обязанности» [4. С. 33].

Несколько упрощая, в международной дискуссии можно выделить несколько ключевых подходов к решению этого вопроса: констатация отсутствия возможности признания правосубъектности за искусственным интеллектом и возложения всех правовых последствий его деятельности на человека как субъекта права [6. P. 1101], применение юридической фикции с установлением для искусственного интеллекта правосубъектности, подобной правосубъектности юридических лиц [7. P. 155, 161], или даже формирование новой отрасли законодательства,

посвященной специфическому регулированию статуса искусственного интеллекта и релевантной этой специфики [8].

Заслуживает внимание мнение российских исследователей о том, что сегодня «наиболее рациональным, но не бесспорным видится использование концепции правосубъектности искусственного интеллекта по типу юридического лица либо электронного лица; подход к правовому регулированию в рамках юридической ответственности, связанной с пользователями, владельцами или производителями систем искусственного интеллекта, а не с технологическими объектами» [9. С. 46].

Важно подчеркнуть: речь идет не о распространении правового режима юридического лица на нейросеть, а именно об использовании опыта правовой фикции для регулирования работы важного участника правоотношений. Проще говоря, правовой режим искусственного интеллекта должен быть отличен и от правосубъектности физического лица, и от статуса юридического лица. Однако наличие такого правового режима представляется все более и более актуальной.

Эта актуальность обуславливается тем, что отношения, реализуемы с использованием нейросети, хотя пока еще и регулируются нормами традиционных институтов права, однако в таком регулировании все чаще и чаще применяется аналогия. Это неизбежно, поскольку сами по себе отношения с привлечением технологий искусственного интеллекта представляют собой принципиально новый объект регулирования. И этот объект требует новых регуляторных норм.

Невозможно в рамках одной статьи охватить все многообразие реальных и потенциальных сфер применения технологий искусственного интеллекта. Однако для иллюстрации вопросов правового порядка, сформулированных выше, в достаточной мере наглядным примером представляется пока еще относительно узкая сфера использования нейросети для создания объектов интеллектуальной собственности.

На сегодня дискуссия о возможности признания авторства за нейросетью остановилась на констатации того, что нейросеть является не субъектом, а инструментом творческой деятельности. Однако при этом важно разделять посылку и вывод следующего экспертного суждения: «в деятельности искусственного интеллекта по созданию результатов, похожих на объекты авторского права, отсутствует творчество, поэтому созданные им результаты не могут быть квалифицированы в качестве объектов авторского права и не подлежат охране правом интеллектуальной собственности» [10. С. 21]. Если мысль об отсутствии в работе нейросети компоненты творчества в собственном смысле этого слова не вызывает возражений, то отказ на этом основании в охране правом интеллектуальной собственности представляется сомнительным.

Невозможность признания авторства за нейросетью не исключает авторства на результаты ее деятельности. Самым простым, хотя и не единственным, подходом к определению авторства в данном случае может служить признание автором того физического лица, творческий импульс которого и послужил отправной точкой для работы нейросети. Проще говоря, того, кто задал ей уникальную комбинацию ключевых слов или последовательность таких комбинаций. Здесь можно

вспомнить прецедент XIX в., когда фотоаппарат казался почти такой же инновацией, какой сегодня для нас кажется нейросеть: в деле «Литографическая компания Берроу-Джайлз против Сарони» 17 марта 1884 г. Верховный суд Соединенных Штатов Америки признал авторские права на конкретную фотографию не за фотоаппаратом и не за его изготовителем, а за фотографом [11].

В этих условиях «введение права на результат деятельности искусственного интеллекта может строиться по модели смежного права, однако оно явно теряет свою связь с авторским правом, а потому уместно, на наш взгляд, в данном ключе говорить о праве sui generis на цифровые результаты деятельности искусственного интеллекта» [12. С. 82]. Причем такие результаты будут существенным образом отличаться от привычных нам результатов интеллектуальной деятельности.

Во-первых, как уже было означено выше, творческий вклад человека хотя и остается решающим фактором в создании текста, изображения или музыкального произведения, но при этом творческие усилия автора при создании такого произведения несоизмеримо меньше по сравнению с активностью нейросети по обработке авторского запроса.

Во-вторых, при обработке такого запроса нейросеть не создает действительно нового контента, а идет путем глубокой обработки уже существующих текстов, изображений и музыкальных произведений. Это ставит перед нами вопрос о необходимости формирования новых стандартов цитирования и заимствования, но стандартов не для права интеллектуальной собственности в целом, а именно для правового регулирования создания произведений с использованием нейросети.

Таким образом, произведения нейросети не должны оставаться вне рамок правового регулирования и правовой защиты – но при этом и существующие правовые институты применять к ним все сложнее и сложнее. В данной парадигме целесообразным представляется согласие с тезисом «о существовании предпосылок для появления в праве интеллектуальной собственности нового правового института – института права на результаты деятельности искусственного интеллекта. Институт является sue generis в рамках права интеллектуальной собственности и не сводится к традиционному авторскому, патентному праву, институту смежных прав и других, хотя в определенной части и основывается на конструкциях таких традиционных институтов» [13. С. 28].

Заключение. За рамками данной статьи остаются многие вопросы, связанные с правосубъектностью искусственного интеллекта, такие как, например, статус робота-водителя или робота врача и потенциальной ответственности за причиненный ими вред. Этим вопросам посвящены специальные исследования, которые в основном склоняются к выводу о субсидиарной ответственности [14. P. 453, 480] – а точнее, о матрице ответственности, на основании которой вопрос о возложении неблагоприятных правовых последствий решается индивидуально в каждом конкретном случае с учетом комплекса фактов [15. P. 81].

Однако и приведенного примера проблематики регулирования правового режима результатов интеллектуальной деятельности, созданных с участием искусственного интеллекта, достаточно для понимания необходимости новых правовых институтов. Нейросеть заметным образом изменяет привычные отношения.

А значит, невозможность наделить нейросеть правами в существующем смысле этого слова не может означать отсутствие правового регулирование для отношений, в которых участвует нейросеть.

Применение к работе нейросети существующих норм – например, норм авторского права на производные произведения – возможно лишь по аналогии. И по мере развития технологий нейросети эта аналогия с неизбежностью будет становиться все более условной, требуя создания специальных норм, учитывающих специфику работы технологий искусственного интеллекта.

Разработка таких норм требует широкой дискуссии экспертного сообщества на междисциплинарной основе, поскольку выводы юридической науки в данном случае с неизбежностью будут строго детерминированы реальностью информационных технологий. Но при этом уже сегодня ясно, что нормы права нейросетей могут и должны быть созданы на основании модификации существующих институтов.

Проще говоря, регулирование искусственного интеллекта не требует революции в праве. С точки зрения системы права нормы, посвященные искусственному интеллекту, могут применяться в качестве специальных норм в рамках уже сложившихся институтов. Вот только формулировка самих этих норм потребует принципиально нового взгляда на мир с учетом новых цифровых реальностей.

Список литературы

1. Lee J-.A., Hilty R., & Liu K-.C. (Eds.). Artificial intelligence and intellectual property. Oxford University Press, 2020.

2. Bertolini A. Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules // Law, Innovation and Technology. 2013. Vol. 5.

3. Leenes R., Lucivero F. Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design // Law, Innovation and Technology. 2014. Vol. 6. Iss. 2. Pp. 194–222.

4. Дурнева П. Н. Искусственный интеллект: анализ с точки зрения классической теории правосубъектности // Гражданское право. 2019. № 5.

5. Nevejans N. European Civil Law Rules in Robotics: Study. European Union, 2016.

6. Calo R., Chizeck H. J., Joh E., Hannaford B. Panel 2: Accountability for the Actions of Robots // Seattle University Law Review. 2018. Vol. 41.

7. Solaiman S. M. Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy // Artificial Intelligence and Law. 2017. Vol. 25.

8. Cofone I. Servers and Waiters: What Matters in the Law of AI // Stanford Technology Law Review. 2018. Vol. 21.

9. 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.

10. Витко В. Анализ научных представлений об авторе и правах на результаты деятельности искусственного интеллекта // Интеллектуальная собственность. Авторское право и смежные права. 2019. № 3. С. 5–22.

11. Burrow-Giles Lithographic Co. v. Sarony. URL: https://www.law.cornell.edu/supremecourt/text/111/53

12. Харитонова Ю. С. Правовой режим результатов деятельности искусственного интеллекта // Современные информационные технологии и право: монография / Московский госуниверситет им. М. В. Ломоносова, Юридический факультет / отв. ред. Е. Б. Лаутс. М.: Статут, 2019.

13. Аникин А. С. К вопросу об охраноспособности результатов деятельности искусственного интеллекта как объекта интеллектуальной собственности // Цивилист. 2022. № 2.

14. Duffy S. H., Hopkins J. P. Sit, Stay, Drive: The Future of Autonomous Car Liability // SMU Science & Technology Law Review. 2013. Vol. 16.

15. Colonna K. Autonomous Cars and Tort Liability // Case Western Reserve Journal of Law, Technology & the Internet. 2012. Vol. 4.

О. Г. Кирсанова,
кандидат экономических наук, доцент,
Финансовый университет
при Правительстве Российской Федерации
(Смоленский филиал)

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНСТИТУТА КОММЕРЧЕСКОЙ ТАЙНЫ И ЕЕ ЗАЩИТА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

Аннотация. В статье рассмотрены актуальные проблемы защиты коммерческой тайны в условиях цифровизации экономики. Проанализированы основные подходы к определению содержания категории «коммерческая тайна», приводится правовая статистика в рамках рассмотрения дела, связанных с нарушением коммерческой тайны. Выявлены основные угрозы и направления правового регулирования института коммерческой тайны и ее защиты.

Ключевые слова: коммерческая тайна, разглашение информации, конфиденциальность, информационная безопасность, защита

LEGAL REGULATION OF THE INSTITUTE OF TRADE SECRETS AND ITS PROTECTION IN THE CONDITIONS OF DIGITALIZATION OF THE ECONOMY

Abstract. The article discusses the current problems of protecting trade secrets in the conditions of digitalization of the economy. The main approaches to the definition of the content of the category “trade secret” are analyzed, legal statistics are considered and analyzed in the framework of the consideration of causes related to the violation of trade secrets. The main threats and directions of legal regulation of the institute of commercial secrets and its protection are identified.

Keywords: trade secret, disclosure of information, confidentiality, information security, protection

Процессы цифровизации, которые в последнее время достаточно активно и тесно интегрируются в коммерческую деятельность субъектов хозяйствования различных организационно-правовых форм, наряду с возможностями, которые открываются в рамках расширения сферы присутствия, наращения клиентской базы посредством использования современных технологий продвижения бренда или продукта, создают угрозы потери конкурентных преимуществ, прежде всего в силу утраты или публичного разглашения коммерческой тайны, являющейся одним из наиболее привлекательных объектов для коммерческого или промышленного «шпионажа» или пришедших им на смену более эффективных хакерских атак на IT-инфраструктуру предприятия, что актуализирует роль правового регулирования и защиты института коммерческой тайны.

Изучение содержания коммерческой тайны и механизма ее правового регулирования и защиты возрастает в условиях цифровизации социально-экономических процессов, которая сопровождается расширением присутствия бизнеса в виртуальной среде, что в свою очередь, способно привести к риску утраты информации, составляющей коммерческую тайну, что подтверждается ростом в течение трех последних лет числа утечек внутренней корпоративной информации различного содержания (преимущественно персональных данных, финансовой информации и т. п.).

Согласно данным ГК InfoWatch, в течение 2019–2022 гг. по ст. 183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайны», было осуждено: в 2019 г. – 41 чел.; в 2020 г. – 35 чел., в 2021 г. – 41 чел., в 2022 г. – 47 чел. Положительная динамика в течение 2019–2022 г. составила 6 случаев, что соответствует 13,7 % [6].

Согласно данным ГАС «Правосудие», в 2019 г. в рамках обозначенной статьи УК РФ в течение 2019–2022 г. было осуждено 69 чел., 70 чел., 40 чел., 42 чел. соответственно, что соответствует росту в 2022 г. в сравнении с 2021 г. на 5,4 %, отражая положительную динамику последних двух лет.

На фоне общего объема утечек информации, рост которых в течение 2022 г., согласно данным ГК InfoWatch, составил 45 %, на долю потери данных, которые составляют категорию коммерческой тайны, пришлось 13 %, что соответствует 305 базам похищенной информации или 187,6 млн записей. В течение 2022 г. профильные компании отразили в 4,5 раза больше атак в сравнении с 2021 г., что к росту затрат, необходимых для ликвидации кибератак и проникновения хакеров в IT-инфраструктуру хозяйствующих субъектов на 20 %. При этом, как отмечает руководитель направления аналитики и спецпроектов ГК InfoWatch Андрей Арсентьев, данные, которые составляют коммерческую тайну, являются востребованными в настоящее время по причине возрастания конкурентной борьбы, преследуя цель причинения максимально возможного экономического ущерба конкуренту, в том числе посредством кражи конфиденциальных данных. Сложившаяся ситуация для бизнеса влечет за собой рост затрат, связанных с потребностями

и задачами улучшения информационной безопасности, что, согласно экспертной оценке заместителя генерального директора дата-центра и облачного провайдера Oxygen Кирилла Орлова, в общем IT-бюджете крупных корпораций составит 12–15 %, в то время как для небольших компаний станет достаточно обременительным [7].

Приведенные данные позволяют сделать вывод об актуальности правового регулирования и защиты института коммерческой тайны как конкурентного фактора хозяйствующего субъекта, который имеет длительную историю и зависим от экономической и технологической трансформации общества.

В. Д. Саттаров отмечает, что формирование и правовое регулирование института коммерческой тайны в российском праве можно проследить, начиная с периода Российской империи вплоть до перехода к рыночных отношениям в 1990 гг., анализ которого достаточно подробно представлен в исследованиях А. А. Фатьянова, в то же время в работах З. Р. Игбаевой и И. С. Корокрина можно увидеть указание на более ранний период формирования коммерческой тайны и ее правового регулирования, который начинается в период Античности [4. С. 120].

В настоящее время институт коммерческой тайны регулируется нормами ст. 23 Конституции Российской Федерации, ч. 2 которой закреплено право каждого на тайну переговоров, переписки, сообщений, при этом под «каждым» целесообразно понимать и хозяйствующие субъекты, являющиеся обладателями коммерческой тайны. Коммерческая тайна, как отдельный институт и объект правового регулирования, определена в ч. 1 ст. 3 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне», и представляет собой сведения, наделенные следующими признаками: наличие потенциальной или реальной ценности, способной принести ее обладателю прибыль либо любую иную выгоду; ограниченность доступа к данным сведениями для третьих лиц, которые, находясь за пределами бизнес-единицы могут не знать о наличии коммерческой тайны или ее содержании; доступ к такой информации ограничен для круга лиц, отвечающих непосредственно на реализацию режима коммерческой тайны, вводимого ее обладателем для защиты сведений, составляющих коммерческую тайну [6. С. 330].

Другими словами, коммерческая тайна в рамках правового регулирования отнесена к информации ограниченного доступа, при этом перечень субъектов, которые могут быть допущены к сведениям, устанавливается ее обладателем, что определяет особенности ответственности и обязанности его в рамках защиты коммерческой тайны от разглашения во внешней среде.

Ценность коммерческой тайны, обуславливающей высокие риски и угрозы ее разглашения, обусловлена тем, что содержащаяся в ней информация позволяет обеспечить формирование конкурентных преимуществ обладателя, сократить его затраты на реализацию хозяйственных процессов, либо получить более высокую в сравнении с конкурентами прибыль. Как правило, к таким сведениям могут быть отнесены перечень клиентской базы с персональными данными клиентов, результаты маркетинговых исследований рынка или научно-технических изысканий, полезные модели, позволяющие оптимизировать производственный цикл и снизить его затраты и прочие сведения, которые представляют корпоративную

ценность и не могут быть опубликованы во внешней среде, поскольку направлены на получение ее обладателем более высокого дохода или обретения конкурентного преимущества.

Особенностью правового регулирования института коммерческой тайны является право, предоставленное ее обладателю, самостоятельного определения ценности имеющейся информации и отнесения ее к категории повышенной конфиденциальности, что в ряде случаев может привести к злоупотреблению правом и сокрытию информации, которая будет иметь важное общественное значение. Во избежание подобных ситуаций ст. 5 Федерального закона № 98-ФЗ «О коммерческой тайне» определен перечень сведений, которые не могут быть отнесены к категории коммерческой тайны, подлежат опубликованию, субъект, осуществивший их разглашение не может быть привлечен к ответственности.

В. Д. Саттаров выделяет три информационных блока таких сведений:

– информация, обеспечивающая предпринимательскую деятельность, в т. ч. в части взаимодействия бизнес-единицы с другими субъектами, например, ФНС России, банками, инвесторами, социальными фондами и т. п.;

– информация, имеющая общественно важный характер (например, сведения о кандидатах, баллотирующихся в органы государственной власти или местного самоуправления, сведения об исполнении бюджета, данные о доходах государственных служащих и т. п.);

– информация, содержащая общественно важные сведения, обязательное опубликование которых прямо закреплено правовыми нормами (например, опубликование данных о выбросах в атмосферу отравляющих веществ или иных техногенных рисках, сейсмологических угрозах и выявленных в процессе фитосанитарного и ветеринарного контроля рисках заражения домашних животных и т. п.) [5. С. 122].

В данном случае прослеживается взаимосвязь со шведским правовым институтом коммерческой тайны «whistle-blowing», буквально означающего «право свистеть», который В. Н. Монахов характеризует как «нельзя держать в секрете то, что в интересах общества должно быть разглашено» [4. С. 122], что положено в основу регулирования отношений, связанных с разрешением спроса между администрацией предприятия и его сотрудниками, которые опубликовали информацию, имеющую общественно важное значение (например, о выбросе отравляющих веществ в атмосферу и т. п.), в отношении которых сформирована соответствующая судебная практика.

В 2019–2022 гг. в судах первой инстанции 53,7 % дел были рассмотрены в рамках только ст. 183 УК РФ, направленной на защиту интересов субъектов бизнеса, ущерб которым был причинен разглашением коммерческой тайны, 46,3 % дел были сопряжены с обвинениями по другим статьям, например, ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», в большинстве случаев по ч. 3 «Деяния, …, совершенные группой лиц по предварительному сговору или организационной группой лиц либо одним лицом с использованием служебного положения».

В случае применения только ст. 183 УК РФ большая часть дел (56,1 %) была рассмотрена по ч. 3 упомянутой статьи, 36,59 % дел были рассмотрены в рамках ч. 2 и 7,31 % – в рамках ч. 1, что позволяет сделать вывод о том, что как правило, преступления и правонарушения, касающееся разглашения коммерческой тайны и опубликования данных, осуществляются должностными лицами организации – обладателя по предварительному сговору и большей части в корыстных целях [7. С. 10].

В большинстве случаев возбужденные дела касались разглашения и намеренной передачи сотрудниками операторов связи информации абонентов (персональных данных, детализации звонков и т. п.), передачи банковскими служащими информации, относимой «банковской тайне» (информация о картах, состоянии счетов клиентов банков и т. п.).

По результатам рассмотрения дел в 44,3 % судами были вынесены обвинительные приговоры, в 39,9 % дела прекращались на основании примирения сторон либо по ходатайству следователя, а также по иным основанием. В отношении 1,1 % дел были вынесены оправдательные приговоры, а также 1,6 % были возвращены следствию [7. С. 12].

При вынесении обвинительных приговоров суды в большинстве случаев (44,7 %) назначали административный штраф, средний размер которого составил 123,8 тыс. руб., максимальный размер – 1 млн руб., минимальный – 8 тыс. руб.). В 36,9 % случаях вынесения обвинительного приговора судами назначен условный срок отбывания наказания (от 6 мес. по одной статье, до 4 лет – по совокупности статей). В 9,2 % обвинительных приговоров были назначены исправительные работы, а также в 9,2 % обвинительных приговоров судами было определено отбывание наказания в исправительных колониях общего режима.

Набирающий в настоящее время процесс цифровизации оказывает все большее влияние на предпринимательский сектор, вынуждая субъекты бизнеса, которые хотят сохранить свою конкурентоспособность и привлекательность среди клиентов и партнеров, расширять сферу присутствия в виртуальной бизнес-среде, вырабатывая новые подходы к формированию баз данных и управлению информацией.

Актуальным трендом, который обозначился в период пандемии COVID-2019, стал удаленный формат работы, закрепивший к настоящему времени практику взаимодействия с клиентами или стейкхолдерами в дистанционном формате, используя современные коммуникационные технологии (например, платформы конференцсвязи) и онлайн-банки при осуществлении необходимых расчетных операций. Параллельно активными темпами осуществляется процесс цифровизации внутренней информации хозяйствующего субъекта, касающейся персональных данных, сведений о способах осуществления производственной и коммерческой деятельности, результатов исследований рынков, ноу-хау и иной информации, которая может обеспечить конкурентное преимущество данного субъекта и принести ему прибыли, и перевод ее в облачные системы хранения, что приводит к замещению классических схем «промышленного шпионажа» хакерскими атаками, которые могут быть куда более болезненными для бизнес-субъекта в части причинения коммерческого ущерба.

Начавшаяся несколько лет назад цифровизация общественной жизни привела, по мнению В. Н. Монахова, к существенным изменениям коллективного сознания, что обусловило переход к поиску новых форм работы с информацией и ее защите [4. С. 123].

В настоящее время риски утраты и опубликования коммерческой тайны возрастают вследствие расширения присутствия ее обладателя в виртуальной среде. Согласно данным записей ГАС «Правосудие», в рамках ст. 183 УК РФ в 37,4 % случаев опубликование коммерческой тайны осуществлялось при помощи ресурсов сети Интернет; 37,4 % – с помощью сервисов мгновенной передачи сообщений (мессенджеров); в 6 % случаев информация передавалась при помощи электронной почты; в 3,6 % – на съемных носителях; в 12 % – на бумажных архивах; в 3,6 % – при помощи устных сообщений. В 70,4 % случаев субъектами, которые осуществили разглашение информации, содержащей коммерческую тайну, являлись непривилегированные сотрудники, занимающие невысокое должностное положение в организации [7. С. 17–18].

Как отмечалось, основным инструментом защиты коммерческой тайны, создающим возможности для разрешения противоречий в рамках судебного процесса, является обязанность ее обладателя установить режим коммерческой тайны, наделяющий его правом самостоятельного определения и регулирования правил доступа к информации, отнесенной им же к категории коммерческой тайны. При этом законодатель подчеркивает, что защиты коммерческой тайны посредством соответствующего режима является не правом, а обязанностью ее обладателя и традиционно предусматривает следующие мероприятия:

– формирование перечня сведений, которые составляют коммерческую тайну на основе признаков, ее характеризующих;

– определение круга пользователей сведений, содержащих коммерческую тайну, которые могут их использовать в процессе решения текущих задач, или определение круга субъектов, которые являются представителями внешней бизнес-среды, однако будут наделены правом доступа к коммерческой тайне в силу взаимных коммерческих интересов;

– формирование системы учета и контроля использования сведений, составляющих коммерческую тайну, и предупреждение их нежелательного опубликования во внешней среде.

Вместе с тем, как показывает статистика, наработанных к настоящему времени мер и рекомендаций по защите коммерческой тайны в актуальных условиях цифровизации информационных потоков недостаточно. Очевидно, что существующие традиционные направления защиты должны претерпеть правовую и цифровую трансформацию.

В качестве предупредительных мер на уровне администрации по защите коммерческой тайны повышается роль криптографического преобразования информации. Вследствие высокого уровня риска ее разглашения посредством сетевых ресурсов или мессенджеров в ряде компаний ограничивается доступ к средствам связи в течение рабочего дня не только для допущенных к работе со сведениями, содержащими коммерческую тайну, сотрудников, но и всего коллектива в целом.

При этом в части рассмотрения дел, связанных с утечкой информации посредством ее размещения на личных страницах в социальных сетях или хранения в электронном почтовом ящике, к настоящему времени отсутствует однозначная правовая позиция.

Так, Постановлением Конституционного суда России от 26.10.2017 № 25-П определено, что случай, связанный с отправлением работником на личный адрес электронной почты персональных данных других сотрудников, служебных документов и прочей конфиденциальной информации в целях продолжения работы с ними дома, следует считать разглашением коммерческой тайны, поскольку компания – владелец почтового сервера получила доступ к пересылаемым охраняемым законом данным. Увольнение сотрудника было признано правомерным. Подобную правовую позицию достаточно часто можно встретить в судебных решениях по аналогичным ситуациям.

Постановление Пленума Верховного Суда Российской Федерации от 17.04.2003 № 2 «О применении судами Российской Федерации Трудового кодекса Российской Федерации» делает обязательным доказывание обладателем ценности разглашенной сотрудником информации как коммерческой тайны, на основе которой оценивается объективность и целесообразность принятого решения об увольнении такого сотрудника и возмещении при необходимости причиненного материального ущерба. На наш взгляд, регулирование процедуры доказывания представляет собой правовой пробел, поскольку в настоящее время сохраняется высокий уровень субъективности в доведении информации до суда, который, в свою очередь, также принимает решение, основываясь на внутреннем убеждении.

Считаем целесообразным в рамках развития института коммерческой тайны и правового регулирования механизмов ее защиты проработать в целях большей объективности аспект, связанный с доказыванием настоящей или будущей ценности разглашенной информации, и определением размера ущерба, который был причинен обладателю коммерческой тайны противоправными действиями третьих лиц.

В настоящее время законодатель предоставляет обладателю коммерческой тайны достаточно широкое правовое поле для ее защиты, ограничивая его лишь гарантией и защитой конституционных прав и свобод человека и гражданина. Следовательно, права и обязанности обладателя коммерческой тайны должны быть направлены на формирование и внедрение внутренних регламентов ее защиты, которые могут быть представлены в виде локального нормативного акта, основанного на нормах действующего законодательства и четко прописывающего основные положения механизма защиты коммерческой тайны, приоритетными из которых являются следующие:

– формирование практики разработки и подписания соглашений о неразглашении информации сотрудниками, имеющими к ней допуск с обязательным ознакомлением с правовыми последствиями в виде различных форм и видов ответственности, предусмотренной отдельными правовыми нормами;

– организация и совершенствование системы контроля физического и электронного доступа к информации на уровне внутренних регламентов использования

внешних съемных носителей, общения в социальных сетях, которые в последнее время активно используются для внутрикорпоративного обмена информацией или сервисах мгновенной передачи сообщений;

– формирование многоступенчатой системы защиты информации с сужением круга лиц, допущенных к ее использованию с подписанием на каждом уровне соответствующего соглашения о неразглашении;

– обучение сотрудников основам работы с информацией, составляющей коммерческую тайну в информационно-коммуникационных сетях (в ряде случаев ее разглашение осуществляется непроизвольно вследствие недостаточно развитых навыков работы с такими ресурсами), а также формирование высокого уровня корпоративной культуры, приоритетным элементом которой станет защита коммерческой тайны.

Подводя итог, отметим, что в настоящее время защита коммерческой тайны от ее неправомерного использования является одним из наиболее острых и проблемных аспектов информационного и предпринимательского права, что обусловлено влиянием процесса цифровизации на принципы и способы работы с корпоративной информацией. Законодатель, создавая обширное правовое поле для защиты конфиденциальной информации, наделяет существенными правами ее обладателя в части защиты коммерческой тайны, фактически вменяя данный процесс в его прямые обязанности, что позволяет выработать и развивать эффективную систему защиты коммерческой тайны в рамках действующего законодательства.

Анализ правоприменительной практики по ст. 183 УК РФ позволяет сделать вывод о возрастающей динамике случаев разглашения коммерческой тайны, что особенно опасно в условиях расширения сферы применения информационных ресурсов в практике хозяйственной деятельности и присутствия бизнес-субъекта в виртуальной бизнес-среде. Следовательно, сформированных к настоящему времени механизмов защиты коммерческой тайны силами ее обладателей недостаточно, что обуславливает актуальность проведения дальнейших исследований практических аспектов работы с информацией, составляющей коммерческую тайну и совершенствование правовых механизмов ее регулирования.

Список литературы

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020. URL: https://www.consultant.ru

2. Уголовный кодекс Российской Федерации: федеральный закон от 13.06.1996 № 63-ФЗ. URL: https://www.consultant.ru

3. О коммерческой тайне: федеральный закон от 29.07.2004 № 98-ФЗ. URL: https://www.consultant.ru

4. Монахов В. Н. Утро пятой свободы (к проблеме совершенствования правового режима свободы информации и знаний как ценностей и драйверов развития) // Право. Журнал Высшей школы экономики. 2014. № 3. С. 121–135.

5. Саттаров В. Д. Право коммерческой тайны в условиях цифровизации общества // Пермский юридический альманах. 2019. № 2. С. 119–127.

6. Сафиуллин А. Р., Смирнова В. С. Коммерческая тайна и ее защита в цифровой экономике // Вузовская наука в современных условиях: сборник материалов 57-й научно-технической конференции. Часть 2. Ульяновск: Издательство УлГТУ, 2023. С. 330–332.

7. Исследование судебной практики по уголовным делам, связанным с незаконным получением и разглашением сведений, составляющих коммерческую, налоговую или банковскую тайну, 2019–2021 гг. // Экспертно-Аналитический центр InfoWatch, 2022 г. 25 с.

8. В России растет число утечек данных, составляющих коммерческую тайну. URL: https://habr.com/ru/news/682834

Ю. А. Комнатная,
кандидат юридических наук,
Белгородский государственный национальный
исследовательский университет

ПРАВО НА ИНФОРМАЦИЮ И ИНФОРМАЦИОННАЯ ВОЙНА

Аннотация. Статья посвящена вопросам соотношения понятий «право на информацию» и «право на доступ к информации» с целью выяснения содержания данных прав для определения их пределов, гарантирующих цифровую и, соответственно, национальную безопасность. Уделено внимание истории развития информационных войн, эффективности различных методов информационной войны при отсутствии должного контроля за информационными потоками со стороны государства. Определен главный критерий информации, а также обозначена необходимость введения института ответственности международных должностных лиц за распространение и использование недостоверной информации, который позволит обеспечить минимальную безопасность государств на международном уровне.

Ключевые слова: информация, право на информацию, право на доступ к информации, информационная война, достоверность информации, цифровая безопасность

THE RIGHT TO INFORMATION AND INFORMATION WARFARE

Abstract. The article is devoted to the relationship between the concepts of «right to information» and «right to access to information» in order to clarify the content of these rights to determine their limits, guaranteeing national security. Attention is paid to the history of the development of information wars, the effectiveness of various methods of information warfare in the absence of proper control over information flows by the state. The main criterion of information is defined, as well as the need to introduce the institution of responsibility of international officials for the dissemination and use of false information, which will ensure minimal security of states at the international level.

Keywords: information, right to information, right to access information, information war, adequacy of information, digital security

Право на информацию в современной доктрине не определено. На международном уровне право на информацию (свобода информации) было закреплено как фундаментальное право человека Генеральной Ассамблеей ООН в 1946 г. (Резолюция 59(I), принятая на первой сессии ГА ООН 14 декабря 1946 г.). Однако в доктрине до конца не разрешен вопрос как соотносятся право на информацию и право на доступ к информации. В. П. Кириленко, Г. В. Алексеев отмечают, что большинство национальных правительств толкует указанные права как элемент базового права граждан на свободу мнения и его свободное выражение [2. С. 40]. В. Д. Клюков предполагает, что неоднозначность восприятия права на информацию связана с самим процессом его эволюции [3. С. 346]. Большинство ученых настаивает на преобладании данной свободы. Между тем, сегодня все чаще речь идет о трансформации информационного общества, о начале информационной эры. Полагают, что мир именно сейчас захватывают информационные войны и теперь нужно начинать защищать право каждого на информацию, право на доступ к Интернету как гарантии естественных прав человека, актуальными становятся и вопросы цифровой безопасности. Несмотря на многочисленные исследования и легальное закрепление понятий, остается открытым вопрос как соотносятся эти понятия. Создается впечатление, что эта проблема возникла лишь в 20 веке и, в сущности, касается только современного поколения. Существует мнение, что в демократическом обществе, в отличие от авторитарного или тоталитарного, должна быть абсолютная свобода информации, однако, как показывает практика, именно эта свобода должна иметь четко установленные пределы для защиты прав каждого гражданина и национальной безопасности государства в целом.

Английский ученый П. Биркиншоу прямо говорит о необходимости тотального контроля над информацией со стороны государства, поскольку утрата этого контроля грозит потерей власти: «Общество станет излишне любопытным, проявятся тенденции к критиканству и деспотии. СМИ, которые берут на себя функции расследования, могут причинить большой ущерб членам общества, в котором существует неограниченная свобода информации» [7. P. 179–180]. Поиск ответа, какая же модель права на доступ к информации наиболее справедлива и оптимальна, продолжается.

Как утверждал А. И. Герцен: «Чтобы понять современное состояние мысли, важнейший путь – вспомнить, как человечество дошло до него…» [1. С. 23–24]. Речь как передача понятийной информации развивалась достаточно долго. Провести историческую границу: вот это еще не речь, а это уже речь – невозможно. Кроме того, речь нельзя рассматривать только с точки зрения восприятия или передачи информации, фактически, это фиксация фактов, их озвучивание, осмысление. При помощи речи, понятий мы думаем. Отсюда важность языка, передающего информацию. О силе воздействия информации на сознание, волю и чувства человека писал Аристотель в IV в. до н. э. На ранних стадиях развития человечества применялись исключительно вербальные технологии (слухи, угрозы и т. д.)

[5. С. 21–22]. С точки зрения современной доктрины информацию можно воспринимать как «обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств» (Н. Винер) [6. С. 18–19]. Отечественная наука при определении категории «информация» исходила из критерия новизны (Ю. А. Шрейдер). Однако значение имеет не только содержание, но и подача информации, отражающая ее несмысловую форму. Эмоционально заряженная информация может дать требуемый отклик, особенно, если она основывается на прямо указанных источниках. Важным критерием информации во все времена была ее достоверность. Именно этот критерий является основополагающим, гарантировать качество информации, равно как и обеспечить ее защиту – главные задачи современного государства. В эпоху развития цифровых технологий обеспечение защиты информации не ограничивается правовым регулированием. Информатизация пронизывает все уровни жизни общества, международные отношения и вопросы обороны государства не являются исключением, в связи с чем цифровая безопасность информации выходит на передний план.

Стоит отметить, что любой конфликт между людьми в первую очередь является информационным. Категория «информационная война» была впервые использована китайскими учеными в 1985 году. При этом концепция информационной войны создавалась на базе «Трактата о военном искусстве» известного древнекитайского военного деятеля Сунь-цзы, жившего в V в. до н. э. и доказавшего эффективность информационного воздействия, отмечая: «Покорить соперника без боя – вот венец искусства» [4. С. 94]. Использование информации как самостоятельного вида оружия было известно с древних времен: слухи, дезинформация, демонизация (дегуманизация) противника (граф Дракула, Иван Грозный и т. д.), цензура, демонстрация (боевые кличи и т. д.), нарушение тайны исповеди (Орден Иезуитов), пропаганда (Третий рейх) и т. п. Эти методы, проверенные временем, широко представлены и сегодня.

Исторически первыми регулирование оборота информации и отнесение многих фактов к государственной тайне начали британцы, закон о государственной тайне в Великобритании издали в 1352 году. В России первые нормы об этом появились лишь в 1649 г. (в Соборном уложении пункты 2 и 20) и касались военной тайны, при этом речь шла лишь о правительстве, отдельных государственных органах и должностных лицах. Начиная с правления Петра I, ситуация изменилась и в России, на государственном уровне стали собирать абсолютно всю информацию, которая может навредить государственным интересам.

В ст. 29 Конституции РФ закреплено широкое толкование права на информацию и ее оборота в нашей стране. Данные положения, отражающие основные идеалы демократии современного мира, позволяют использовать в борьбе за экономическое и политическое влияние в международных отношениях скрытные и гибкие формы влияния, где ведущую роль играет контроль и управление информационными ресурсами государств. Сегодня информация и управление ею становится полноценным самостоятельным видом оружия, соответственно, утрата значимой информации может иметь фатальные последствия.

Информационно-психологическая война – наиболее популярная и самая опасная форма информационного воздействия. Она направлена на угнетение морального духа, содействует снижению сопротивления и экономии ресурсов нападающих. Целью воздействия является формирование такого чувства как страх, под воздействием которого противник принимает решение о бегстве или сдаче. Информацию используют для дезориентации, компрометации, дискредитации и т. д. Цифровые технологии передачи и публикации цифровой информации сегодня позволяют мгновенно распространить ложную информацию неопределенному кругу лиц. Единственный путь противостояния данному воздействию – образование и воспитание, базирующееся на религии, обычаях, традициях, историческом опыте и т. д. Однако стоит понимать, что сама по себе информационная война является лишь средством для достижения иных целей. Методы, которые используются при ведении информационной войны, разнообразны. Это и традиционные создание культа превосходства с помощью высмеивания, формирование образов неадекватности, варварства, а также смешение фактов, замалчивание, ложное объяснение, иллюзия поддержки большинства и т. д., и новый уровень воздействия с помощью дипфейков и иных технологий. Распространение условно достоверной или откровенно ложной информации возможно лишь там, где отсутствуют законодательно установленные пределы права на информацию и права на доступ к информации. Определить данные пределы, сохраняя права человека и обеспечивая одновременно его безопасность, это первостепенная задача каждого государства.

Таким образом, на современном этапе развития целесообразно раскрывать право на информацию и право на доступ к информации как самостоятельные понятия с уточнением, что человек имеет право на достоверную информацию, а право на доступ к достоверной информации должно гарантироваться государством. Достоверностью должна обладать не только информация, но и системы, платформы, ресурсы. Последние поправки в законодательство Российской Федерации, закрепившие ответственность за распространение ложной информации, частично обеспечивают достоверность информации на территории государства, однако только этих мер недостаточно. Право на достоверную информацию и на доступ к достоверной информации должны не просто декларироваться, а реально защищаться во всем мире и на международном уровне – уровне сети Интернет. К ответственности должны привлекаться международные должностные лица, распространяющие ложную информацию с целью достижения каких-либо политических целей. Игнорирование достоверной информации на международном уровне имеет такой же негативный эффект, как и использование ложной информации. События последних двух лет показали, что право на информацию должно быть не просто конкретизировано доктринально, оно должно иметь жесткие стандарты единые во всем мире и во всех сферах.

Список литературы

1. Герцен А. И. Письма об изучении природы / В кн. Избранные философские произведения. Т. 1. М.: Госполитиздат, 1948. 293 с.

2. Кириленко В. П., Алексеев Г. В. Право доступа к информации и медиабезопасность // Теоретическая и прикладная юриспруденция. 2019. № 1. С. 39–49.

3. Клюков В. Д. Право на информацию и право на доступ к информации: понятие и соотношение // Образование и право. 2019. № 8. С. 344–348.

4. Конрад Н. И. Сунь-цзы: Трактат о военном искусстве. М., 1950. 404 с.

5. Манойло А. В. Государственная информационная политика в особых условиях: Монография. М.: МИФИ, 2003. 388 с.

6. Чернавский Д. С. Синергетика и информация: динамическая теория информации. М.: Наука, 2001. 243 с.

7. Birkinshaw P. Freedom of Information: the Law, the Practice and the Ideal. Cambridge: Cambridge University Press, 2010.

8. Birkinshaw P. Freedom of Information and Openness: Fundamental Human Rights? // Administrative Law Review. 2006. Vol. 58 (1). P. 177–218.

О. И. Ларина,
кандидат экономических наук, доцент,
Государственный университет управления
Н. В. Морыженкова,
кандидат экономических наук,
Государственный университет управления

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В БАНКАХ И ПРАВО ПОТРЕБИТЕЛЯ НА ИНДИВИДУАЛЬНОЕ ОБСЛУЖИВАНИЕ

Аннотация. На сегодняшний день рынок искусственного интеллекта активно растет и развивается, предлагая новые возможности в сфере обслуживания банковских клиентов. Результаты опроса показали, что подавляющее большинство потребителей готовы к взаимодействию с технологиями искусственного интеллекта в банковской сфере, однако до сих пор предпочитают иметь возможность взаимодействия с сотрудником-человеком. Внедрение технологий искусственного интеллекта в банковской сфере снова поднимает вопросы безопасности и конфиденциальности данных клиентов, а также вызывает дискуссию о правосубъектности «электронного лица».

Ключевые слова: искусственный интеллект, клиентский сервис, права потребителя, некорректное цифровое проникновение, защита персональных данных, конфиденциальность данных, правосубъектность искусственного интеллекта

ARTIFICIAL INTELLIGENCE IN BANKS AND THE CONSUMER'S RIGHT TO INDIVIDUAL SERVICE

Abstract. Today, the artificial intelligence market is actively growing and developing, offering new opportunities in the field of servicing banking customers. The survey results showed that most consumers are ready to interact with artificial intelligence technologies in the banking sector, but still prefer to be able to interact

with a human employee. The introduction of artificial intelligence technologies in the banking sector again raises issues of security and confidentiality of customer data, and also raises a discussion about the legal personality of the “electronic person”.

Keywords: artificial intelligence, customer service, consumer rights, incorrect digital penetration, protection of personal data, data privacy, legal personality of artificial intelligence

Важным трендом последних лет является технологическое развитие внутренней и внешней бизнес-среды на основе цифровых технологий. Из наиболее актуальных и перспективных технологий следует выделить искусственный интеллект (ИИ), который представляет собой комплекс технологических решений, позволяющий имитировать когнитивные функции человека. Российский рынок искусственного интеллекта растет, и на данный момент существует около 600 компаний, которые развиваются, используя технологию ИИ в своей деятельности. Уже сейчас ИИ выполняет разные задачи. С появлением этой технологии многие специалисты начали говорить о том, что ряд профессий «умирает», потому что всю работу, которую выполнял специалист, теперь можно поручить искусственному интеллекту. Так ли это на самом деле?

В настоящее время очень популярны указанные технологии в области решения маркетинговых задач (как финансовых организаций, так и нефинансовых): создание рекламных текстов, текстов с характеристиками продуктов, рисунков по запросам; работа специализированных маркетинговых платформ, основанных на работе ИИ, которые предоставляют различные услуги – автономные медиапокупки и формирует непрерывное общение с клиентом (направляет сообщения через электронную почту, формирует целевые SMS-рассылки, настраивает социальные сети (комьюнити), анализирует поисковой трафик и демонстрирует таргетированную рекламу). Кроме того, ИИ также будет анализировать текущие рекламные кампании и выявлять перспективные направления их оптимизации; автоматизация работы контакт-центра (внедрение робота для разговоров по часто задаваемым вопросам); анализ трендов отрасли для создания наиболее востребованных продуктов (например, анализ текстов научных статей, патентных заявок, отраслевых публикаций) и др.

Банки уже освоили первые возможности применения ИИ и продолжают искать новые способы использования этой технологии в различных бизнес-направлениях. Так, например, А. Ведяхин (первый заместитель председателя правления ПАО «Сбербанк»), отметил, что в Сбере на данный момент успешно функционируют системы ИИ на уровне принятия многих важных решений: построение оптимального маршрута для инкассации; составление ответов чат-бота и колл-центра; вычисление необходимого количества сотрудников в отделениях банка; оптимизацией предложений для конкретных клиентов и т. п. Банк применяет технологии ИИ в процессе корпоративного и потребительского кредитования (на данный момент подобных сделок порядка 80 %). Финансовый эффект в 2022 г. от внедрения ИИ оценивается в 230 млрд руб., т. е. на каждый вложенный рубль технология уже принесла около 6,7 руб. прибыли [5].

В связи с тем, что рынок искусственного интеллекта также растет и развивается, появляется большое количество новых продуктов и технологий, которые могут создавать другие новые возможности для обслуживания банковских клиентов, сфера применения искусственного интеллекта будет расширяться и далее, облегчая трудоемкие и рутинные задачи персонала. Компании и банки без внедрения искусственного интеллекта в бизнес-процессы могут утратить в дальнейшем свою конкурентоспособность. Вместе с тем с целью выявления текущих проблем и перспектив применения ИИ в банковских продуктах авторами был проведен опрос респондентов (100 человек), результаты которого следующие: аудитория в основном нейтрально (58 %) и положительно (38 %) относится к внедрению технологий ИИ в сферу финансов (отрицательно – 4 % опрошенных); однако общению с роботом аудитория предпочитает общение со специалистом (68 %); сборку своего инвестиционного портфеля доверили бы искусственному интеллекту, решение которого будет обработано оператором-человеком, 73 % респондентов, специалисту-человеку при этом доверяет 19 % респондентов, а ИИ всего – 8 %.

Таким образом, результаты опроса показали, потребители готовы к взаимодействию с системами ИИ. Вместе с тем, пока присутствует недоверие к решениям и продуктам, предлагаемым на основе ИИ. Клиенты считают, что необходимо наличие естественного интеллекта, способного анализировать решения искусственного, т. е. определенный баланс между персональным обслуживанием и автоматизацией. В связи с этим важным моментом при внедрении в гражданский оборот продуктов с применением технологий ИИ встает вопрос о правах граждан на выбор обслуживания. На наш взгляд, потребитель должен иметь выбор о взаимодействии с сотрудником – человеком или роботом при решении его индивидуальных проблем.

Рост популярности нейронных сетей (компьютерная технология, применяемая для работы ИИ) вызвал множество дискуссий в научном сообществе. Так, в статье С. М. Авдошина и Е. Ю. Песоцкой анализируются проблемы цифровой защиты, которые появляются в связи с широким внедрением нейронных сетей в современном обществе [1]. Авторы отмечают, что использование цифровых технологий дает преимущества и увеличивает возможности как бизнеса, так и общественных и социальных институтов. Вместе с тем появляются и риски, и серьезные угрозы, связанные с использованием ИИ в части работы с персональными данными пользователей (некорректное цифровое проникновение).

Другой автор, Ю. Б. Бочаров рассматривает как преимущества жизни в «умном» доме, городе, так и проблемы, вызываемые возможной ненадежностью сохранности базы данных потребителей, проживающих в «умных» городах [4]. Возникает дилемма, что главнее и нужнее обществу для бесперебойной и четкой работы на благо всех членов данного общества: права граждан, личная свобода, конфиденциальность личной жизни или возможность удовлетворения всех потребностей каждого индивидуума, еще до того, как они возникли?

В статье С. Ф. Афанасьева рассматривается вопрос о современной правовой политике в области возможного придания правосубъектности такому цифровому явлению, как искусственный интеллект [2]. С точки зрения автора, если ИИ

сможет в ближайшем будущем воспроизводить почти все основные познавательные человеческие компоненты и компетенции, то это не означает, что он будет автоматически наделен правосубъектностью, включающей в себя правоспособность и дееспособность. Этот же вопрос поднимает О. С. Болотаева [3].

Идет полемика о возможности наделения юнитов искусственного интеллекта правосубъектностью «электронного лица» с тем, чтобы обеспечить в первую очередь возможность несения ими юридической ответственности за правонарушения, совершенные в процессе функционирования технологии. Ряд ученых придерживаются мнения, что искусственный интеллект допустимо рассматривать исключительно как инструмент, используемый человеком для решения каких-либо задач. Однако некоторые исследователи уверены, что юниты искусственного интеллекта, обладающие значительной степенью автономии и способные принимать решения, имеющие в том числе правовые последствия, должны быть наделены правосубъектностью.

Таким образом, несмотря на перспективы, которые открывает технология искусственного интеллекта для улучшения качества обслуживания клиентов в банковской сфере, ее внедрение в банковские продукты может вызвать некоторые проблемы. Одной из основных задач является обеспечение безопасности и конфиденциальности данных клиентов. Вторая задача – обеспечить принятие клиентов. Важно на переходном этапе обеспечить клиентам возможность взаимодействия с сотрудником-человеком. Возможности обработки естественного языка и понимание данных клиентов означают, что ИИ может стать отличным решением для обеспечения более персонализированного, эффективного и удобного пользовательского опыта в банковских услугах.

Список литературы

1. Авдошин С. М., Песоцкая Е. Ю. Доверенный искусственный интеллект как способ цифровой защиты // Бизнес-информатика. 2022. Т. 16, № 1. С. 62–73.

2. Афанасьев С. Ф. К вопросу о правовой политике в сфере придания правосубъектности искусственному интеллекту // Правовая политика и правовая жизнь. 2022. № 2. С. 226–235.

3. Болотаева О. С. Правосубъектность искусственного интеллекта // Право и государство. 2022. № 4(208). С. 15–17.

4. Бочаров Ю. Б. Искусственный интеллект в управлении «умным» городом, где грань между благом и проблемой? // Мировая наука. 2022. № 8 (65). С. 21–27.

5. Заруцкая Н. Сбербанк рассказал о перспективах использования искусственного интеллекта в банках. URL: https://www.vedomosti.ru/finance/articles/2023/07/06/984101-sberbank-rasskazal-o-perspektivah-ispolzovaniya-iskusstvennogo-intellekta-v-bankah

О. С. Лиликова,
кандидат юридических наук, доцент,
Белгородский государственный национальный
исследовательский университет

ОСОБЕННОСТИ РАССМОТРЕНИЯ КОРПОРАТИВНЫХ СПОРОВ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБЩЕСТВА

Аннотация. Корпоративные споры являются главной составляющей развития бизнеса в России. Чем меньше споров возникает, тем больше иностранного капитала финансируется в экономику страны. В связи с последними событиями, Россия столкнулась с проблемой рассмотрения корпоративных споров, которое влечет за собой ухудшение качества продукции на рынке, уменьшение количества товара, рост цен. Правительство РФ смогло предотвратить коллапс экономической сферы и остановку развития рынка; а с уходом иностранных компаний, дать рывок для отечественного бизнеса и привлечение других стран к инвестициям и расширение партнерства корпораций уже на другом рынке. Но, к сожалению, проблема корпоративных споров никуда не ушла, и для решения данной проблемы в первую очередь нужно создать эффективную систему законодательства, а также судебную систему, которая будет эффективно решать данные корпоративные споры, что неизбежно приведет к тенденции снижения этих споров.

Ключевые слова: корпоративные споры, корпорации, бизнес, конфликты, стороны, арбитражный суд

FEATURES OF CONSIDERATION OF CORPORATE DISPUTES IN THE CONTEXT OF DIGITAL TRANSFORMATION OF SOCIETY

Abstract. Corporate disputes are the main component of business development in Russia. The less disputes arise, the more foreign capital is financed into the country's economy. In connection with recent events, Russia is faced with the problem of resolving corporate disputes, which entails a deterioration in the quality of products on the market, a decrease in the quantity of goods, and an increase in prices. The government of the Russian Federation was able to prevent the collapse of the economic sphere and stop the development of the market; and with the departure of foreign companies, give a boost to domestic business and attract other countries to invest and expand partnerships between corporations already in another market. But, unfortunately, the problem of corporate disputes has not gone anywhere, and in order to solve this problem, first of all, it is necessary to create an effective system of legislation, as well as a judicial system that will effectively resolve these corporate disputes. Which will inevitably lead to a downward trend in corporate disputes.

Keywords: corporate disputes, corporations, business, conflicts, parties, arbitration court

Корпоративные споры являются неотъемлемой частью корпоративного права (его еще называют антимонопольное право), которое за последние годы

претерпело множество изменений. В России развитие корпораций началось относительно недавно, большинство аспектов данного права было взято из опыта стран Запада. На данный момент Российская Федерация уделяет особое внимание данной отрасли права и смогла создать уникальную систему корпоративного права, которая испытывает изменения со сложившейся ситуацией в стране, такие как пандемия и санкции, которые включают в себя объемные ограничительные меры.

Сам, по себе термин корпоративные споры, уже говорит о многом, это прежде всего споры, возникающие между коммерческими и некоммерческими организациями, предпринимателями согласно статье 225.1 Арбитражного процессуального кодекса Российской Федерации (далее – АПК) [1]. Обычно, данные споры возникают в связи с реорганизацией деятельности компании, а также вопросы, связанные с управлением и ведением финансово-хозяйственных разногласий. Корпоративные споры – это прежде всего отношения, которые связаны с процессом создания, развития, ликвидации деятельности корпорации, которые связаны с участием в управлении членов, а также органов, которые были созданы в рамках этой самой корпорации. Сам по себе термин корпорации является обширным и имеет множество трактовок. Так, например, данный термин И. В. Тиболт объясняет так: понятие «корпорация» может существовать в трех аспектах:

– организационно-правовая форма;

– отраслевая принадлежность;

– организационно экономическая форма [7, с. 16]

Корпоративные споры являются главной составляющей развития бизнеса в России. Бизнес, в первую очередь – это конкуренция и борьба между корпорациями на рынке, без нее невозможно представить рост экономики самого государства.

Сегодня все больше и больше компаний занимаются международным бизнесом, заключая контракты и договора с иностранными партнерами. Однако, несмотря на все усилия для предотвращения возможных споров в процессе работы, они иногда все же возникают. И в этой ситуации часто возникает вопрос: каким образом можно эффективно разрешить коммерческий спор с участием иностранных элементов?

Проблемы разрешения коммерческих споров с участием иностранных элементов становятся актуальной темой для многих компаний, которые имеют дело с международными контрактами. При этом, такие проблемы могут быть вызваны различными факторами: от непонимания культурных особенностей до несовпадения правовых систем стран-участников.

Разрешение коммерческих споров с участием иностранных элементов – это одна из наиболее сложных задач в юридической практике Российской Федерации. Наличие иностранных элементов в споре приводит к тому, что его разрешение требует большего внимания со стороны юристов, а также учитываются особенности правовых норм Российской Федерации и международного права. Кроме того, разрешение таких споров часто связано с определенными рисками и вызывает особую осторожность.

В рамках Организации Объединенных Наций была принята Модельная законодательная база о международном коммерческом арбитраже. Этот документ

разработан с целью унификации правовых норм в области международного коммерческого арбитража и его признания, и приведения в исполнение. Основной принцип при разрешении коммерческих споров с участием иностранных элементов – это принцип свободного договора сторон. Стороны вправе самостоятельно определить компетентный суд и применимое право к разрешению спора. В случае, если в договоре не установлены соответствующие установки, решение о компетентном суде и применимом праве принимается на основании норм международного права и российского права.

При разрешении коммерческих споров в России может быть применен международный закон только в случае, если это предусмотрено договором или на основании норм международного права. Кроме того, важно учитывать особенности законодательства той страны, в которой был заключен договор. Если законодательство данной страны предусматривает наличие каких-либо особенностей, отличных от законодательства РФ, то нужно учитывать их при разрешении спора.

Рассмотрев порядок рассмотрения корпоративных споров, можно понять, насколько законодательство готово к решению проблемы. Прежде всего данные споры делят на объективные и субъективные, объективные споры возникают в связи с отсутствием каких-либо жестких действий за нарушения корпоративных обязательств, не совершенствование самого законодательства в целом. Субъективные споры имеют более узкую направленность, например, обход уплаты налогов, при оформлении компании на своих близких, что ведет в будущем к конфликту и борьбе за власть, устранение руководителя компании, если его доля в компании не менее 10 %, это неизбежно приведет к разбирательству в суде и данных примеров можно привести еще множество.

Немаловажно сказать о субъектах и объектах корпоративных споров. Субъектами выступают участники корпоративных споров, а объектами – права участников спора. Затрагиваются интересы многих участников, что создает специфику судебного разбирательства. В основном дела, связанные с корпоративными спорами, рассматриваются арбитражными судами, особенностью дела является углубление суда с учетом принципа диспозитивности и свободы предпринимательских отношений. Например, в договоре поставки, четко не указано, как именно должен перевозится товар, в следствии чего товар приедет поврежденным – суд не может вторгаться в определение условия договора, так как это независимая сфера участников договора и определяется только их волей. Большинство субъектов спора сталкиваясь с данной ситуацией, не находят другого решения вопроса, как обратиться в суд, считая, что данный орган поможет им выйти из так называемого «тупика». Общие собрания участников корпорации являются достаточно формализованными, т. е. изначально проходит подготовка действий и процедурные нормы, которые регулируют проведение собрания. Чаще всего такие действия игнорируются и собрания проводятся в неформальной обстановке, главным доказательством проведения собрания служит – протокол, подписанный всеми участниками данного собрания, такие собрания, не нарушают законодательство. Проследив развитие данных дел, мы увидим, что если ранее суды, отклоняли

в решение данного вопроса, то на сегодняшний день суд более подробно изучает участников сторон.

Одной из наиболее распространенных проблем при разрешении коммерческих споров с участием иностранных элементов в России является понимание особенностей международного права сторонами спора. Различные правовые системы могут иметь принципиальные отличия в понимании таких понятий, как договор, вина, невыполнение обязательств и т. п. В связи с этим может возникнуть непонимание сторонами, который может привести к возникновению новых конфликтов или отказу от решения судьи. В юридической практике это называется «конфликтом квалификаций». Российское законодательство нашло следующий выход: согласно статье 1187 Гражданского Кодекса Российской Федерации «при определении права, подлежащего применению, толкование юридических понятий осуществляется в соответствии с российским правом, если иное не предусмотрено законом. Если при определении права, подлежащего применению, юридические понятия, требующие квалификации, не известны российскому праву или известны в ином словесном обозначении либо с другим содержанием и не могут быть определены посредством толкования в соответствии с российским правом, то при их квалификации может применяться иностранное право» [2].

Еще одной распространенной проблемой является несоответствие правил проведения дела в соответствии с международными стандартами. Например, некоторые страны могут предъявлять требования к документации, которая не соответствует международным нормам, что может затруднить получение необходимой информации для анализа дела. Также при разрешении таких споров может возникать проблема с выбором компетентного суда. Каждая сторона может настаивать на разрешении спора в своей стране или территориальном суде, которым она управляет. В таких случаях важно учитывать мнение каждой из сторон и довести до консенсуса о выборе наиболее подходящего суда. Считаем, что правильным подходом будет являться указание в соглашении сторон о международной подсудности конкретного государства, в суд которого следует обратиться при возникновении коммерческого спора. Статья 1210 Гражданского Кодекса Российской Федерации также определяет, что «стороны договора могут при заключении договора или в последующем выбрать по соглашению между собой право, которое подлежит применению к их правам и обязанностям по этому договору».

Разрешение коммерческих споров с участием иностранных элементов является сложной задачей, требующей особого подхода и компетенции в области международного права. Компании, занимающиеся международным бизнесом, сталкиваются с проблемами, связанными с различными юрисдикциями и правовыми системами, а также со сложностью доказательств и перевода документов.

При разрешении коммерческих споров с участием иностранных элементов в юридической практике Российской Федерации используются различные способы урегулирования споров. Одним из таких способов является арбитражный суд, в котором спор рассматривается независимым судьей или коллегией международных экспертов. В Постановлении Пленума Верховного Суда РФ № 23 «О рассмотрении арбитражными судами дел по экономическим спорам, возникающим

из отношений, осложненных иностранным элементом» [3], отражено, что «участники международных экономических отношений и иных отношений, связанных с осуществлением экономической деятельности, вправе заключить пророгационное соглашение о рассмотрении споров в арбитражном суде Российской Федерации (договорная компетенция). Пророгационным соглашением является соглашение сторон о передаче в арбитражный суд Российской Федерации всех или определенных споров, которые возникли или могут возникнуть между ними в связи с каким-либо конкретным правоотношением, независимо от того, носило такое правоотношение договорный характер или нет. В таком случае арбитражный суд Российской Федерации будет обладать исключительной компетенцией по рассмотрению данного спора при условии, что такое соглашение не изменяет исключительную компетенцию иностранного суда (ст. 249 АПК РФ).

Примером коммерческого спора с участием иностранных элементов может служить дело «Asia Auto Parts» против компании «Volvo». В этом случае компания «Asia Auto Parts» настаивала на том, что компания «Volvo» не выполнила свои обязательства в рамках договора о поставке запчастей для автомобилей. Стороны спора не смогли достичь соглашения, и дело было передано в арбитражный суд. В результате суд признал правоту компании «Asia Auto Parts» и обязал компанию «Volvo» выплатить компенсацию за несоблюдение условий договора.

Одним из путей решения коммерческих споров является альтернативное разрешение споров (АРС). АРС – это методы разрешения споров, которые не включают в себя судебный процесс. Они могут быть использованы как для национальных, так и для международных дел.

Основными методами альтернативного разрешения споров (далее – АРС) являются: медиация, арбитраж (третейское разбирательство), переговоры, экспертиза. При медиации спорные стороны пытаются достичь соглашения с помощью посредника. Международный институт по развитию бизнеса и права (МИРБИС) разработал Модельное руководство по медиации в международном коммерческом обороте. Это руководство содержит рекомендации по использованию механизма медиации для разрешения коммерческих споров с участием иностранных элементов.

Е. А. Борисова отмечает, что «переговоры являются базовым видом АРС, выступая основой для остальных способов урегулирования конфликта» [4. С. 26]. В. В. Котлярова выделяет, что переговоры «представляют собой примирительную процедуру, в которой принимается совместное решение и урегулируется конфликт сторонами непосредственно или при содействии своих доверенных лиц без привлечения независимой третьей стороны» [5. С. 19].

Экспертиза – процесс, при котором эксперт оценивает доказательства и дает заключение в отношении спорного вопроса. В юридической практике РФ также широко используется консультативный совет, при котором междуспорные конфликты разрешаются на основе рекомендаций юристов.

АРС предоставляет сторонам возможность сохранить бизнес-отношения и избежать длительных судебных разбирательств. Однако не все случаи могут быть решены через АРС. Например, если одна из сторон нарушает закон или

отказывается выполнять обязательства по контракту, то может потребоваться обращение в суд. Для успешного разрешения коммерческих споров также необходимо правильно подготовиться к судебному процессу. Важно иметь все необходимые доказательства, как письменные, так и устные, а также своевременно представить их в суде. При этом следует учитывать особенности юридической системы страны, где рассматривается дело.

Наконец, для эффективного разрешения коммерческих споров необходимо иметь четкий план действий на случай возникновения конфликта. Компания должна иметь политику по управлению рисками и стратегию по разрешению споров, чтобы минимизировать потери в случае конфликта.

Еще один суд, который вправе рассматривать дела по корпоративным спорам является третейский. Важным отличием третейского суда, от арбитражного является быстрота рассмотрения дела. В третейском суде отсутствует инстанций кассации и апелляции, благодаря этому и обусловлена скорость рассмотрения спора, что делает его более оптимальным для решения конфликта среди участников. Положительной стороной суда, является его закрытость, т. е. утечка какой-либо информации о конфликте между участниками невозможна, также это относится и к результатам рассмотрения дела. Несмотря на все достоинства, третейские суды не так популярный, что делает их уровень нагрузки низким, он значительно отличается от государственных, что также влияет на скорость рассмотрения дела и на фокусировании на одном конкретном деле, небольшое количество дел позволяет более качественно рассматривать спор. Третейский и арбитражный суд схожи между собой, так по мнению И. В. Черниковой: понятия «арбитраж» и «третейское разбирательство» теперь используются как синонимы, что делает схожими до степени смешения термины «решение арбитражного суда» и «арбитражное решение», «арбитражный суд» и «арбитраж», относящиеся, при этом, к совершенно разным областям: области государственного судопроизводства и альтернативного разрешения споров соответственно [9. С. 30]. Главным минусом третейского разбирательства в том, что арбитражные суды наделены полномочиями осуществления дополнительного контроля над данным видом судопроизводства, что перечеркивает его независимость в отношение решения спора, при этом не входя в государственную систему судебного производства.

Все это, конечно же, затягивает решение корпоративного спора, происходит накапливание данных конфликтов и тормозит развитие корпораций. Сковывание судов в рамках одной государственной системы, затрудняет расширение корпораций и заставляет юридическое лицо ликвидировать его, не найдя поддержку в суде.

Затруднение решением споров является, отсутствием четкой нормы к какому виду спора его отнести, существует мнение по определению круга корпоративных споров, так, например, А. В. Терентьев пишет: законодателю необходимо исчерпывающе определить круг корпоративных споров либо установить четкие правила их определения. Поскольку первая задача представляется трудновыполнимой, полагаем правильным сосредоточить усилия на второй, а именно определить отношения, из которых могут возникать корпоративные споры, установить

круг лиц, которые вправе обратиться в суд с требованием о возбуждении дела по корпоративному спору, и круг лиц, которые будут выступать в качестве ответчиков. Для этого нужно внести соответствующие изменения не только в процессуальное, но и в материальное законодательство, в том числе в Гражданский кодекс РФ [8. С. 70].

Рассматриваемые споры можно разделить на категории, к первой чаще всего относится распределение и расходование прибыли внутри корпорации, ко второй – конфликты, которые связаны с правами на собственность и третьи – это споры, связанные с игнорированием интересов руководителей. На данный момент, законодатель, не смог установить правило их определения, связанное с затруднением данного процесса, но данные изменения лишь вопрос времени.

Развитие законодательства, это неизбежный процесс, для достижения целей, а прежде всего увеличение эффективности деятельности местных корпораций. Такой опыт нам в первую очередь нужно перенимать у наших близких друзей, а именно Китайская Народная Республика. Китай смог свести уровень корпоративных споров до минимума, привлекая иностранный капитал, что в будущем дало толчок для развития местных корпораций, что вывело китайскую продукцию на мировой уровень имея 18 % мирового валового внутреннего продукта, что делает ее второй экономикой мира. Данный результат был возможен лишь с развитием законодательной базы в стране. Все эти изменения происходили постепенно, внедряя новые нормы или наоборот, исключая уже устоявшиеся. Как пример, в нашем законодательстве, а именно в корпоративном праве, был легализован параллельный импорт, который долгое время находился под запретом, данные изменения помогли избежать дефицита товара и недобросовестную конкуренцию.

Избежать корпоративный спор достаточно тяжело, но возможно, прежде всего суд прибегает к обеспечительным мерам. В вопросах решения корпоративных споров чаще всего используются:

– арест на акции, доли в уставном капитале и другие активы;

– наложение запрета на совершение сделок с акциями, долями в уставном с другими активами;

– запрет на принятие решений в отношении предмета спора; запрет на исполнение решений юридического лица;

– запрет на совершение записей по учету акций, переходу прав на ценные бумаги, их размещение и обращение.

Составление искового заявления по делам о корпоративных спорах можно считать уникальными с правовой точки зрения, а именно выделением исков по материально-правовому признаку. Так, Д. Д. Короткова и многие ученые отмечают, что: «деление исков на виды по их материально-правовой природе имеет важное значение: именно материально-правовой природой иска определяются его подведомственность, направленность судебного процесса, субъективный состав участников процесса и те процессуальные особенности, которые характерны для отдельных категорий дел…» [5. С. 234].

В настоящее время Верховный Суд РФ является высшим судебным органом в разрешении экономических споров. Действия Президента по ликвидации

Высшего Арбитражного Суда РФ изначально вызвало критику среди многих судей, якобы нарушается принцип равенства судей, судебная система которая строилась годами будет нарушена, а также нарушается Конституция. Проследив рассмотрение дел судебной коллегии по экономическим спорам, можно заметить, что помощь в разрешение конфликтов между участниками, возросла. С правовой точки зрения, спустя столь долгое время можно сделать выводы, что данные изменения имеют как положительные, так и отрицательные результаты. Появилась проблема определения подведомственности спора, отнесение его к экономической или предпринимательской деятельности, что, в свою очередь, затрудняет само по себе решение спора и приводит к его затягиванию. Указ Президента по ликвидации Высшего Арбитражного Суда РФ привел к единству подходов рассмотрения споров между физическими и юридическими лицами, установила общие правила организации судопроизводства, но на эффективность рассмотрения дел никак не повлияло.

Таким образом, проблемы разрешения коммерческих споров с участием иностранных элементов требуют внимательного и комплексного подхода. Необходимы прозрачность и справедливость при принятии решений, а также учет международных стандартов и правовых норм для достижения эффективного разрешения споров, которые удовлетворят все заинтересованные стороны. Разрешение коммерческих споров с участием иностранных элементов в России – это сложная и ответственная задача, требующая особого внимания со стороны юристов. Практика разрешения коммерческих споров с участием иностранных элементов в России показывает, что проблемы могут быть решены при помощи арбитражных судов, медиации, арбитража, переговоров и консультативных советов, а также при условии учета мнения каждой из сторон.

Особенность и порядок рассмотрения корпоративных споров, в нашем законодательстве несовершенно и требует развития. В последние годы Россия столкнулась с множеством трудностей и намерением недружественных стран затормозить развитие страны, несмотря на это коллапса экономической сферы достичь не удалось, а наоборот создало почву для экономического развития. Российская Федерация, меняя вектор, перенимает опыт у новых дружественных государств, справляясь с проблемой корпоративных споров все более эффективно, что с течением времени неизбежно выведет страну на уровень развитых стран. Изменения в законодательстве приведут к уменьшению конфликтов среди участников корпораций, следовательно, подъем корпораций будет неизбежен.

Список литературы

1. Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 № 95-ФЗ. URL: https://www.consultant.ru

2. Гражданский кодекс Российской Федерации (часть третья) от 01.11.2001 № 156-ФЗ. URL: https://www.consultant.ru

3. О рассмотрении арбитражными судами дел по экономическим спорам, возникающим из отношений, осложненных иностранным элементом: Постановление Пленума Верховного Суда РФ от 27.06.2017 № 23. URL: https://www.consultant.ru

4. Борисова Е. А. Альтернативное разрешение споров: учебник. М.: Городец, 2019. 417 с.

5. Короткова Д. Д. Корпоративные споры. Определение и особенности // Молодой ученый. 2022. № 24 (419). С. 234–235.

6. Котлярова В. В. Альтернативные способы урегулирования и разрешения споров в России: учебное пособие. Самара: Издательство Самарского университета, 2021. 104 с.

7. Тиболт И. В К вопросу о корпорации // Инженерный вестник Дона. 2014. Т. 28, № 1. С. 16–19.

8. Терентьев А. В. Корпоративные споры в современном российском законодательстве // Российский юридический журнал. 2019. № 3. С. 70–73.

9. Черникова И. В. Понятия «арбитраж», «третейский суд» и «арбитражный суд» в российском законодательстве и вопросы, возникающие при их использовании // Российский судья. 2020. № 4. С. 29–33.

Ю. Ю. Малышева,
кандидат юридических наук, доцент,
Казанский институт (филиал)
Всероссийского государственного
университета юстиции

ВРАЧЕБНЫЕ ОШИБКИ И «ВИНА» ПАЦИЕНТА ПОД ПРИЗМОЙ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Аннотация. Проблема видится в том, что не всегда пациент предоставляет врачу полную, честную и достоверную информацию о состоянии своего здоровья. Поэтому границы «вины» врача существенно сужаются под призмой «вины» пациента. Цифровые технологии безусловно являются неотъемлемой частью гражданского общества XXI века, и поэтому в век цифровых технологий, врачебные ошибки могут быть сведены к минимуму. Актуальность проблемы врачебной ошибки очевидна, поскольку с ней сталкивается каждый «первый» доктор. На данном этапе использование цифровых технологий, в частности, электронной медицинской карты пациента, стало мощным подспорьем в руках медицинских работников, поскольку собирание точного анамнеза пациента с отражением в цифровой медицинской карте больного стало набирать обороты не только в популярных столичных клиниках, но и во всех регионах России.

Ключевые слова: цифровизация здравоохранения в уголовном праве, цифровые технологии в уголовном праве, уголовно-правовая охрана медицинских работников в уголовном праве, «вина» пациента в уголовном праве

MEDICAL ERRORS AND «FAULT» OF THE PATIENT UNDER THE LIGHT OF DIGITAL TECHNOLOGIES

Abstract. The problem is seen by the author in that the patient does not always provide the doctor with complete, honest and reliable information about the state of his health. Therefore, the boundaries of the «guilt» of the doctor are significantly narrowed under the prism of the «guilt» of the patient. Digital technologies are certainly an integral part of the civil society of the 21st century, and therefore, in the digital age, medical errors can be minimized. The urgency of the problem of medical error is obvious, since every «first» doctor faces it. At this stage, the use of digital technologies, in particular, the patient's electronic medical record, has become a powerful help in the hands of medical workers, since collecting an accurate patient history with reflection in the patient's digital medical record has begun to gain momentum not only in popular metropolitan clinics, but also in all regions Russia.

Keywords: digitalization of healthcare in criminal law, digital technologies in criminal law, criminal law protection of medical workers in criminal law, «Guilt» of the patient in criminal law

Цифровые технологии дарят огромные возможности сфере здравоохранения – и медицинским работникам, и пациентам, позволяя, к примеру, отслеживать течение болезни и эффективность лечения, прием лекарственных препаратов, хронические заболевания и многое другое с помощью цифровой карты пациента. Избежать врачебных (медицинских) ошибок в медицинской деятельности даже в век цифровизации здравоохранения, к сожалению, не представляется возможным.

Можно констатировать, что в уголовном праве и медицине научный подход к категории «врачебной ошибки» находится на «одной волне», где исходными понятиями выступают «добросовестность», «заблуждение» и «погрешность» в медицинской деятельности. Бесспорным является то, что ошибается каждый человек. Другое дело, если человек ошибается не по своей вине, а из-за неточно предоставленной информации другим человеком. Сегодня, в XXI век цифровых технологий, врачебные ошибки безусловно не могут не существовать совсем, но могут быть сведены к минимуму [4. С. 131].

Ошибка врача, способная причинить вред жизни и здоровью больного выступает сложнейшей проблемой в профессиональной практике медицинских организаций всего мира [5. С. 26]. В современный век цифровизации применение цифровой медицинской карты пациента набирает обороты во всем цивилизованном мире. Поэтому собирание полного и точного анамнеза пациента с последующим отражением процесса лечения в цифровой медицинской карте больного становится огромным подспорьем в руках медицинских работников.

Как мы уже неоднократно подчеркивали в своих научных работах, полностью разделяя позицию Л. М. Рошаля, уход от врачебных ошибок равен уходу из профессии врача. К примеру, в начале 2023 г. в США опубликована статья о том, что ученые пришли к мнению, что ковид лечили неправильно, о некорректности

терапии и гипотетическом выводе о том, что это могло увеличить смертность от ковида. Безусловно, было множество ошибок в лечении ковида, поскольку даже сегодня, по прошествии пандемии COVID-19, до сих пор стандарта лечения данного заболевания в мире нет. Для этого должны пройти годы наблюдений и взвешенных исследований, отраженных в цифровых медицинских картах больных. Во времена пандемии COVID-19 пациенты часто занимались самолечением от крепкого алкоголя до преднизолона на дому. Мы не знакомы с американским протоколом лечения ковида, но в российский протокол лечения COVID-19 антибиотики вводили не сразу и довольно долго. Также в России в отличие от Америки умерших от ковида вскрывали всех и сразу, а не спустя года, как это делали в США.

Достоверным и доказанным фактом в медицине является тот факт, что любая, даже мелкая ошибка медицинского работника, уже не гарантирует верного диагноза и полного излечения пациента [10. С. 324]. Или, к примеру, обоснованный риск в деятельности неотложного хирурга (кардиохирурга) является неотъемлемой частью профессии данных специалистов [6. С. 112].

Напрямую с исследованиями применения сложностей ситуаций с врачебными ошибками в уголовном праве стоит проблема применения ч. 2. ст. 28 УК РФ. Уголовно-правовая дилемма, как отмечает А. И. Рарог, проявляется в том, что врач не имеет реальной возможности предотвратить последствия своей ошибки [9. С. 87].

Профессор С. В. Шевелева по данному вопросу отмечает, что условно ситуацию, предусмотренную ч. 2 ст. 28 УК РФ, можно именовать «субъективной непреодолимой силой, поскольку ее источник лежит в извинительной неспособности действующего сделать надлежащий выбор варианта поведения», что также подтверждает нашу позицию [2. С. 148].

Зачастую вина пациента имеет ключевое значение в признании (непризнании) врачебной ошибки как таковой [7. С. 200]. В цифровых медицинских картах пациентов отражены следующие сведения.

К примеру, пациентка средних лет, недавно перенесшая маммопластику, жалуется на нестабильный имплант в левой груди, когда карман, где стоит имплантат, разбалтывается и протез мигрирует в подмышечную впадину, либо переворачивается плоской стороной, меняя тотально эстетический вид, который и был целью проведенной операции. В правой груди все хорошо. Доктор задает несколько вопросов, касающихся повседневной жизни пациентки, в том числе, соблюдает ли она все послеоперационные рекомендации. Пациентка заверяет доктора, что все, указанное в выписке, женщина выполняет. Но в непринужденной беседе, доктор выясняет, что на даче ремонт, а муж попал в больницу, и женщина сама таскала мешки с цементов на второй этаж. Именно так врач выяснил причину разбалтывания кармана после проведенной маммопластики, поскольку такие физические нагрузки и с подъемом тяжестей противопоказаны.

Безусловно, таких историй много у врача любой специальности, и при производстве экспертизы, позицией клиники в споре нередко выступает предположение, а соблюдал ли пациент рекомендации лечащего врача, поскольку осложнения могли быть связаны с неверно проведенным реабилитационным периодом

[1. С. 54]. В данном случае для клиники, если особенности пациента не были зафиксированы в цифровых медицинских картах пациентов, последующими врачами или другими объективными данными, следствием и судом это воспринимается несерьезно, только в качестве предположения [8. С. 143].

Еще один пример, когда мама, обратившаяся со своим сыном по поводу кровохаркания к детскому хирургу, отрицала, что в семье есть больные туберкулезом, что было зафиксировано в цифровой медицинской карте пациента, хотя ее муж, отец ее семнадцатилетнего сына, проходил на тот момент лечение от туберкулеза. Врач сделал ребенку рентген, и увидел каверну в верхней доле справа, и конечно отправил пациента в тубдиспансер. Тот факт, что отец ребенка проходил лечение от туберкулеза, врач узнал от пульмонологов, которых поставил в известность, и уже они выяснили детали, необходимые для лечения.

Следующий пример, стоматолог несколько раз переделывал пломбу пациенту на переднем зубе, пока не узнала, что пациент рыбак и на рыбалке перекусывает больным зубом леску.

Примером от терапевта выступает классический вариант, когда пациент, мучаясь от гипертонии, жалуется на неэффективность таблеток, назначенных доктором, тем не менее, игнорируя рекомендации врача, при этом злоупотребляя алкоголем, умалчивая о последнем, даже при постановке целенаправленных вопросов.

Представляется, что для самих пациентов подобное, даже неосознанное, сокрытие информации от врача может обернуться трагедией, когда от этого зависит жизнь и здоровье пациента. К примеру, осложнение на введение антиковид-вакцины, оказавшееся в реалии отравлением этиленгликолием.

По нашему мнению, является бесспорным, что врачебная (медицинская) ошибка ни в коей мере не говорит о вине медицинского работника, представляя собой лишь некую погрешность в деятельности медицинского работника, которая могла случиться и по «вине» пациента, не полностью предоставившего или не предоставившего вовсе сведений о своем здоровье (самочувствии).

К сожалению, в России, в частности Татарстане, и даже в век цифровых технологий, наблюдается большой отток медицинских работников. К примеру, в Республике Татарстан в 2022 г. уволилось 5,4 тысячи врачей, при этом на работу вновь приняли 4,9 тысячи. Таким образом, отток медицинских кадров составил 567 человек, о чем заявила директор территориального фонда обязательного медицинского страхования (ФОМС) Татарстана А. Мифтахова. Сегодня в 2023 г. наблюдается нехватка врачей – специалистов, когда число уволившихся оказалось выше количества принятых. Согласно данным директора ФОМС Татарстана в 2022 г. из медицинских организаций уволилось 3,9 тысяч специалистов среднего звена, когда вновь принято только 3,5 тысячи. Данный факт безусловно подтверждает всю сложность профессии врача и негласный «запрет» на врачебные ошибки.

Другим примером оптимизации медицины и как следствие врачебных ошибок является рабочий поселок Вохтога Волгоградской области с населением в 5,5 тысяч человек. При этом по состоянию на июнь 2023 г. в Вохтоге имеется всего три кареты скорой помощи при пяти действующих фельдшерах, а работающих врачей

в поселке нет. В июне 2023 г. женщина 70 лет потеряла сознание на улице, прохожие вызвали скорую помощь, но на вызов приехала машина скорой медицинской помощи в составе одного водителя и через 13 минут с момента вызова пациентка была доставлена в стационар, но уже на момент поступления женщины в стационар реанимационные мероприятия были неэффективны, и была констатирована смерть с причиной – сердечно-сосудистого заболевания.

Причин неукомплектованности медицинских кадров – великое множество – от низкой заработной платы медицинских работников до сложных условий труда при отсутствии машин скорой помощи, необходимого оборудования, лекарств и уважения к профессии врача.

Выводом по нашему исследованию является то, что подробный сбор анамнеза и его полное отражение в цифровой карте пациента, если таковая имеется, – 60 % успеха лечения пациента, и в то же время и защита самого доктора, учитывая то, что пациент сообщил о себе и своем состоянии здоровья честную и полную информацию, с четкими выполнениями всех предписаний врача [3. С. 540]. В противном случае привлечение врача к уголовной ответственности неминуемо, поскольку врачебные (медицинские) ошибки в настоящее время не смогут освободить медицинского работника от уголовной ответственности, к примеру, в случае применения ст. 124 УК РФ.

Уверены, что от взаимоотношений пациента и системы здравоохранения, в частности, врача, зависит жизнь и здоровье пациента, а также благополучие самого медицинского работника.

Список литературы

1. Воронин В. Н. Уголовная ответственность за незаконную выдачу рецептов или иных документов, дающих право на получение наркотических средств или психотропных веществ // Законодательство. 2023. № 1. С. 52–56.

2. Воронин В. Н. Медицинская деятельность и невиновное причинение вреда: уголовно-правовые аспекты // Юридический вестник Дагестанского государственного университета. 2021. Т. 39, № 3. С. 144–150.

3. Галюкова М. И. Медицинская деятельность как основа формирования уголовно-правовых отношений в сфере безопасности здоровья пациента // Уголовное право: стратегия развития в XXI веке: Материалы XV Международной научно-практической конференции, Москва, 25–26 января 2018 года. Москва: РГ-Пресс, 2018. С. 538–541.

4. Малышева Ю. Ю. К вопросу о врачебных ошибках в условиях пандемии COVID-19 в контексте уголовного закона // Вестник Волжского университета им. В. Н. Татищева. 2021. Т. 1, № 3 (99). С. 131–139.

5. Малышева Ю. Ю. Ятрогенные преступления в момент пандемии Covid-19 // Гуманитарные и политико-правовые исследования. 2021. № 3(14). С. 25–40.

6. Малышева Ю. Ю., Малышев К. В. О некоторых вопросах репродуктивных прав человека, донорства и ятрогений с позиций уголовного закона // Право и биоэтика инновационных медицинских технологий: монография. Проспект, 2021. С. 109–132.

7. Малышева Ю. Ю. Языковые средства для обозначения категории «обмана» в уголовном праве // Уголовное право: стратегия развития в XXI веке: Материалы XV Международной научно-практической конференции, Москва, 25–26 января 2018 г. Москва: РГ-Пресс, 2018. С. 199-202.

8. Малышева Ю. Ю. Уголовно-правовые и криминологические аспекты служебного подлога в медицинской деятельности // Вестник Волжского университета им. В. Н. Татищева. 2023. Т. 1, № 2 (104). С. 142–149.

9. Рарог А. И. Вина в советском уголовном праве: для научных работников, преподавателей, аспирантов и студентов юридических факультетов. М.: Проспект, 2018. 192 с.

10. Рарог А. И., Понятовская Т. Г. Медицинский риск в уголовном праве // Всероссийский криминологический журнал. 2021. Т. 15, № 3. С. 321–331.

Д. А. Мальцева,
кандидат политических наук, доцент,
Санкт-Петербургский государственный университет
О. Д. Сафонова,
кандидат политических наук, доцент,
Санкт-Петербургский государственный университет
Д. А. Федотов,
студент,
Санкт-Петербургский государственный университет

ЦИФРОВОЙ СУВЕРЕНИТЕТ ГОСУДАРСТВА В НОВОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ: ПОЛИТИКО-ПРАВОВОЙ АСПЕКТ

Аннотация. В представленном исследовании затрагиваются актуальные вопросы, связанные с концептуализацией цифрового суверенитета, анализом специфики современного цифрового пространства в целях обеспечения национальной безопасности в условиях развития информационного общества и эскалации глобального конфликта. В качестве основных проблем обозначаются отсутствие единого понятийного аппарата в контексте изучения современных форм суверенитета, необходимость социального измерения и согласования его актуальных моделей, а также трансформации существующего законодательства в этой области.

Ключевые слова: цифровой суверенитет, человеческий капитал, информационные технологии, национальная безопасность, цифровое право

Финансирование: Исследование выполнено при финансовой поддержке ЭИСИ в рамках научного проекта «Динамика трансформации цифрового публичного управления в современной России: политические стратегии и риски в условиях эскалации глобального конфликта», который реализуется в ИНИОН РАН

DIGITAL SOVEREIGNTY OF THE STATE IN THE NEW INFORMATION SPACE: POLITICAL AND LEGAL ASPECT

Abstract. The presented study addresses current issues related to the conceptualization of digital sovereignty, analysis of the specifics of the modern digital space in order to ensure national security in the context of the development of the information society and the escalation of the global conflict. The main problems identified are the lack of a unified conceptual apparatus in the context of studying modern forms of sovereignty, the need for a social dimension and coordination of its current models, as well as the transformation of existing legislation in this area.

Keywords: digital sovereignty, human capital, modern technologies, national security, digital law

В последние годы проблема цифрового суверенитета является предметом активной научной дискуссии [4], которая особенно актуализируется в дискурсе распространения интернет-технологии нового поколения формата Web 3.0.

Правовое регулирование отношений в сети интернет-формата Web 2.0, характерной особенностью которых являлось создание контента пользователями, подразумевает перцепцию информации в Web преимущественно самим индивидом. Сегодня же Web 2.0 сменяется форматом Web 3.0, который обеспечивает обработку данных в Web в первую очередь посредством компьютерных систем. Web 3.0 строится на базе технологии блокчейна, что позволяет преодолеть недостатки централизованной сети и создать принципиально новый подход к организации интеракций. Существует множество справедливых аргументов в отношении формата web 2.0, в которых отмечаются его существенные недостатки, создающие опасность для правового поля [3]. Публикуемый пользователями контент в большинстве случаев принадлежит не автору, а владельцу сервера, что приводит к частым спорам между авторами и владельцами цифровых платформ. В ряде случаев владелец в праве распоряжаться содержимым контента, т. е. имеет возможность его удалить, заблокировать или ограничить доступ.

Разумеется, правовые споры также возникают вокруг безопасности и конфиденциальности данных. Большие объемы пользовательских персональных данных хранятся на сторонних серверах, которые могут находится вне юрисдикции государства, в котором эти данные были созданы, соответственно, они уязвимы к кибератакам, кражам и злоупотреблениям [1]. При этом к рискам добавляется отсутствие единой системы цифровой идентификации, что вынуждает пользователей оставлять свои персональные данные на каждом веб-ресурсе, где предусмотрена регистрация.

Стоит также отметить, что формат Web 2.0 препятствует развитию искусственного интеллекта, поскольку большая часть данных в сети не структурирована и не оптимизирована для обработки методами машинного обучения. В свою очередь, ключевой особенностью Web 3.0 является оцифровка активов посредством их токенизации [5], что выступает основой криптоиндустрии, которая на

сегодняшний день в известной степени недосягаема для государства, что представляет собой феномен «невидимой угрозы».

Таким образом, можно утверждать, что стратегическое и тактическое, структурное и системное управление сферой информационной безопасности на государственном уровне выступает не только глобальной политической и военной потребностью, но и гарантией локальной защиты личности от множества разнокачественных угроз, механизмом обеспечения прав и свобод, а также общего национального суверенитета. В свете современных технологий необходимо расширить интерпретацию понятия суверенитета как категории политической науки и международного права. Понятие государственного суверенитета, включающее в себя военные, дипломатические, экономические, политические и идеологические аспекты, уже недостаточно для академического исследования и требует анализа своих цифровых измерений.

В доктрине информационного права до сих пор фокус внимания концентрируется на вопросах трансграничного информационного взаимодействия и проблемах применения юрисдикций различных государств в информационной сфере. Сам механизм реализации, защиты и обеспечения государственного суверенитета в информационном пространстве остается без должного внимания, что доказывает потребность и своевременность разработки нового концептуального подхода к анализу сущности и содержания понятия цифрового государственного суверенитета и моделям его информационно-правового обеспечения при осуществлении стратегического государственного управления и нормативного правового регулирования в сфере информационных отношений в период функционирования формата web 2.0 при активном становлении web 3.0, что является новым вызовом для правовой и политической систем.

Для успешного разрешения вышеупомянутой проблемы в первую очередь необходима систематизация терминологии. Требуется определение и утверждение понятия «цифровой суверенитет». Следующим шагом станет подготовка актуального законодательства, регулирующего данный вопрос на уровне государства.

Подводя итог, можно выделить несколько стратегических направлений обеспечения и защиты суверенитета с учетом его новых аспектов:

1. Улучшение материально-технической инфраструктуры, создание национальной операционной системы и программного обеспечения. Развитие информационных технологий в глобальном масштабе приводит к возникновению новых подходов и стратегических подходов к информационной борьбе, которые можно принимать в виде сетевого, кибер-, гибридного и информационного конфликта.

2. Подготовка высококвалифицированных специалистов, включая представителей инженерно-технической отрасли, а также экспертов в области юриспруденции, информационной безопасности и профессионалов в правоохранительной сфере.

3. Подтверждение «цифрового суверенитета» в рамках международного контура. Данное направление требует инициирования дискуссий по указанной проблематике на международном уровне, с привлечением ученых и экспертов. Задача

данной деятельности приоритетна для государства, так как реализуется в интересах стратегических и тактических целей Российской Федерации.

4. Регулирование информационно-цифровых отношений через проведение государственной информационной политики и осуществление информационных функций.

5. Защита традиционных ценностей. Одним из условий цифрового государственного суверенитета являются традиционные ценности в информационном пространстве. Их охрана и защита, в свою очередь, – это залог информационной безопасности Российской Федерации [2].

Список литературы

1. Азизов Р. Ф., Архипов В. В. Отношения в сети Интернет формата WEB 2.0: проблема соответствия между сетевой архитектурой и правым регулированием // Закон. 2014. № 1. С. 90–104.

2. Кропачев Н. М., Архипов В. В. Традиционные духовно-нравственные ценности в контексте цифровой трансформации общества: теоретико-правовые аспекты // Вестник Санкт-Петербургского университета. Право. 2023. Т. 14, № 2. С. 294–306.

3. Чернов А. В., Дворянова М. В. Скринлайф: авторская рефлексия в контексте проблематики медиакоммуникации эпохи Web 2.0 // Вестник Костромского государственного университета. 2020. Т. 26, № 4. С. 187–193.

4. Роблес-Каррильо, М. Суверенитет и цифровой суверенитет // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 673–690. EDN: NFWLYF.

5. Захаров Н. А. Web 3.0: новые возможности и новые вызовы //Автоматизация в промышленности. 2023. № 1. С. 60–64.

О. В. Медяник,
кандидат психологических наук, доцент,
Санкт-Петербургский государственный университет
Н. И. Легостаева,
кандидат социологических наук,
Санкт-Петербургский государственный университет
С. И. Медяник,
аспирант,
Санкт-Петербургский государственный университет

СТРАТЕГИИ ФИНАНСОВОГО ПОВЕДЕНИЯ РОССИЯН В УСЛОВИЯХ РОСТА КИБЕРРИСКОВ

Аннотация. В настоящее время растет число преступлений, связанных с цифровым мошенничеством в экономическом секторе, и увеличивается уровень финансовой тревожности потребителей цифровых товаров и услуг. В мае 2023

года авторы данного исследования провели онлайн-опрос по РФ с выборкой 1018 респондентов. В результате были выявлены доминирующие стратегии финансового поведения россиян: рациональная, доверительная, недоверчивая, интуитивная и тревожная. Полученные результаты исследования будут полезны для дальнейшей работы в области описания риск-профилей, а также разработки профилактических мер и образовательных программ с целью обеспечения информационной безопасности.

Ключевые слова: киберриски, кибермошенники, финансовое поведение, психотипы, цифровые товары и услуги, информационная безопасность, киберграмотность, цифровизация

Финансирование: исследование выполнено за счет гранта Российского научного фонда, № 23-28-00701, https://rscf.ru/project/23-28-00701

STRATEGIES OF FINANCIAL BEHAVIOR OF RUSSIANS IN THE CONTEXT OF GROWING CYBER RISKS

Abstract. Digital fraud crimes in the economic sector are on the rise and the financial anxiety of consumers of digital goods and services is increasing. In May 2023, the authors of this study conducted an online survey on the Russian Federation with a sample of 1018 respondents. As a result, the dominant strategies of financial behavior of Russians were identified: rational, trusting, distrusting, intuitive and anxious. The obtained results of the study will be useful for further work in the field of describing risk profiles, as well as developing preventive measures and educational programs to ensure information security.

Keywords: cyber risks, cyber fraudsters, financial behavior, psychotypes, digital goods and services, information security, cyber literacy, digitalization

Введение. Высокая скорость интеграции цифровых технологий в повседневную жизнь привела к появлению и развитию новых научных направлений – цифровой рискологии, цифровой коммуникации и социальной инженерии. Последствия цифровой коммуникации с активным развитием социальных сетей, голосовых помощников, чат-ботов, дистанционных форм работы и досуга (виртуальные галереи, стримы концертов и др.) привели к появлению новых структур (акторов) коммуникации – фейковых аккаунтов, троллей, ботов, ботнетов, а также новых процессов в коммуникативной сфере – ложная идентификация, астротурфинг, кибербуллинг и др. Интенсификация цифровой экосистемы экономического сектора привела к появлению новых экономических субъектов – цифровых потребителей и воздействующих на них кибермошенников.

Основная часть. В процессе разработки типологии психотипов потребителей цифровых товаров и услуг и стратегий их финансового поведения небходимо учитывать как их субъективные качества (например, опыт цифрового финансового поведения, уровень киберграмотности), так и объективные факторы (например, качество обслуживания). Ряд исследователей сосредоточились на изучении

мобильной виктимизации как одной из форм киберагрессии. В результате были разработаны типологии жертв, исходя из следующих переменных: технологический прогресс, частота использования мобильного телефона, уровень привязанности к мобильному телефону [4]. Milanova и Schreiber разработали типологию финансовой уязвимости на основе четырех факторов, влияющих на принятие решений о страховании потребителей: финансовая грамотность, вовлеченность, информационное поведение и ответственность [5]. В своем исследовании они проиллюстрировали, как личные характеристики влияют на величину рисков уязвимости, которым подвергаются потребители. Saridakis с помощью опроса активных пользователей [6] изучал взаимосвязь моделей поведения в социальных сетях, личных характеристик, технической эффективности и риска столкновения с угрозой виктимизации в Интернете.

Авторы данного исследования, изучая цифровую трансформацию экономического сектора, выявили 11 факторов, влияющих на финансовое поведение россиян: финансовая тревожность, финансовое беспокойство, финансовый оптимизм, восприятие страховых рисков, успешное использования FinTech, рациональное финансовое поведение, ответственное финансовое поведение, инвестиционное поведение, деструктивные финансовые установки, управление личными финансами в цифровых приложениях, отношение к расходованию денежных средств. Был сделали вывод, что финансовые установки, цифровые навыки, предпочтения и привычки российских потребителей формируются в период их активной цифровой социализации и во многом зависят от уровня образования, наличия цифровой и финансовой грамотности. В результате анализа признаков каждого из одиннадцати факторов были сформированы четыре психотипа финансового потребителя: доверчивый, недоверчивый, тревожный, рациональный [1; 2].

Исследование стратегий финансового поведения российских потребителей. В мае 2023 г. был проведен онлайн-опрос, в котором приняли участие 1 018 россиян, из них 58,5 % женщин и 41,5 % мужчин. В возрасте от 26-35 лет – 33,4 % опрошенных, от 36-45 – 31,5 %, от 18-25 – 18,2 %, 46-65 – 16 %. Чуть менее половины участников опроса отметили, что у них высшее образование (диплом специалиста, бакалавра, магистра и т. п.) – 47,1 %, 22,3 % – среднее специальное образование (колледж, техникум и т. п.), 77,3 % участников исследования отметили, что у них нет экономического образования. В результате факторного анализа были выявлены следующие стратегии финансового поведения россиян: рациональное поведение, доверительное поведение, недоверчивое поведение, интуитивное поведение и тревожное поведение.

Рациональное поведение включает позиции, связанные с внимательностью потребителя к языку тела продавца, внешнему виду, жаргону для выявления возможных манипуляций и ловушек. Люди со стратегией рационального финансового поведения с большей вероятностью будут осторожны и смогут избежать рискованных ситуаций. Доверительное поведение в проведенном исследовании коррелировало с привлекательной внешностью субъекта воздействия. Потребители с доверительной стратегией финансового поведения склонны доверять людям, особенно если они выглядят привлекательными, и они более подвержены обману со стороны

мошенников, которые используют свою привлекательность. Стратегия недоверия связана со склонностью финансового потребителя к поиску подтверждения и проверке информации. Люди, у которых отмечается данная стратегия финансового поведения, реже доверяют другим без достаточных для них доказательств. Стратегия интуитивного финансового поведения связана с влиянием внешнего вида продавца и первого впечатления на решение покупателя приобрести товар или услугу. Потребители-интуиты в большей степени зависят от первого впечатления, чем от объективных факторов. Стратегия тревожного финансового поведения связана с ожиданием факта мошенничества и недоверием к незнакомым людям. Потребители с данной линией финансового поведения склонны к тревоге и страху, что может привести к избеганию новых знакомств и финансового опыта.

Большинство респондентов согласны с утверждениями, связанными с рациональной стратегией финансового поведения (вес фактора 6,6):

1) «обращает внимание на язык тела продавца, чтобы распознать возможные манипуляции и ловушки»;

2) «обращает внимание на внешность мошенника, чтобы распознать возможные манипуляции и ловушки»;

3) «склонен к критическому мышлению и анализу, чтобы выявить потенциальные ловушки и обман»;

4) «уверен в своих способностях анализировать ситуацию и распознавать за маской мошенника»;

5) «склонен анализировать жаргон мошенников, чтобы почувствовать возможный обман».

Многие респонденты согласны с утверждениями, связанными со стратегией доверчивого финансового поведения (вес фактора 5,9): 1) «Я могу отдать деньги привлекательному мошеннику»; 2) «Скорее всего, если мошенник обаятельный, он может легко обмануть меня»; 3) «Я склонен доверять людям, особенно если они выглядят привлекательно»; 4) «Мне трудно распознать манипуляции мошенников (жаргон, язык тела), потому что я склонен смотреть на них слишком лояльно»; 5) «Я не всегда умею анализировать ситуацию, если за маской скрывается мошенник».

На третьей позиции стоят потребители, которые выразили согласие с утверждениями, коррелирующими со стратегией недоверчивого финансового поведения (вес фактора 4,99): 1) «Я склонен искать подтверждения и проверять информацию перед тем, как довериться кому-то, даже если он выглядит привлекательно»; 2) «Я часто проверяю информацию и факты, чтобы быть уверенным в ее правдивости». Это указывает на то, что подавляющее число людей предпочитает быть осторожными и проверять информацию, прежде чем довериться кому-то.

На четвертой позиции отмечены потребители с интуитивной стратегией финансового поведения (вес фактора 4,66), для которых первое впечатлением о продавце или магазине имеет высокое значение: 1) «Внешний вид продавца может повлиять на первое впечатление покупателя о магазине»; 2) «Первое впечатление о продавце может повлиять на решение покупателя о приобретении товара»; 3) «Эффективность рекламы может быть снижена, если первое впечатление

о магазине или продавце негативное»; 4) «Даже если качество товара высокое, негативное первое впечатление о продавце может привести к отказу от покупки»; 5) «Покупатели могут быть более склонны к сотрудничеству с продавцами, которые создают положительное первое впечатление».

Пятую позицию занимают потребители с тревожной стратегией финансового поведения (вес фактора 3,9):

1. «Ожидает обмана и не доверяет незнакомым людям»;

2. «Предпочитает избегать новых ситуаций и людей, чтобы не сталкиваться с возможным обманом».

Заключение. В результате проведенного исследования авторы описали 5 стратегий финансового поведения российских потребителей товаров и услуг: рациональная, доверчивая, недоверчивая, интуитивная и тревожная. Среди описанных стратегий лидирующие позиции занимают рациональная и доверчивая стратегии, что ведет к выводу о доминировании рационально-доверчивого психотипа финансового потребителя. В соответствии с «Основными направлениями развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов» [3] полученные результаты могут использоваться при разработке информационно-просветительского контента по информированию граждан о мошеннических схемах, а также при разработке программ по повышению финансовой киберграмотности и пропаганде кибергигиены для различных категорий населения, в том числе для лиц с низким уровнем дохода и социально незащищенных категорий населения.

Список литературы

1. Медяник О. В., Легостаева Н. И. Трансформация финансового поведения россиян в условиях цифровизации рынка финансовых услуг // Вестник Пермского национального исследовательского политехнического университета. Социально-экономические науки. 2022. № 4. С. 22–37.

2. Медяник О. В., Легостаева Н. И. Финансовое поведение россиян: факторы, типы, коды уязвимости // Телескоп. 2022. № 4. С. 50–55.

3. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов. URL: https://www.cbr.ru/Content/Document/File/148351/onrib_2025.pdf

4. Lusinga S., Kyobe M. Testing a Typology of Mobile Phone Victimisation Using Cluster Analysis // The Electronic Journal of Information Systems in Developing Countries. 2017. Vol. 78. Pp. 154-200.

5. Milanova V., Schreiber F. One size does not fit all: A typology of financial consumer vulnerability, 2017 Winter AMA Conference, Orlando, FL, USA, 2017.

6. Saridakis G., Benson V., Ezingeard J.-N., Tennakoon H. Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users // Technological Forecasting and Social Change. 2016. Vol. 102. Pp. 16–32.

С. Р. Решетняк,
старший преподаватель,
Российская академия народного хозяйства
и государственной службы при Президенте Российской Федерации,
Северо-Кавказский институт – филиал
Е. С. Минеева,
студент,
Российская академия народного хозяйства
и государственной службы при Президенте Российской Федерации,
Северо-Кавказский институт – филиал

АВТОРСКОЕ ПРАВО НА ПРОИЗВЕДЕНИЯ, СОЗДАННЫЕ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

Аннотация. В статье дается анализ существующего сегодня международно-правового регулирования вопроса авторского права на произведения, созданные искусственным интеллектом. Делается акцент на современных подходах к пониманию результатов работы искусственного интеллекта, которые влияют на особенности правового регулирования результатов его деятельности, и соотношения с авторскими правами лиц, так или иначе связанных с процессом создания произведения искусственным интеллектом. Осуществляется оценка развития института авторского права с учетом появления искусственного интеллекта, и появления произведений, созданных им. Предлагается правовая регламентация на законодательном уровне рассматриваемых вопросов в России.

Ключевые слова: авторское право, объект авторского права, авторские произведения, искусственный интеллект, цифровизация, гражданское законодательство, IT-технологии

COPYRIGHT FOR WORKS CREATED BY ARTIFICIAL INTELLIGENCE

Abstract. The article analyzes the existing international legal regulation of the issue of copyright for works created by artificial intelligence. At the same time, emphasis is placed on modern approaches to understanding the results of the work of artificial intelligence, which affect the peculiarities of the legal regulation of the results of its activities, and the relationship with the copyrights of persons in one way or another connected with the process of creating a work of artificial intelligence. The article also evaluates the development of the copyright institute, taking into account the emergence of artificial intelligence, and the appearance of works created by it. And proposals are being made on legal regulation at the legislative level of the issues under consideration in Russia.

Keywords: copyright, object of copyright, copyrighted works, artificial intelligence, digitalization, civil legislation, IT technologies

Введение. В современном мире все большее значение приобретают IT-технологии. Беспилотные автомобили, бесконтактная оплата товаров и услуг, онлайн банкинг, искусственный интеллект, уже не представляются как плод воображения писателей-фантастов. Они уже существуют, и со временем будут становиться лишь технологически совершеннее и все более автономными от человеческого контроля.

Наиболее сложным из перечисленных объектов является искусственный интеллект. Поскольку, что пока еще рано говорить о его полноценной самодостаточности, вследствие чего он скорее генерирует результат своей деятельности, например, условное творческое произведение за счет обработки и компиляции заложенных в него шаблонов, каждый из которых имеет привязку к авторству конкретного лица.

Однако появление искусственного интеллекта уже сейчас в существенной мере оказывает влияние на сферы искусства и науки. «Созданные» искусственным интеллектом произведения нисколько не уступают по качеству авторским работам, а по степени их востребованности у покупателей и популярности в цифровой среде, зачастую могут их превосходить. Что создает неопределенность в вопросе правовой оценки результатов функционирования искусственного интеллекта, и требует устранения соответствующего пробела при регулировании авторских прав.

Основная часть. В научном сообществе существуют радикально противоположные подходу к пониманию существования авторских прав в отношении объектов, созданных искусственным интеллектом.

Среди них можно выделить следующие подходы к пониманию отношения к результатам «творчества» искусственного интеллекта:

– это авторские произведения, поскольку искусственный интеллект является субъектом авторского права;

– искусственный интеллект и человек являются соавторами произведения;

– искусственный интеллект имеет черты технического средства для получения человеком авторского продукта$

– искусственный интеллект не является субъектом авторского права, права на произведение закрепляются исключительно за человеком, который его использовал;

– авторское право на произведение закрепляется за разработчиком (владельцем) искусственного интеллекта.

При этом данные подходы актуальны не только для российской правовой системы, но и для многих других стран мира, поскольку мировое сообщество также заинтересовано в урегулировании поднятого вопроса. Поэтому данный вопрос становится актуальным предметом исследования на уровне национального законодательства в Европе, Азии и Америке.

Так, в 2023 г. Бюро авторского права США (United States Copyright Office) выступило с предложением об обсуждении закона, который регулировал сферу авторского права на произведения, созданные искусственным интеллектом, а также материалов, защищенных авторским правом, использованных в процессе обучения искусственного интеллекта.

Также 16 марта 2023 г. была запущена инициатива, в соответствии с которой будет проведен мониторинг текущего законодательства США относительно авторского права и его связи с искусственным интеллектом. В этой связи был выпущено новое «Руководство по регистрации авторских прав: Произведения, содержащие материалы, созданные искусственным интеллектом» [6].

Новшеством для авторского права США стала обязанность раскрывать информацию о включении материалов, созданных искусственным интеллектом при подаче произведения на регистрацию [7].

Однако ряд стран категорически отказываются от признания существования авторских прав у искусственного интеллекта, или тех произведений, которые создаются с его использованием.

Так в Федеративной Республике Германия в «Законе об авторском праве и смежных правах», в части 1, разделе 3 указано, что создателем произведения является его автор, иными словами автором возможно признать исключительно человека [5].

Но существует и несколько альтернативная позиция, согласно которой авторство на произведение, созданное искусственным интеллектом, следует закрепить за создателем программного обеспечения, при помощи которого объект авторского права был создан. Подобной позиции придерживаются Великобритания, Индия, Ирландия. В частности, в ходе судебного разбирательства по делу «Nova Productions Ltd v Mazooma Games Ltd» было принято решение, в соответствии с которым авторское право на элементы игры, созданные с использованием искусственного интеллекта, принадлежит его разработчику [8].

Схожий подход на настоящий момент времени используется не только в Британии, но и в Европейском Союзе. Так, Европарламент оперирует тем, что авторским правом априори может обладать лишь человек [4]. Искусственный интеллект по своей сути является машиной и не может иметь черты субъекта правоотношений, связанных с авторством.

Однако при этом Европарламент не исключает, что данный подход может со временем измениться. О чем говорится в соответствующей резолюции от 16 февраля 2017 года [3].

В Российской Федерации отсутствуют правовые нормы, способные полностью урегулировать вопросы авторского права на произведения, созданные искусственным интеллектом. Так, в соответствии с пунктом 1 статьи 1228 Гражданского кодекса Российской Федерации, автором может быть признан только гражданин[1].

В соответствии с текущим законодательством Российской Федерации искусственный интеллект является инструментом для создания объектов авторского права.

Однако наиболее рациональным является исходить из оценки вложенных в создание произведения физических и интеллектуальных ресурсов человека. В качестве перспективы развития отечественного права можно выделить возможность создания критериев для оценки творческого вклада при создании произведения, что позволит разрешить обозначенные нами вопросы.

Заключение. Данные отношения не имеют полноценной законодательной регламентации, несмотря на принятие в 2019 г. Национальной стратегии развития

искусственного интеллекта на период до 2030 г. [2], определяющей как развитие искусственного интеллекта, так создание правового регулирования отношений, возникающих в связи с его применением. Однако практических шагов законодателем пока не предпринято, что говорит о необходимости как продолжения доктринального изучения вопроса, так и создания полноценной правовой основы статуса искусственного интеллекта, в том числе и с последующей корректировкой гражданского законодательства в вопросе лиц и объектов гражданского права.

Резюмируя описание критерия авторского произведения, необходимого для его защиты, можно отметить, что на настоящий момент времени, произведение может быть объектом правовой защиты лишь в том случае, если он было создано автором и является результатом его творческой деятельности.

Таким образом, в контексте рассмотренного вопроса можно сделать вывод о том, что в действительности существует разносторонний подход к урегулированию вопроса. Однако в то же время необходим единый международный подход к решению вопроса об авторском праве искусственного интеллекта, ибо данная проблема влечет трудности полноценного введения результатов искусственного интеллекта в оборот, а потому требует скорейшего решения.

Список литературы

1. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // Собрание законодательства Российской Федерации. 2006. № 52 (ч. I). Ст. 5496.

2. Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства Российской Федерации. 2019. № 41. Ст. 5700.

3. Texts adopted – Civil Law Rules on Robotics – Thursday. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html

4. Решетникова А. Творец или инструмент в руках автора? URL: https://zakon.ru/blog/2019/12/02/tvorec_ili_instrument_v_rukah_avtora

5. Gesetz über Urheberrecht und verwandte Schutzrechte Gesetz vom 09.09.1965 (BGBl. I S. 1273) zuletzt geändert durch Gesetz vom 23.06.2021 (BGBl. I S. 1858) m.W.v. 01.12.2021. URL: https://dejure.org/gesetze/UrhG

6. Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence. URL: https://clck.ru/36ozFy

7. Copyright Office Launches New Artificial Intelligence Initiative. URL: https://www.copyright.gov/newsnet/2023/1004.html

8. Nova Productions Ltd v Mazooma Games Ltd – Case Law – VLEX 793307357. URL: https://vlex.co.uk/vid/nova-productions-ltd-v-793307357

Р. И. Миннуллин,
преподаватель,
Всероссийский государственный университет юстиции
(РПА Минюста России),
Казанский институт (филиал)

УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ ЯТРОГЕННЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ВЫСОКОТЕХНОЛОГИЧНОГО ОБОРУДОВАНИЯ

Аннотация. В статье анализируются основные уголовно-правовые аспекты института ятрогенных преступлений, совершенных с использованием высокотехнологичного оборудования. Приводится определение понятия «ятрогенные преступления» с уголовно-правовой и криминалистической точки зрения. Рассматриваются отдельные примеры ятрогенных преступлений, совершенных с помощью высокотехнологичного оборудования в свете современного уголовного права России. Обосновывается необходимость предупреждения подобных правонарушений, совершаемых с использованием высокотехнологичного оборудования.

Ключевые слова: ятрогенные преступления, медицинское оборудование, медицинские технологии, медицинский работник, врач, пациент

CRIMINAL LEGAL ANALYSIS OF IATROGENIC CRIMES COMMITTED WITH USING HIGH-TECH EQUIPMENT

Abstract. The author of the article analyzes the main criminal legal aspects of the institution of iatrogenic crimes committed by using high-tech equipment. In particular, the author of the article provides a definition of the concept of “iatrogenic crimes” from a criminal legal and forensic point of view. In the article, the author examines certain examples of iatrogenic crimes committed with the using of high-tech equipment in the light of modern Russian criminal law. Also in the article, the author substantiates a necessity to prevent such offenses committed with using high-tech equipment

Keywords: iatrogenic crimes, medical equipment, medical technologies, medical worker, doctor, patient

Специальные знания в расследовании ятрогенных преступлений является неоценимыми. В течение последних четырех лет XXI в. появились различные тенденции в развитии заболеваний, несущих в себе большую опасность для жизни человека, и в то же время появились и развиваются медицинские технологии, фармацевтическое производство, разрабатывающие медицинские препараты для лечения вирусных заболеваний, с которыми ранее человечество не сталкивалось. Развитие высокотехнологичного медицинского оборудования, с помощью которого медицинские работники проводят обследования и лечение больных граждан, говорит о развитии доверия со стороны медицинских специалистов к указанным оборудованиям. Как правило, действия хирурга в отделениях микрохирургии,

производятся с использованием оборудования и ошибка хирурга либо сбой оборудования, в процессе операции может сыграть не самую лучшую роль для пациента, а может даже и роковую.

Как мы знаем, понятие ятрогения – это причинение вреда здоровью путем лечения, либо его назначения, другими словами, действие или бездействие врача, равноценно отрицательно отражающееся на состоянии человека. А как же рассмотреть тот факт, что причинение вреда было осуществлено резким сбоем высокотехнологического оборудования при осуществлении операции. Как необходимо расценивать данный факт? Ведь о данных последствиях и об ответственности мало кто задумывается.

Определить четкое состояние человека до и после оказания или не оказания врачебной помощи непросто, в данном случае зависеть будет от сроков обращения данного человека, который обратился за врачебной помощью. А если обращение было дистанционным, по телефону фиксируется ли данный факт каким-либо способом? Ведь и некоторые психологические воздействия, и доверчивое отношение к использованию медицинских технологий, внедренных с целью проведения четкого и быстрого лечения, воспринимаются человеком по-разному, все эти факты так же влияют на способы лечения и на состояние человека.

Ведь очевидно, для этого необходимо определить состав ятрогенных преступлений, куда входит несколько преступных посягательств на здоровье и на жизнь человека. В некоторых случаях ятрогению указывают как заболевание, которое является неблагоприятным последствием, допущенным нарушением со стороны медика в системе отношений «врач-пациент», как правило, допущение нарушения врачом установленных предписаний при оказании медицинской помощи, и в том и другом случае преступные посягательства вызваны:

– ненадлежащим исполнением медиком своих профессиональных обязательств при оказании помощи больному, (пациенту), (ч.2 ст. 109, ч.2 ст. 118, ч. 4 ст. 122 УК РФ) [3];

– неправомерными действиями (бездействием) медика по оказанию медицинской помощи (ч.3 ст. 123, ст. 124, 235 УК РФ) [3].

Все же при лечении с использованием высокотехнологического оборудования, с допущением ряда нарушений, к примеру: ввиду сбоя, либо резкого недомогания хирурга, вызванных неправильными действиями, может повлечь смерть или причинить вред больному. И в этой ситуации никто не может быть застрахован. Не своевременное действие хирурга или даже кратковременное бездействие хирурга может привести к вышеназванным последствиям.

В части неправомерных действий, (бездействий), и определения момента обращения к сотруднику медицинской организации, а именно скорой помощи можно представить следующий пример: у ребенка шести лет резко повысилась температура до 40 градусов, мать ребенка оказала первичную помощь, дав дочери лекарственные средства для снижения температуры. Через 45 минут температура снизилась буквально на 15-20 минут. Через указанное время температура у ребенка вновь поднялась до 41 градуса. После того, как мать ребенка не смогла справиться в домашних условиях, была вынуждена обратиться за помощью и набрала

номер 112 для экстренного вызова скорой помощи. По телефону она объяснила свои предпринятые действия и указала на то, что температура после приема лекарственных препаратов у дочери не снижается, и ей необходима медицинская помощь, на что по телефону сотрудница спросила: «С чего это вдруг Вы посчитали, что к Вам должна быть направлена скорая помощь?». Неоднократно по телефону мама ребенка пыталась объяснить о том, что дочери плохо и она без сил, температура не снижается. И все же сотрудница скорой помощи сообщает: «ждите», и вешает трубку. Заново перезвонив в скорую медицинскую помощь, уже другой сотрудник пояснил, что скорая медицинская помощь не направлена, а вызов был адресован в поликлинику и в связи с этим необходимо ожидать на дому участкового врача. С одной стороны, вызов был принят, с другой, было осуществлено перенаправление вызова участковому врачу. Сам факт заключается в том, что принятый вызов скорой медицинской помощи не был осуществлен. Кроме того, при обращении с жалобой в Министерство здравоохранения, было выявлено следующее: сотрудник, принимавший вызов от гражданки записала неточные данные, вместо озвученной температуры 41 градус, указала 38,7. Тем самым, с одной стороны, данный факт указывает на умышленные неправомерные действия медицинского работника. А с другой, необходимы доказательства, о наличии вышеуказанного обращения (к примеру, запись разговора с сотрудником). Ведь такие данные никто не представляет.

Содержания понятия, по своей сути, «медицинская помощь» и определение ее качества указаны в Законе об охране здоровья. На основании его положений можно сформулировать принципы оказания медицинской помощи, и произвести оценку ее качества. Принципами оказания медицинской помощи, прежде всего, являются: своевременность, профессиональность, преемственность, оказание медицинской помощи утвержденными методами и (или) с соблюдением условий применения научно обоснованных неутвержденных методов (обоснованность) в достаточном объеме, в пределах имеющихся возможностей учреждения здравоохранения или медицинского работника (оптимальность), при согласии пациента на медицинскую помощь и с соблюдением его права на получение информации о своем здоровье и перспективах лечения. В итоге медицинская помощь должна приводить к максимально благоприятному для пациента результату. По приведенному примеру, можно судить о несоблюдении принципа оказания медицинской помощи, что также является ненадлежащим исполнением медиком своих профессиональных обязательств при оказании помощи пациенту. Но и о доказательствах обращения и ненадлежащего действия персонала скорой помощи по телефону представляет определенную сложность [1].

Ятрогенное заболевание является неблагоприятным последствием допущенным нарушением со стороны медика в системе государственных отношений «врач – пациент», как правило, это нарушение врачом установленных предписаний, стандартов при оказании медицинской помощи. Указанные выше стандарты включают в себя необходимый перечень лечебно-диагностических мероприятий по наблюдению больных конкретной формой с учетом возраста, пола и ряда других биологических факторов [2].

Известно, что ятрогения возникает из-за неосторожного действия медицинского работника. Однако и прямо противоположные действия, а именно, при надлежащем действии врача вызванные обстоятельствами, когда врач не мог и не должен был предвидеть отклонений от правил. Однако с вышеприведенным примером сотруднику скорой медицинской помощи на руку указать не верную информацию при приеме вызова.

Отклонения от указанных правил оказания медицинской помощи классифицируется:

– по содержанию:

– превышение профессиональных полномочий, выход за установленные границы предписанной медицинской деятельности по оказанию помощи больным;

– не выполнение предписаний по оказанию медицинской помощи, необходимых для успешного, желаемого достижения результата по восстановлению здоровья, сохранению и улучшению жизни больного;

– по характеру:

– положительному: отклонению, связанному с профессиональным риском, когда медицинские правила положительно применяются в установленном законом порядке, имеет апробацию на практике и достаточное количество научных разработок, при этом пациентом дано согласие на его проведение согласно ст. 32, 43, кроме того, врач работает при этом с достаточным опытом по данной профессиональной деятельности. Далее отклонения могут быть связанные с проведением медицинского эксперимента, где лечение и лекарственные препарату не допущены к применению, но имеются добровольное согласие, оформленное письменно, медицинские технологии осуществляются в интересах пациента, которые в свое время прошли проверку на животных [1].

Мы не видим возможности привлечения к ответственности медицинского работника при допущении неточного алгоритма работы, либо сбоя при использовании высокотехнологичного оборудования и отсутствия возможности получения доказательств записи при установлении обращения в скорую медицинскую помощь.

Список литературы

1. Возбуждение уголовного дела и начальный этап расследования. URL: https://mylektsii.ru/4-10231.html#2

2. Тузлукова М. В. Актуальные вопросы расследования ятрогенных преступлений // Вестник Московского университета МВД России. 2012. № 11. С. 34–36.

3. Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

Ф. А. Мухитдинова,
доктор юридических наук, профессор,
Ташкентский государственный юридический университет

ПРИМЕНЕНИЕ ЦИФРОВИЗАЦИИ В ЮРИДИЧЕСКОЙ НАУКЕ: ТЕОРЕТИКО-ПРАВОВОЙ АНАЛИЗ

Аннотация. В статье рассматривается правовая основа, регламентирующая процесс цифровизации, а также осуществляется теоретико-правовой анализ цифровизации, сравнительное и научное исследование современных тенденций в использовании цифровых технологиий в жизни человека на основе изучения зарубежного и национального опыта.

Ключевые слова: цифровизация, ресурс, интернет, отношения, закон, суд, иск, архив, Узбекистан

APPLICATION OF DIGITALIZATION IN LEGAL SCIENCE: THEORETICAL AND LEGAL ANALYSIS

Abstract. The author examines the legal framework governing this process, as well as theoretical, historical and legal analysis of digitalization, comparative and scientific research of modern trends in the use of digital technologies in human life; based on the study of foreign and national experience.

Keywords: digitalization, resource, Internet, relations, law, court, lawsuit, archive, Uzbekistan

Новый Узбекистан выбрал путь инновационного развития в рамках реализации стратегии развития. В этом становятся необходимыми новые подходы и механицизм. Самое главное, что в поисках ответа на вопрос о том, что препятствует инновационному развитию общества с человеческими ресурсами, было разработано множество теорий и концепций, но новая цифровизация и анализ ее правовой базы включают причины вышеуказанных проблем.

Цифровизация – новые подходы к применению в различные сферы жизни общества и производства с внедрением современных цифровых технологий.

Также в основе цифровизации есть защита прав человека без вмешательств человеческих факторов. Например, перевод через компьютерную технологию, и в этом есть значения цифровизации, лежит аналитика данных. Также, если устроить ребенка хоть в детский сад или в школу, то с подключением социальных сетей можно узнать через системы мониторинга рейтинг этих учреждений и вакансии, любой человек сможет получить данные о загруженности и рейтинга. А на основе этих данных – выбирать подходящее для своего ребенка. А логическим продолжением являются дистанционное обучение. Это привело почти все страны к переходу к технологиям дистанционного обучения, что показало отличные результаты в сфере образования в том числе для современного Узбекистана.

Во-первых, в цифровом образовании каждый преподаватель может составлять учебные программы в соответствии с индивидуальной скоростью и способностями каждого своего ученика.

Во-вторых, цифровое обучение дает множество преимуществ и развивает навыки самому ребенку, даже студенту, например, моторику, принятие решений, что заметно повышает общий уровень знаний и успеваемости.

В-третьих, в образовательных учреждениях благодаря использованию цифровых методов пользуются презентациями, видеоматериалами, также практические демонстрации, онлайн-обучение тоже являются преимуществом цифровизации в сфере образования.

А если просмотреть в сфере медицине, то можно сказать, что одна из важных и ключевых целей цифровизации медицины – повышение удобства пользования ее услугами и сервисами. Например, при внедрении электронных рецептов при лечении пациента, то преимущества использования таких документов очевидны для всех участников – и врача, и пациента, и фармацевта. Электронные рецепты очень удобны в перспективе для пациентов с хроническими заболеваниями. Именно им больше выгодны электронные рецепты, так как им не придется в очередной раз ходить за выпиской препарата.

Логическим продолжением хочу отметить, что в здравоохранении тоже пользуются применением цифровой технологий, что позволит: быстрее обследовать пациента и ставить более точный диагноз больному. Это повысить статус медицинских работников, и доверие пациентов врачам.

Основная часть. Важность и актуальность цифровизации уже проанализирована и доказана в работах многих ученых разных направлениях науки, как педагогика, медицина, юриспруденция, строительство и др.

Уже со второй половины прошлого века модели использования электронных и компьютерных средств в образовании предлагались на Западе, убрать молодежь Востока стремилась учиться в европейских вузах. Оправданная концепция нового времени применений новых технологий в образовании еще развивалась к концу XX века с новыми идеями. Изучая доступность применений новейших цифровых технологий как цифровых, ученые стали разрабатывать новые условия для обучения молодежи.

К примеру, можно привести научную работу Ш. Ш. Садыкова про специфику цифрового обучения и совершенствование высшего образования Республики Узбекистан в условиях цифровой трансформации экономики. Что важно в этих исследовательских работах, в новое время применяется дистанционное обучение, с применением программу «ZOOM», а в аудиториях уже несколько лет применяются проекторы, электронные журналы, дневники и т. д. Об этом свидетельствуют научные труды Х. М. Ромеро-Родригес, И. Аснар-Диас, Ф. Х. Фенохо-Лусена.

Опыт Германии: статьи В. Е. Гаибова, Л. Н. Данилова «Digitalization in higher education: new didactic concepts» внесли новшество о применяемых цифровых элементах и технологиях в высшем образовании в разных странах. По данным их исследований можно предложить следующее: во-первых, ссылаясь на отечественные педагогические методы и применения цифрового обучения, можно говорить

о использовании в цифровом формате лекций с применением проекторов и компьютера, и др.

Во-вторых, улучшение и применение мобильного обучения, обучения в социальных сетях;

В-третьих, применение имитационных моделирований.

Сегодня уже четверый вид применяется уже в межгосударственных мероприятиях, как научные конференции в формате онлайн-формы и др.

Прежде всего, поясним: цифровизация образования и дистанционное онлайн-образование – не одно и то же. Понятие цифровизации гораздо шире. Оно означает использование различных программ, приложений и других цифровых ресурсов для электронного обучения как удаленно, так и непосредственно в школе или вузе (например, когда какие-то задания выполняются на компьютере или на планшете в классе).

Кроме того, цифровизация касается не только учебных процессов, но и организационных. Например, те же электронные дневники и журналы, а также возможность написать учителю электронное сообщение вместо того, чтобы звонить или приходить в школу лично, – это тоже цифровизация.

Цифровизация образования стала особенно заметной после начала пандемии коронавируса. Школы и вузы вынужденно переехали на дистант в онлайн, и это затронуло всех – школьников и их родителей, учителей, студентов и преподавателей вузов.

Но на самом деле процессы цифровизации начались гораздо раньше. Использование цифровых средств в образовании – мировой феномен. О масштабах явления свидетельствует хотя бы размер рынка образовательных цифровых технологий (этот рынок называется EdTech) – к 2025 году, по оценке Всемирного экономического форума, он достигнет 342 млрд долларов США. Только на одной платформе Coursera в прошлом году училось онлайн 100 миллионов слушателей.

Цифровизация всех сфер деятельности человека приводит к тому, что обучение в высшей школе тоже нуждается в цифровой модернизации, традиционный педагогический процесс дополняется электронным. Фактически первая категория в немецком исследовании – это цифровые средства, третья – цифровые практические методы обучения, четвертая – формы организации обучения.

Так 29 июня 2021 года было принято постановление Президента Республики Узбекистан «О мерах по дальнейшему совершенствованию деятельности юридических служб государственных органов и организаций». По постановлению, предусматривалось создание центров юридического обслуживания во всех районах (городах) республики. На данный момент центры, которые начали свою деятельность, выполняют поставленные перед ними задачи один за другим.

Центр юридических услуг, который поставил перед собой ряд целей, таких как оказание качественной и квалифицированной юридической помощи государственным организациям и повышение правовой грамотности и правовой культуры работающих в них сотрудников, а также обеспечение юридической и всесторонней тщательности и высокого качества документов, принятых государственными

органами. Государственные организации сегодня используют возможности цифровизации.

Электронная система «е-юрист» создает легкость при выполнении таких работ, как внедрение в электронную систему образцов документов внутреннего распорядка, договоров и другого правового характера и бесплатное использование образцов существующих проектов документов, доступ к личному кабинету организациями, использующими электронную систему, подготовка любого проекта документа и аналитических материалов к нему, обработка

В частности, подготовка соответствующих заключений ответственными сотрудниками Центров, прикрепление документов к электронной системе электронной цифровой подписью и взаимный обмен документами, выдача и электронный прием специального номера, который не может быть повторен после получения положительного заключения от центров организациями, использующими электронную систему, автоматическая нумерация этих документов в последовательной последовательности, подтверждение

Указ «О дополнительных мерах по коренному совершенствованию юридического образования и науки в Республике Узбекистан», подписанный президентом, служит для вывода деятельности нашего университета на новый уровень в направлении научных работ и инноваций, а также во всех сферах.

Необходимо отметить, что сегодня от системы образования, особенно юридического, требуется быстрая адаптация к новым вызовам, с которыми сталкиваются общество и экономика в эпоху глобализации.

Особенности образовательного процесса в высших учебных заведениях, а также значение университетов в обществе и экономике быстро меняются. Во всем мире университеты конкурируют друг с другом в привлечении студентов, преподавателей и финансов. В такой конкуренции университеты, которые идут в ногу со временем и используют новые цифровые возможности, получают преимущество перед другими.

Цифровизация предоставила новые возможности для образования и управления, облегчив сбор и анализ данных, взаимодействие и коммуникацию. Преимущества оцифровки включают в себя повышение эффективности, активности учащихся, личностно ориентированное образование и использование новых методов обучения. Также она облегчает управление университетами, учебными планами, профессорами, персоналом и ресурсами.

Одним из главных преимуществ цифровизации является возможность повышения активности студентов. Используя цифровые инструменты, такие как платформы онлайн-образования, социальные сети и мобильные приложения, университеты могут создавать интерактивные и увлекательные образовательные программы, которые поддерживают мотивацию студентов и позволяют им двигаться в нужном направлении. Цифровизация также позволяет университетам использовать новые методы обучения, такие как игры и виртуальная реальность.

Также определены приоритеты дальнейшего развития юридического образования и науки, среди которых создана образовательная среда, которая открыта,

прозрачно, свободной от субъективизма и злоупотреблений, внедряет систему «Электронный университет» (E-University).

В соответствии с этим в Ташкентском государственном юридическом университете разработан и внедрен ряд электронных систем. В частности, оформлена электронная заявка для студентов по любому вопросу, внедрен специальный центр обслуживания студентов, который работает по принципу «единого окна», создана электронная система защиты выпускных квалификационных работ и магистерских диссертаций и отбора научных руководителей, механизм электронного получения договора об оплате и был запущен онлайн-контроль задолженности по платежам.

Сегодня в вузах применяются на занятиях использование цифровых учебников, видеоуроков, видеолекции совмещаются даже в Ютубе. Молодежь в любое время может использовать и повышать своих знаний с использованием видео лекции любого ученого и по юриспруденции, и по медицине, и так далее. Но важно то, что сегодня многие люди, которые находятся дома, с использованием компьютерных технологий, мобильного устройства могут узнать положительные и отрицательные стороны любой лекарственных препаратов, даже народное лечение.

Самым основным результатом, связанным с образовательным процессом, стало внедрение платформы дистанционного обучения и электронной системы оценивания. Университетская платформа дистанционного обучения (http://distant.tsul.uz), в то время как в всемирно признанной системе «Moodle» (объектно-ориентированная динамическая среда обучения) эта система была значительно усовершенствована. В частности, используются программное средство «Zoom» для проведения лекционных занятий, механизмы подачи контрольных работ и передачи их из системы «Антиплагиат», на сайте размещено более 21 тысячи электронного контента (видеозапись, аудио, электронные рефераты, материалы Kazus), образовательная платформа.

Сегодня Ташкентский государственный юридический университет имеет более 40 зарубежных партнеров, 31 из которых являются престижными университетами в международном рейтинге. В рамках этого международного сотрудничества определены вопросы академического обмена студентами, взаимодействия профессоров и преподавательского состава в области юридической науки и образования, стажировок.

С этой целью было достигнуто соглашение с Регенсбургским университетом, что повышает интерес обучения в Германии и студентам, и даже профессорскому составу. Правовой основой является двухсторонний договор, который был подписан в 2020 г. в Ташкенстком государственном юридическом университете с открытием центра немецкого права и сравнительно-правовых исследований.

Выпускники юридического университета идут на работу как в судебную власть, адвокатуру, нотариальные конторы где и сегодня уже пользуются компьютерными технологиями, но больше всего меня интересует цифровизация после окончания университета, использование в судопроизводстве выпускниками.

Во-первых, это имеет огромное значения для обеспечения открытости, гласности, в работу, судов особое внимание уделяется внедрению новейших информационных технологий, где мало используется человеческий фактор. Во-вторых, электронное обращение граждан в судебную систему или наоборот через систему электронного судопроизводства, дистанционно рассматриваются судебные дела.

Указ Президента Республики Узбекистан от 13 июля 2018 года «О мерах по дальнейшему совершенствованию судебно-правовой системы и повышению доверия к органам судебной власти» стал правовой основой внедрения практики процедуры систематических публикаций судебных решений.

К чему привела цифровизация в судебной власти? Во-первых, после того как применяться обращение граждан через системы электронных судов Республики Узбекистан суды стали оснащаться современными средствами информационно-коммуникационных технологий. Особое место занимает в судебной власти, где граждане, проживающие в разных регионах республики одновременно могут участвовать через онлайн-видеоконферец-связь, не выходя из дома, могут участвовать дистанционно в судебных заседаниях, защищая свои права. Какие преимущества имеет такая цифровизация в судебной власти? Эта система удобна тем, что участие в судебных заседаниях без необходимости покидания участниками своего региона;

Во-вторых, такое внедрение позволяет сократить время для рассмотрения иска в краткие сроки, сэкономить финансовых средств сторон.

В-третьих, в судах первой инстанции внедрено полностью программное обеспечение, что без вмешательство со стороны равномерно распределяет и исковые дела среди судей, позволяет внесение справедливых решений, подписанные электронных цифровой подписью судьи.

Логическим продолжением стало внедрение в практику отправления в электронном виде решений, вынесенных судами исполнительных документов, в органы принудительного исполнения. Сегодня даже решения по алиментам на ребенка или на родителей тоже могут получить истцы в этом виде.

Также, новшеством стало создание электронного архива, сохраняющего решения судов.

Поэтому гражданам сегодня нравится защищать свои права, находясь дома, в электронном виде обращаться в суды. Ведь им доступен отслеживать ход рассмотрения своих заявлений.

Есть споры и дискуссии в сфере цифровизации, так как некоторым кажется цифровизация спорным процессом.

Ведь доступно и легко использовать цифровизацию в любой сфере жизни. Самое простейшее – вызов такси через приложения в мобильном устройстве как «Яндекс», «Такси». Или приобретение билетов на самолет, поезд и т.д. Еще более доступным становиться туристические обслуживание: любая страна, любой вид туризма через онлайн-программ. Очевидно, что не любой цифровой инструмент – благо для обучения и что иногда неудачи в процессе внедрения технологии сводят на нет благие намерения.

Поэтому сегодня мы хотим поддерживать цифровизацию во всех сферах жизни общества как противостояние коррупции, вмешательству со стороны.

Реализуемые государственными органами программы и проекты в сфере цифровизации и в сфере образования ориентированы на трансформацию всего технологического процесса обучения и подготовку высококвалифицированных специалистов инновационной формации, соответствующих новым требованиям цифровой экономики. Применительно к Ташкентскому юридическому университету, хотела бы отметить что в университете идет колоссальная работа для обучения студентом английского, китайского права с использованием смарт контрактов и международными электронными договорами, которые являются основой развития международного торговля и международно- частные правовых отношений современности.

В этом я вижу значение цифровизации в юриспруденции.

Следует отметить, что в ближайшем будущем юридическая наука и образование современного Узбекистана, глубоко интегрированные с передовым мировым юридическим образованием, использованием цифровизации, внесут свой вклад в правовое обеспечение всех сфер нашей страны. И в заключение хочу отметить организаторов международной онлайн-конференции, которые дали возможность ученым многих стран участвовать и обменяться своими исследовательскими научными работами в сфере цифровизации в юридической науке. Как профессор Ташкентского государственного юридического университета, преподаватель истории государства и права, а также истории политических и правовых учений хочу отметить самое главное: «Цифровизация – это удар по коррупции в любой сфере жизни общества».

Список литературы

1. Об утверждении Указа Президента Республики Узбекистан, от 29.04.2020 № УП-5987 «О дополнительных мерах по кардинальному совершенствованию юридического образования и науки в Республике Узбекистан». URL: https://lex.uz/ru

2. Об утверждении Постановления Президента Республики Узбекистан, от 29.06.2021 г. № ПП-5168 «О мерах по дальнейшему совершенствованию деятельности юридических служб государственных органов и организаций». URL: https://lex.uz.

3. The Main Directions of Improving Higher Education in the Republic of Uzbekistan in the Context of Digital Transformation of the Economy.

4. Romero-Rodríguez J. M., Aznar-Díaz I., Hinojo-Lucena F. J. Models of good teaching practices for mobile learning in higher education // Palgrave Commun. 2020. Vol. 6(80).

Л. Т. Назаркулова,
кандидат юридических наук, доцент,
Западно-Казахстанский университет,
имени М. Утемисова
Л. С. Серикова,
кандидат исторических наук, заведующая кафедрой,
Западно-Казахстанский университет
имени М. Утемисова

НЕКОТОРЫЕ ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЦИФРОВИЗАЦИИ В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация. В статье рассмотрены основные направления развития информационнно-коммуникативных технологий и цифровизации в Республике Казахстан, а также некоторые проблемы правового регулирования общественных отношений в этой сфере. Обоснован ряд основных проблем в сфере правового регулирования процессов цифровизации в стране. Отмечается значительный разрыв между развитием общественных отношений в сфере цифровизации и их правовым регулированием. Проблемы правового регулирования цифровизации создают риски для обеспечения кибербезопаности страны и нарушения прав граждан. Однако кодификация законодательства в сфере цифровизации обосновывается как преждевременная мера.

Ключевые слова: цифровизация, информационно-коммуникационные технологии, цифровое государство, цифровой Казахстан, невидимое государство, финтех, цифровой кодекс

SOME ISSUES OF LEGAL REGULATION OF DIGITIZATION IN THE REPUBLIC OF KAZAKHSTAN

Abstract. The article examines the main directions of development of information and communication technologies and digitalization in the Republic of Kazakhstan, as well as some problems of legal regulation of public relations in this area. A number of main problems in the field of legal regulation of digitalization processes in the country are substantiated. There is a significant gap between the development of public relations in the field of digitalization and their legal regulation. Problems of legal regulation of digitalization create risks for ensuring the country's cybersecurity and violation of citizens' rights. However, the codification of legislation in the field of digitalization is justified as a premature measure.

Keywords: digitalization, information and communication technologies, digital state, digital Kazakhstan, invisible state, fintech, digital law

Информационно-коммуникационные технологии (далее – ИКТ), цифровизация – приоритетные направления развития Республики Казахстан. В этих целях был принят ряд стратегических государственных программ, нормативных

правовых актов (Государственная программа «Информационный Казахстан-2020» 2013 г. и др.).

Одним из важнейших таких документов стала Государственная программа «Цифровой Казахстан» на 2018–2022 годы (утверждена постановлением Правительства Республики Казахстан от 12 декабря 2017 г.) были поставлены две основные цели:

1) «цифровизация существующей экономики» (ускорение темпов развития экономики республики и улучшение качества жизни населения за счет использования цифровых технологий в среднесрочной перспективе;

2) «создание цифровой экономики будущего» (создание условий для перехода экономики Казахстана на принципиально новую траекторию развития, обеспечивающую создание цифровой экономики будущего в долгосрочной перспективе.

В рамках программы было поставлено десять основных задач, которые можно сгруппировать в следующие пять основных направлений:

– цифровизация отраслей экономики (цифровизация промышленности и электроэнергетики, транспорта и логистики, сельского хозяйства, развитие электронной торговли, финансовых технологий и безналичных платежей);

– цифровизация государства (Государство – гражданам, государство – бизнесу, цифровизация внутренней деятельности государственных органов);

– «Реализация цифрового Шелкового пути» (развитие высокоскоростной и защищенной инфраструктуры передачи, хранения и обработки данных);

– «Создание инновационной экосистемы» («умные» города, расширение покрытия сетей связи и ИКТ инфраструктуры, обеспечение информационной безопасности в сфере ИКТ), ;

– развитие человеческого капитала (повышение цифровой грамотности в образовании и среди населения, поддержка площадок инновационного развития, развитие технологического предпринимательства, стартап культуры и НИОКР, привлечение «венчурного» финансирования).

Основная часть. Программа, принятые НПА дали большой импульс для развития ИКТ во многих сферах общества. Наиболее активными участниками программы стало само государство в лице различных государственных органов и бизнес.

В государственной сфере в результате цифровизации продолжает развиваться «Электронное правительство», автоматизируется деятельность государственных органов. По всей стране функционируют центры обслуживания населения, единый контакт-центр, площадка Открытого правительства, портал «открытых данных». Предполагается полная цифровизация налогового контроля, объединение на единой цифровой платформе сведений о состоянии сельскохозяйственных земель, водных ресурсов, ирригационных систем, транспортной доступности. Активно «оцифровывается» судебная система: создан «Судебный кабинет», разрабатывается цифровой аналитический инструментарий, который призван обеспечить единообразие в отправлении правосудия.

Новым этапом развития ИКТ в государственной сфере стала реализация нового формата получения государственных услуг – Invisible Government

(«невидимое правительство»). При этом главная цель такого формата – человекоцентричность, оперативное решение запросов гражданина с минимизаций личного взаимодействия гражданина с представителями госорганов, недопущение проволочек с бюрократией, коррупцией. Сегодня уже множество видов государственных услуг можно получить через мобильное приложение eGov или в тех мобильных приложениях, которыми пользуется население, в частности, приложения банков. Реализуются проекты «Цифровая карта семьи», «Социальный кошелек», «Е-заявление» и др. Одно из последних достижений – это возможность упрощенного подписания документов посредством QR с предварительным ознакомлением с содержанием документа. Эта возможность также активно может использоваться и бизнесом. Маленькими шагами Казахстан движется к большим амбиционным целям – стать крупнейшим цифровым хабом в Евразийском пространстве.

В сфере бизнеса одним из бурно растущих направлений развития ИКТ являются финансовые технологии. Это связано с ростом потребительского спроса, активным сотрудничеством финансовых и нефинансовых организаций с цифровыми компаниями, поддержке государства, в том числе и в лице Международного финансового центра «Астана» (МФЦА) и др. Эти и другие факторы способствовали росту потенциала Казахстана для финтех-инноваций и стратапов, сокращению разрыва среди населения к доступу к финансовым услугам.

Среди наиболее активно развивающихся направлений в финансовой сфере можно назвать рост цифровых платежей, благодаря биометрическим технологиям, расширенной аналитике данных, возможностям мгновенных переводов, управлением цифровым согласием клиента на использование его персональных данных и др.

Расширение интеграции финансовых инструментов и государственных сервисов способствуют повышению качества получения государственных, а также росту транзакционной активности банков, что выгодно всем сторонам (об этом упоминалось выше). Например, широкую популярность среди населения обрели приложения банков Kaspi и Homebank, через которые возможно получение различных государственных услуг: получение справок, цифровых документов, оплата налогов, регистрация ИП, продажа и регистрация автомобилей и другое.

Активно развиваются онлайн-сервисы в сфере B2B-услуг, такие как выставление счетов, бухгалтерский учет, платежи, кадровая и юридическая поддержка. Ряд технологических решений (биометрическая идентификация, мобильные приложения и др.) сделали рынок капитала более доступным для розничных инвесторов. Развиваются экосистемные сервисы, прежде весго, когда в одном приложении можно получить большое число услуг (финансовые, гражданско-правовые, государственные и др.). Широкое развитие получает электронная коммерция. Создана бизнес-ассоциация по содействию развитию в Казахстане сильного рынка электронной коммерции и торговли.

Правовое обеспечение процессов цифровизации обеспечивается целым рядом НПА: Законы Республики Казахстан «Об информатизации», «Об электронном документе и электронной цифровой подписи», «О персональных данных и их защите», «О связи» и другими; а также целым рядом подзаконных НПА.

Несмотря на значительные достижения по цифровизации и развитию ИКТ вместе с тем следует отметить и проблемы в этой сфере. Одной из острых проблем является совершенствование и систематизация НПА, регулирующих общественные отношения в сфере цифровизации. Одна из мер была озвучена в июле 2022 года уполномоченным органом, который предложил разработать Цифровой кодекс [1]. Однако данное предложение подверглось критике со стороны юристов. Профессор С. К. Идрышева справедливо отмечает, что принятие цифрового кодекса является не вполне своевременной мерой. Автор предлагает вместо объемлющего кодифицированного акта разработать рамочный закон, который позволяет одновременно совершенствовать действующие НПА и принимать отдельные НПА по новым объектам цифровизации. Дальнейшая апробация такого законодательного массива позволит сформировать материал для успешной кодификации в будущем [2. С. 72]. Мы поддерживаем мнение автора. Во-первых, это противоречит закону РК «О правовых актах», где не предусмотрена кодификация законодательства в сфере цифровизации. Во-вторых, кодификация – это более сложный вид систематизации права, предполагающий высокий уровень владения юридической техникой, апробированного массива правовых норм.

Но на данном этапе развития цифровизации острой проблемой для Казахстана является неразработаность терминов и правовых институтов в сфере ИКТ, что обусловлено в немалой степени и кадровым голодом, нехваткой высококвалифицированных It-специалистов, тем более обладающих юридическими навыками и знаниями. Важно развивать цифровые компетенции и цифровую культуру студентов по юридическим специальностям. Введение учебной дисфициплины «Цифровое право» в учебный процесс специальности «Правоведение» могло бы стать одним из решений данной проблемы [3].

Действующие НПА, регулирующие вопросы цифровизации, отличаются недостаточным уровнем качества, о чем неоднократно писали эксперты/4/. Более приемлемым является закрепление рамочных параметров регулирования общественных отношений в сфере цифровизации, совершенствование действующих НПА и принятие отдельных законоов по новым объектам цифровизации.

Не секрет, что правовое регулирование многих общественных отношения, прежде всего, где развиваются цифровые технологии, осуществляется реактивно: сначала в обществе развиваются те или иные общественные отношения, а затем в спешном порядке принимаются НПА. Так произошло с онлайн-кредитованием. Первые онлайн-кредиты стали выдаваться в 2014 г., но долгое время данный вид деятельности не рассматривался как вид финансовых услуг, не подлежал контролю и правовому регулированию со стороны уполномоченного органа. Это привело к закредитованности населения, нарушениям прав потребителей таких услуг. Только после того, как проблема обрела общественное звучание, стали приниматься первые поправки в действующее законодательство. Несмотря на принятые правовые меры, тем не менее пока еще в этой сфере ряд проблем: слабая защищенность прав потребителей финансовых услуг, значительное число преступлений и злоупотреблений.

Одна из острых проблем – это защита персональных данных, кибербезопасность. В 2019 г. персональные данные 11 млн казахстанцев утекли с серверов Центральной избирательной комиссии. В 2020 г. специалисты ЦАРКА обнаружили утечки данных из Генеральной прокуратуры и Системы контроля качества в сфере здравоохранения. В том же году команда «белых» хакеров проверила на наличие уязвимостей 91 государственный веб-ресурс [5].

Для обеспечения безопасности и защиты персональных данных предлагаются путем их обработки в распределенном реестре, использование которого основано на технологии блокчейн. Считается, что данная технология направлена на упрощение взаимодействия между субъектами расчетных отношений, а также позволяет защищать данные от незаконного изменения и подделки. Вместе с тем пока еще в законодательстве Казахстана недостаточно отражены такие технологические возможности, которые с одной стороны, способствовали бы росту цифровизации, электронной торговле, но с другой – надежно защищали бы права граждан, их персональные данные.

В целях обеспечения кибербезопасности важная роль отводится совершенствованию норм уголовного законодательства с учетом специфики IT-сферы. Уголовным кодексом РК предусмотрена ответственность за создание, использование и распространение вредоносных компьютерных программ и программных продуктов. Однако диспозиция данной статьи не в полной мере учитывает специфику определения «вредоносности» программ. На практике при определении «вредоносности» программ исходят от номенклатуры ведущих производителей антивирусного программного обеспечения, т. е. фактически ставится знак равенства между «вирусом» и «вредоносной программой», что не соответствует действительности. В этой связи, следует внести соответствующие изменения и дополнения в положения уголовного кодекса.

В современных условиях глобализации цифровые технологии играют роль ключевого фактора, который способны кардинально изменить мир. Цифровая глобализация, цифровая экономика и цифровое право – становятся реальностью современного мира. В осмыслении происходящих процессов, прогнозировании позитивных и негативных последствий для общества активных процессов цифровизации, значительная роль отводится юридической доктрине. Однако в Казахстане пока еще недостаточно ведется научных исследований процессов цифровизации в различных сферах общества. В этой связи, рекомендуется включить в перечень приоритетных научных направлений тематику цифрового права, создавать соответствующие научно-исследовательские центры и институты, проводить научно-практические форумы с участием специалистов юристов, IT-специалистов, экономистов и др.

Подытоживая вышеизложенное, отметим, что развитие ИКТ, цифровизация общества актуализируют потребность расширения круга общественных отношений, регулируемых правом. В целях успешной реализации поставленных амбициозных целей и задач в сфере цифровизации важно глубоко осмыслить состояние действующего права, определить приоритеты его дальнейшего развития и конкретные направления совершенствования. Важная роль отводится подготовке кадров, обладающих комплексными знаниями и навыками (технические, юридические,

экономические др.), способными заложить фундамент для эффективного правового обеспечения развивающихся общественных отношений в сфере информатизации. Не менее важная роль отводится юридической доктрине в целях выработки оптимальной модели механизма правового регулирования общественных отношений в сфере цифровизации.

Список литературы

1. Цифровой кодекс – единая регуляция всех областей digital-сферы. URL: https://drfl.kz/ru/tsifrovoi-kodieks

2. Идрышева С. К. О цифровом кодексе Казахстана // Государство и право. 2022. № 3(96). С. 72–85.

3. Bugrova V., Kovalevskaia N., Matyashova D., Geleta I. Teaching digital law as a prerequisite for the formation of students' digital competence and digital culture// Revista conrado. Vol. 18. Pp 640–646.

4. Сулейменов М. К. Цифровизация и совершенствование гражданского законодательства (статья третья, исправленная и откорректированная в связи с принятием Закона о цифровых технологиях). URL: https://online. zakon.kz/Document/?doc_id=35012332

5. Как цифровизация в Казахстане стала угрожать кибербезопасности. URL: https://cabar.asia/ru/kak-tsifrovizatsiya-v-kazahstane-stala-ugrozhat-kiberbezopasnosti

В. Д. Никишин,
кандидат юридических наук, доцент,
Московский государственный юридический
университет имени О. Е. Кутафина

ПРАВО НА СВОБОДУ СЛОВА VS. ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ В ЦИФРОВОМ МИРЕ

Аннотация. В статье на примере наиболее актуальных трендов деструктивного контента в современных интернет-медиа раскрыта проблема обеспечения информационно-психологической безопасности интернет-пользователей. Продемонстрировано, что обеспечение информационно-психологической безопасности с правовой точки зрения предполагает соблюдение баланса права на свободу слова, с одной стороны, и право на честь, достоинство, доброе имя, деловую репутацию; право на свободу и личную неприкосновенность; право на жизнь; право на неприкосновенность частной жизни; право на свободу совести и т. д., с другой стороны. Предложены законодательные меры обеспечения информационно-психологической безопасности с учетом новых вызовов криминогенной цифровой коммуникации.

Ключевые слова: безопасность, информационная безопасность, медиабезопасность, информационно-мировоззренческая безопасность, информационно-психологическая безопасность, права человека, цифровая среда, информационное право, информационные угрозы

THE RIGHT TO FREEDOM OF SPEECH VS. INFORMATION SECURITY IN THE DIGITAL WORLD

Abstract. In the article the problem of ensuring the information (psychological) security of Internet users is revealed on the examples of the most relevant trends of destructive content in modern Internet media. It is demonstrated that ensuring information (psychological) security from a legal point of view involves maintaining a balance of the right to freedom of speech, on the one hand, and the right to honor, dignity, good name, business reputation; the right to liberty and security of person; the right to live; the right to privacy; the right to freedom of conscience, etc., on the other hand. Legislative measures are proposed to ensure information (psychological) security, taking into account the new challenges of criminogenic digital communication.

Keywords: security, information security, media security, information and ideological security, information and psychological security, human rights, digital environment, information law, information threats

1. Права человека в цифровом пространстве. Понятие информационно-психологической безопасности. Сегодня, когда Интернет и цифровые технологии конструируют не параллельную реальность (куда бы мы могли время от времени «погружаться»), а фактически модифицируют нашу реальность, заполоняя собой и работу, и быт, и иные сферы жизнедеятельности, вопросы защиты прав человека в цифровом пространстве, обеспечения информационной безопасности личности и когнитивного суверенитета государства приобретают все большую актуальность.

Возможность ограничения свободы слова, свободы самовыражения, свободы печати в целях противодействия деструктивному информационно-психологическому воздействию, т. е. обеспечения информационно-психологической безопасности, предусматривается ст. 29, ст. 55 Конституции Российской Федерации, большинством международных актов, гарантирующими данные права и свободы (например, Всеобщей декларацией прав человека от 10 декабря 1948 года [1], Международным пактом о гражданских и политических правах (ст. 19-20) [7], Конвенцией о защите прав человека и основных свобод от 4 ноября 1950 года [5], Международной конвенцией о ликвидации всех форм расовой дискриминации от 21 декабря 1965 года [6], Декларацией Генеральной Ассамблеи ООН от 25 ноября 1981 года о ликвидации всех форм нетерпимости и дискриминации на основе религии или убеждений [9], Европейской конвенцией о правах человека (ст. 10, ст. 17) [3] и др.).

Интернет – и благо, и зло одновременно: пространство знаний и свалка разносортной информации; пространство продуктивного взаимодействия и среда для деятельности мошенников, манипуляторов, социальных «инженеров», вербовщиков, пропагандистов и т. д.

Деструктивное информационно-психологическое воздействие в цифровой среде посягает на такие права человека, как право на доступ к информации; право на честь, достоинство, доброе имя, деловую репутацию; право

на неприкосновенность частной жизни; право на свободу и личную неприкосновенность; право на свободу совести; право на жизнь и т. д. [8].

Информационно-психологическая безопасность предполагает защиту от манипулирования сознанием личности, насаждения симулякров и формирования, соответственно, псевдореальности, картины мира с искаженными или подмененными ценностями, установками и т. д., где во главу угла ставится культ агрессии к окружающим (собственно агрессивный дискурс) или к себе самому (депрессивно-аутодеструктивный дискурс) [2].

2. Актуальные тренды деструктивной цифровой коммуникации. В настоящей статье будут рассмотрены только отдельные, наиболее актуальные, угрозы информационно-психологической безопасности в цифровой среде.

Во-первых, в распространяемом сегодня в интернет-медиа деструктивном контенте красной нитью проходит идеология обесценивания человеческой жизни, культивация человеконенавистничества.

Во-вторых, продолжается распространение контента, направленного на возбуждение ненависти и вражды (ст. 282 УК РФ), культивацию сепаратистских настроений (ст. 280.1 УК РФ), аргументируемых политикой «деколонизация» (распространяется ложный тезис о насильственном присоединении российским государством южных, сибирских и др. регионов и необходимости выхода конкретных субъектов из состава Российской Федерации/делении Российской Федерации на ряд самостоятельных государств), при этом в ряде случаев администраторы онлайн-сообществ типа «Свободный(-ая) <наименование субъекта РФ>» впоследствии раскрывали факт своей деятельности с территории Украины.

В-третьих, ввиду политики блокировки ресурсов экстремистских организаций и контанта, запрещенного к распространению на основании Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» [14], наблюдается «мимикрия» деструктивных сетевых субкультур, использование обновляемого сленга и эвфемизмов (в том числе во избежание блокировки по ключевым словам). Отсюда налицо необходимость совершенствования механизмов мониторинга социальных сетей и мессенджеров, совместная работа научного сообщества, правоохранительных органов, Роскомнадзора и администраций социальных сетей для обновления баз ключевых слов (тезаурусов) для автоматизированных мониторингов. Необходима проработка вопроса ответственности администраций социальных сетей за ведение самостоятельного мониторинга деструктивного контента, так как такая обязанность на них возложена ст. 10.6 Федерального закона «Об информации, информационных технологиях и о защите информации» [12].

В-четвертых, в профилактической работе необходимо учитывать использование манипуляторами потенциала фэндомных сообществ для проведения психологических операций. Яркий пример – квазисубкультура «ЧВК «Редан», «раскрученная» за счет фан-сообщества аниме «Hunter x Hunter». Распространение так называемых редановцев – наглядный пример psy-операции, применения технологий социального инженеринга, когда у нас на глазах в течение пары дней в социальных сетях была создана сеть ресурсов «ЧВК Редан» и мессенджерах

с многотысячными охватами аудитории – сеть, оказывающая реальное психологическое воздействие на подростков и выводящая их на «забивы». Причем история переименований сообществ нередко показывают, что ранее ряд сообществ носил проукраинскую тематику («Слава Украине» и т. п. названия). Такие сообщества, ранее со сравнительно малочисленным количеством подписчиков, за эти несколько дней многократно увеличили свою аудиторию, так как стали появляться в результатах поисковых запросов по ключевому слову «Редан». Есть и примеры сообществ, созданных «с нуля» 19–20 февраля и моментально вовлекших тысячи подростков в свои подписчики. Инфоповод «Редан» является отличным примером создания универсального объекта ненависти у молодых людей различных субкультур, зачастую конфликтующих между собой, а также той части молодежи, которая избегает офлайн-проявлений своих настроений («дед-инсайды»). Так, объединялись в группировки совершенно идеологически недружественные друг к другу группы молодежи: представители кавказской молодежи, АУЕшники, националистические группировки, группы скинхедов и оффников с целью насильственных акций по отношению к представителям «Редана». В свою очередь, множество подростков, причисляющих себя к «дед-инсайдам» или вовсе не состоящие ранее ни в каких субкультурах, выходят на улицы в погоне за «хайпом». Более того, общественный резонанс вокруг «ЧВК Редан» активно использовался представителями теневого сегмента: в крупных телеграм-сообществах «ЧВК Редан» активно рекламировались ресурсы, пропагандирующие и романтизирующие наркоторговлю, употребление наркотиков, сваттинг, продажу нелегального оружия, кардинг и т. д.

В-пятых, еще один существенный тренд медиаповестки социальных сетей, активно распространяющийся примерно с 2020 года, – это распространение контента, популяризирующего антисемейные ценности. Такие информационные стратегии выступают элементом продвижения депопуляционной (антидемографической) политики и выражаются в:

– продвижении ЛГБТ-повестка;

– пропаганде трансгендерство (смены пола), а также склонении к смене пола кураторами (фактически по модели «групп смерти»);

– формировании отрицательного образа материнства, брака, детей, семьи;

– нормализации насилия в отношении детей и беременных женщин;

– проабортной агитации, распространении информации о способах абортов без обращения к врачам.

3. Предложения по гармонизации правового регулировании. Во-первых, назрела необходимость пересмотра перечней видов запрещенной и ограниченной к распространению среди несовершеннолетних информации (видов информации, причиняющей вред здоровью и (или) развитию детей, ст. 5 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» [13].

Во-вторых, нужна системная гармонизация терминологического аппарата описания составов в кодифицированных актах (преступлений и правонарушений, связанных с распространением деструктивной информации): как между собой, так и в корреляции с запретами на распространение отдельных видов информации,

закрепленных в специализированных федеральных законах (ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Законе о СМИ [4], ФЗ «О противодействии экстремистской деятельности» [11], ФЗ «О противодействии терроризму» [10] и т. д.).

В-третьих, востребована единая критериология деструктивного контента, гармонизация методических подходов, используемых в судебно-экспертных исследованиях информационных материалов (прежде всего, судебной лингвистической экспертизе), в рассмотрении спорных материалов уполномоченными органами (принимающими решения о блокировке контента на основании Постановления Правительства РФ от 26.10.2012 № 1101) и в экспертизе информационной продукции, осуществляемой на основании главы 4 ФЗ о защите детей от информации.

В-четвертых, необходимо усиление контроля выдерживания владельцами социальных сетей и иных интернет-медиа возрастного ценза в группах 18+ с привлечением к ответственности по ст. 6.17 КоАП РФ.

Кроме того, актуальна проработка законодательного регулирования распространения информации в свете использования в интернет-среде инструментов big data, формирующих «информационные колодца», тоннели виртуальной реальности пользователей, т. е. формирующих за пользователя спектр информации, попадающей в его ленту, раздел «Рекомендовано» и т. д.

Список литературы

1. Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.). URL: http://www.consultant.ru/document/cons_doc_LAW_120805

2. Галяшина Е. И., Никишин В. Д. Информационно-мировоззренческая безопасность в интернет-медиа. М., Проспект. 2022. 424 с.

3. Европейская конвенция по правам человека, измененная и дополненная Протоколами № 11 и № 14 в сопровождении Дополнительного протокола и Протоколов № 4, 6, 7, 12 и 13. URL: https://www.echr.coe.int/documents/convention_rus.pdf

4. Закон РФ от 27.12.1991 № 2124-1 «О средствах массовой информации» // СПС «КонсультантПлюс».

5. Конвенция о защите прав человека и основных свобод. URL: http://www.consultant.ru

6. Международная Конвенция о ликвидации всех форм расовой дискриминации. URL: https://base.garant.ru/2540327

7. Международный пакт о гражданских и политических правах. URL: http://www.consultant.ru/document/cons_doc_LAW_5531

8. Никишин В. Д. Трансформация института личной безопасности в условиях новой реальности: информационно-мировоззренческая безопасность цифровой коммуникации. В книге: Право и общество в эпоху социально-экономических преобразований XXI века: опыт России, ЕС, США и Китая. Коллективная

монография к 90-летию Университета имени О. Е. Кутафина (МГЮА) / под общей ред. В. В. Блажеева, М. А. Егоровой. М., 2021. С. 265–284.

9. Резолюция Генеральной Ассамблеи ООН от 25 ноября 1981 г. № 36/55 «Декларация о ликвидации всех форм нетерпимости и дискриминации на основе религии или убеждений». URL: https://base.garant.ru/2565457

10. Федеральный закон 06.03.2006 № 35-ФЗ «О противодействии терроризму» // СПС «КонсультантПлюс».

11. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» // СПС «КонсультантПлюс».

12. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».

13. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // СПС «КонсультантПлюс».

14. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // СПС «КонсультантПлюс».

Б. А. Окишев,
аспирант,
Московский государственный юридический
университет имени О. Е Кутафина

ПРОБЛЕМА ОТНЕСЕНИЯ СВЕДЕНИЙ ОБ ИНВАЛИДНОСТИ К СПЕЦИАЛЬНЫМ КАТЕГОРИЯМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. Статья посвящена ряду вопросов правовой охраны и защиты персональных данных в сфере медицины и здравоохранения, в частности проблеме отнесения сведений об инвалидности к специальным категориям персональных данных в Российской Федерации; судебной практике отнесения сведений об инвалидности к определенной категории; проблематике совершенствования законодательства об основах охраны здоровья граждан в Российской Федерации в соответствии с законодательством о персональных данных.

Ключевые слова: правовая охрана, персональные данные, врачебная тайна, обработка и распространение персональных данных, раскрытие персональных данных, сведения об инвалидности, специальная категория персональных данных

THE PROBLEM OF ATTRIBUTING DISABILITY INFORMATION TO SPECIAL CATEGORIES OF PERSONAL DATA

Abstract. The article is devoted to a number of issues of legal protection and protection of personal data in the field of medicine and healthcare, in particular, the problem of attributing information about disability to special categories of personal data in the Russian Federation; judicial practice of attributing information about disability; the problems of improving legislation on the basics of protecting the health of citizens in the Russian Federation in accordance with the legislation on personal data.

Keywords: legal protection, personal data, medical secrecy, processing and dissemination of personal data, disclosure of personal data, information about disability, special category of personal data

Персональные данные, составляющие сведения о здоровье граждан, представляют собой медицинские данные. Федеральным законом «О персональных данных» [9] (далее – «Федеральный закон № 152-ФЗ») сведения о состоянии здоровья отнесены к персональным данным.

Сфера данных о здоровье гражданина охватывает широкий спектр информации. Сюда входит личная информация о гражданине (именуемая персональными данными), относящаяся к состоянию здоровья человека, а также медицинская информация (например, рецепт врача, направления, протоколы медицинских осмотров, лабораторные анализы и т. д.), административная и финансовая информация о здоровье (в частности расписание приемов к врачу, счета за медицинские услуги, медицинские справки для оформления больничных листов и т. д.).

Стоит обратить внимание, что напрямую вопросы здоровья граждан отнесены именно к медицинской информации (медицинскими данными, содержащимися в медицинских документах), в то время как административная и финансовая информация лишь косвенно затрагивают медицинские данные гражданина, выполняя «обслуживающие» функции. Данное разделение имеет практическое значение в части реализации охраны персональных данных граждан в сфере медицины, так как от того, какая именно информация закреплена и какими именно документами она подтверждается, зависит круг лиц, которым сведения, составляющие информацию о здоровье граждан, могут быть переданы. Например, отделу кадров работника, находящегося на больничном, медицинской организацией будет разглашена информация, составляющая персональные данные в сфере медицины, лишь косвенно затрагивающая вопросы здоровья работника, а именно в виде листка нетрудоспособности, что по выделенной нами классификации относится к административной и финансовой информации [2. С. 120–126].

С учетом развития права в сфере защиты персональных данных, интересным и спорным вопросом, который носит непосредственно практический правоприменительный спор – является проблема отнесения сведений об инвалидности к специальным категориям персональных данных

Однозначного ответа на вопрос, относятся ли сведения об инвалидности к специальным категориям персональных данных, в законе нет. Часть 1 статья 10 Федерального закона № 152-ФЗ относит к специальным категориям персональных данных сведения касающиеся состояния здоровья. При этом закреплено легальное определение только «здоровья» (п. 1 ч. 1 ст. 3 Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 № 323-ФЗ [8] (Далее – «Федеральный закон №323ФЗ»), но в законе не приведено термина «состояние здоровья».

Данный пробел прямого регулирования вопроса породил определенную практическую проблему, так мнение по отнесению сведений об инвалидности к специальным категориям персональных данных у судов и Роскомнадзора разделилось.

В частности, кажется, что данная проблема состоит в не профильности суда по разрешению конкретных споров.

Согласно позиции Роскомнадзора от 02.04.2012 № 01ШР.07234 в ответе на частное обращение, информация в листке нетрудоспособности, в том числе об установлении или изменении группы инвалидности, является сведениями о состоянии здоровья субъекта персональных данных [3]. В частном ответе на запрос, Роскомнадзор в октябре 2022 уточнил, что обработка справки об инвалидности по зрению подразумевает обработку специальных категорий персональных данных [5]. Не требуется согласия на обработку персональных данных в связи с обработкой справки об инвалидности по зрению в целях реализации права такого инвалида на использование факсимильного воспроизведения собственноручной подписи. Основание обработки здесь п. 2.3. ч. 2 ст. 10 Федерального закона №152-ФЗ, а также ст. 14.1 Федерального закона «О социальной защите инвалидов в Российской Федерации» от 24.11.1995 № 181-ФЗ [10] (Далее – «Федеральный закон №181-ФЗ»).

Судебная практика в части разрешения споров, связанных к отнесению информации о группе инвалидности к специальной категории персональных данных – немногочисленная. В вынесенных решениях суды к единой позиции не пришли. В ряде дел отмечается, что обработка данных об инвалидности подпадает под понятие обработки одной из специальных категорий персональных данных [6]. Суд указал, что нижестоящие суды обоснованно исходили из наличия в действиях предприятия нарушений требований части 1 статьи 10 Федерального закона №152-ФЗ, поскольку в ходе проверки выявлено содержание данных об инвалидности в скриншотах с базы данных кадровой службы и в анкете кандидата, заполняемой при приеме на работу.

При этом в другом решении суда утверждается, что инвалидность – это социальный статус. То есть к специальным категориям персональных данных, данные об инвалидности не относятся [7].

Так, суд в решении по делу указал, что согласно статье 1 Федерального закона № 181-ФЗ инвалид – лицо, которое имеет нарушение здоровья со стойким расстройством функций организма, обусловленное заболеваниями, последствиями травм или дефектами, приводящее к ограничению жизнедеятельности и вызывающее необходимость его социальной защиты. Признание лица инвалидом осуществляется федеральным учреждением медико-социальной экспертизы. Исходя из положений указанной статьи, следует вывод о том, что обработка данных о состоянии здоровья (степень расстройства функций организма, заболевания, дефекты и травмы) осуществляется учреждениями медико-социальной экспертизы. После присвоения группы инвалидности, лицо получает статус, требующий его социальной защиты, с чем работают социальные учреждения, в том числе центры по трудоустройству. Таким образом, данную категорию персональных данных как инвалидность, в соответствии с пунктом 2 части 2 статьи 10 Федерального закона № 152-ФЗ можно отнести к общедоступным.

На практике операторы персональных данных до сих пор принимают решение об отнесении данных об инвалидности к сведениям о состоянии здоровья в зависимости от сложившейся в компании риск-культуры. Обоснование данного

поведения компаний достаточно понятное – компании идут по пути закрытия наибольших рисков для компании.

В случае классификации сведений об инвалидности к социальному статусу нужно быть готовым к доскональному обоснованию позиции при проверке и суду с Роскомнадзора. Ответственность за нарушение требований закона может быть, как по ст. 19.7 КоАП РФ [1], так и по одной из частей ст. 13.11 КоАП РФ.

В случае отнесения инвалидности к специальной категории персональных данных нужно быть готовым к их обработке в строго определенных случаях (ч. 2 ст. 10 №152-ФЗ), большему вниманию к защите, повышению риска проверок Роскомнадзором. Обработка специальной категории персональных данных и (или) биометрических персональных данных относится к группе тяжести «А» в соответствии с Постановлением Правительства РФ от 29 июня 2021 г. № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных» [4].

Заявляя тему и проблему соотношения баланса правовой защиты и сбора персональных данных в Российской Федерации, необходимо отметить, что для гражданско-правовых отношений, отношений трудовых и в бытовом понимании граждан – данные об инвалидности без подробностей о характере и подробных данных из медицинской книжки – является статусом гражданина, который необходим обработчику (обществу) для учета особенности работы, рабочего места, характера работы. Усложнение обработки таких данных ведет к тому, что обществам труднее взаимодействовать с более незащищенным слоем общества – с инвалидами. Если учитывать, что бытовая запись в опроснике анкете работодателя об инвалидности является специальной категорией персональных данных, то степень сложности защиты ее хранения и обработки кратно возрастает, это влечет за собой расходы и излишнюю необходимость более серьезно охранять систему и данные ради нескольких сотрудников (например), которые составляют меньшинство в организации.

Таким образом, необходимо выработать легкие и понятные подходы об отнесении категорий информации к той или иной категории и соблюдать равновесие защиты данных и их необходимости обработки в обыденных и бытовых сложившихся обстоятельствах, не допуская дополнительных оснований для дискриминации особых субъектов общества – инвалидов. Мы придерживаемся позиции, что инвалидность – это социальный статус и к специальным категориям персональных данных, данные об инвалидности не относятся.

Список литературы

1. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ. URL: https://www.consultant.ru

2. Окишев Б. А. Реализация охраны персональных данных в сфере медицины // Вестник Университета имени О. Е. Кутафина. 2022. № 4 (92). С. 120–126.

3. Письмо Роскомнадзора «О результатах рассмотрения обращения» от 02.04.2012 № 01ШР.07234. URL: https://rppa.ru/_media/analitika/01shr-07432_02.04.2012.pdf

4. Постановление Правительства РФ от 29 июня 2021 г. № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных». URL: https://base.garant.ru/401416524

5. Пояснения Роскомнадзора по актуальным вопросам. URL: https://t.me/privacyexpert/1100

6. Решение АС города Москвы от 06.05.2011 по Делу №А40-129859/10-146-801. URL: https://clck.ru/36p2KT

7. Решение АС Краснодарского края от 29.04.2011 по Делу № А-32-2810/2011. – URL: https://clck.ru/36p2L6

8. Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 № 323-ФЗ. URL: https://docs.cntd.ru/document/902312609

9. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (ред. от 02.07.2021) // Собрание законодательства РФ. 2006. № 27 (ч. 1). Ст. 5159

10. Федеральный закон от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации». URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102038362

Л. Н. Осауленко,
кандидат юридических наук,
Евразийская экономическая комиссия

ЗАЩИТА ПРАВ ПОТРЕБИТЕЛЕЙ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЕАЭС

Аннотация. В статье рассматриваются основы и предпосылки формирования потребительского права Евразийский экономического союза, а также подходы, способствующие совершенствованию механизмов обеспечения и защиты потребительских прав граждан государств – членов ЕАЭС в контексте цифровой трансформации экономических процессов. Объектом настоящего исследования явились основные механизмы защиты прав потребителей, закрепленные в законодательстве государств – членов ЕАЭС. Цель исследования – определение направлений дальнейшего развития международного интеграционного сотрудничества государств – членов ЕАЭС для защиты прав потребителей в условиях цифровой трансформации. В результате проведенного исследования представлены общие действующие и разрабатываемые механизмы обеспечения и защиты прав потребителей в ЕАЭС, а также представлены предложения, направленные на дальнейшее развитие политики ЕАЭС в рассматриваемой сфере.

Ключевые слова: право, цифровые технологии, права потребителей, международные отношения, электронная торговля, евразийская интеграция, ЕАЭС

CONSUMER PROTECTION IN THE CONTEXT OF THE EAEU DIGITAL TRANSFORMATION

Abstract. The study presents the basics and prerequisites for the formation of eurasian consumer law, as well as mechanisms for ensuring and protecting consumer rights of citizens of the EAEU member states in the context of digital transformation of economic processes. The object of this study was the main mechanisms of consumer protection enshrined in the legislation of the EAEU member states. The purpose of the study is to determine the directions for further development of international integration cooperation of the EAEU member states to protect consumer rights in the context of digital transformation. As a result of the conducted research, the general existing and developing mechanisms for ensuring and consumer protecting are presented, as well as proposals aimed at further development of the EAEU policy in this area are presented.

Keywords: law, digital technologies, consumer rights, international relations, electronic commerce, eurasian integration, EAEU

Введение. Интеграционное объединение Евразийский экономический союз (далее также – ЕАЭС, Союз) образован независимыми государствами на основе международного права. Как отмечают исследователи, целью создания ЕАЭС, как субъекта региональной экономической интеграции, является достижение синергического эффекта, за счет повышения уровня социально-экономического развития и конкурентоспособности национальных экономик его участников [1, 8].

Международная экономическая интеграция, как процесс взаимодействия государств в рамках трансграничного и безбарьерного перемещения товаров и услуг, подразумевает постепенное экономическое сближение в рамках общего (единого) рынка потребительской продукции и услуг, основанное на гармонизации национального законодательства и установлении единого или сходного регулирования в отдельных сферах.

Население государств – членов ЕАЭС (далее – государства-члены) составляет 183 млн человек, каждый из которых является потенциальным потребителем [18]. При этом потребительские расходы в странах ЕАЭС составляют более половины национальной структуры использования валового внутреннего продукта.

Для эффективного развития ЕАЭС особого внимания заслуживают вопросы защита экономических интересов граждан, как потребителей, от рисков, которые многократно увеличиваются при снятии административных барьеров в условиях формирования единого евразийского рынка товаров и услуг [17].

С принятием 29 мая 2014 года Договора о Евразийском экономическом союзе от (далее – Договор о ЕАЭС), на уровень международной интеграции было передано около 140 властных полномочий [4].

Договором о ЕАЭС закреплены международные гарантии правовой защиты граждан, как потребителей, на территории всего Союза [6].

Одновременно, практическая работа по определению и внедрению процедур и механизмов защиты потребительских прав граждан, остаются в компетенции

государств-членов, которые взаимодействуют на пространстве ЕАЭС в формате согласованной политики в данной сфере.

Защита прав потребителей, как одно из интеграционных направлений международного сотрудничества, осуществляется в рамках компетенции Союза и основывается на рекомендательных актах, принимаемых Евразийской экономической комиссий (далее также – Комиссия).

Основная часть. Новые экономические реальности характеризуются с одной стороны, развитием цифровизации, стремительным распространением товаров и услуг дистанционным способом через электронные каналы связи, с другой – пересмотром системы мер государственного контроля в сторону минимизации административной нагрузки на бизнес. Указанная ситуация увеличивает вероятность возникновения новых вызовов для обеспечения потребительских прав и интересов граждан на едином рынке ЕАЭС.

В ЕАЭС предприняты попытки формирования единого правового поля в сфере электронной торговли. В частности, решением Евразийского межправительственного совета № 10, принятым 19 ноября 2021 г. был утвержден План мероприятий, которым предусматривается совершенствование механизмов регулирования электронной торговли товарами и подготовку международного соглашения по данному вопросу, в том числе с проработкой принципов защиты прав и интересов участников электронной торговли [11], которые должны выстраиваться в контексте общей работы и уже принятых и реализуемых решений по данному направлению.

Договор о ЕАЭС содержит основные принципы и гарантии защиты потребительских прав граждан.

При этом данное право не привязано к гражданству лица, являющегося потребителем.

Граждане и все проживающие на территориях государств-членов лица пользуются равными возможностями в области защиты прав потребителей и имеют право обращаться в компетентные органы и организации, в том числе в судебные инстанции для защиты своих прав.

Государства-члены в рамках ЕАЭС стремятся к формированию равных условий для потребителей в целях защиты их интересов во взаимоотношениях с бизнесом.

При этом, как показывает практика, положения, связанные с защитой прав потребителей, предусмотренные Договором о ЕАЭС и реализуемые посредством принятия актов, носящих для государств-членов рекомендательный характер, не позволяют обеспечить формирование в ЕАЭС равных условий для граждан государств-членов по защите их интересов от недобросовестной деятельности хозяйствующих субъектов.

Это связано с тем, что в каждом государстве-члене Союза сформирована самостоятельная нормативная правовая база, имеющая достаточно существенные различия, которые увеличиваются с каждым годом. В виду этого, в государствах-членах созданы различные механизмы и функционируют неравнозначные как по полномочиям, так и по сферам компетенции институты защиты права потребителей.

В законодательстве государств-членов установлены разные сроки процессуальных действий, связанных с защитой прав потребителей, различны подходы к осуществлению расчетов между участниками потребительских правоотношений. В законодательстве каждого государства-члена установлено право потребителя на качество товара, однако понятие «качество» различно, или не сформулировано.

Различны подходы к досудебному разрешению споров с участием потребителей. В Республике Казахстан, к примеру, активно внедряются альтернативные процедуры урегулирования споров. Так, споры с участием потребителей вправе рассматривать субъекты досудебного урегулирования потребительского спора, которыми являются арбитраж, медиатор [9].

Вопросы внедрения медиативных процедур, связанных с разрешением споров с участием потребителей, рассматриваются на уровне законодательных инициатив в Российской Федерации, однако конкретных решений по данному вопросу пока не выработано.

В других государствах – членах ЕАЭС (Армения, Беларусь, Кыргызстан) вопросы досудебного урегулирования путем внедрения альтернативных механизмов и процедур пока не находят активного развития.

Система защиты прав потребителей в государствах-членах сформирована за счет деятельности уполномоченных государственных органов, органов местного самоуправления, судов (государственная защита) и общественных потребительских объединений (общественная защита).

При этом объем полномочий и компетенция таких органов и организаций существенно различаются.

Зачастую, государственные органы, обладающие компетенцией в сфере защиты прав потребителей, являются не самостоятельным профильным ведомством (к примеру, в России – Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека), а комитетом, или агентством, созданным при координирующем министерстве (к примеру, в Казахстане – Комитет по защите прав потребителей Министерства торговли и интеграции, в Кыргызстане – Служба антимонопольного регулирования при Министерстве экономики и коммерции), либо являются одной из функций отраслевого министерства (к примеру, в Армении – Министерство экономики, в Беларуси – Министерство антимонопольного регулирования и торговли).

В современных условиях стремительно развиваются и создаются все новые формы торговли, основывающейся на различных цифровых технологиях и решениях.

Результаты изучения общественного мнения, проведенного Евразийской экономической комиссией в 2023 году, показали, что 95 % опрошенного населения стран ЕАЭС отдают предпочтение дистанционному заказу товаров в сети Интернет, 78 % граждан заказывают таким способом услуги [16].

По возрастным категориям самыми активными пользователями электронных каналов торговли являются лица в возрасте от 26 до 40 лет, которые составили 45 % всех опрошенных. Следующая категория – потребители в возрасте от 41 до 55 лет, которые занимают 37 % всех опрошенных [16].

85 % опрошенного населения стран ЕАЭС знают о том, что законодательство о защите прав потребителей действует в сфере электронной торговли, при этом 55 % покупателей, осознают или сталкивались с определенными рисками, влияющими на возможность защитить их потребительские права в сети Интернет. При этом треть опрошенных потребителей не знает, как защитить права в случае их нарушения интернет-магазином [16].

Только 6 % потребителей не опасаются совершать покупки в Интернете. Более чем 30 % опрошенных опасаются получить некачественный товар, в остальных случаях потребители опасаются, что товар не доставят в срок, либо видят иные риски, в основном, связанные с мошенничеством и обманом [16].

Опрос, проведенный ЕЭК, показывал, что 93 % потребителей обращают внимание на предлагаемые продавцом формы оплаты покупки в Интернете.

При этом 85 % опрошенных считают существенным условием установление платы за отказ от товара. При установлении условия о взимании магазином платы за возврат такого товара, потребители подтвердили, что будут более тщательно подходить к выбору, прежде чем сделать заказ [16].

Совершая дистанционную покупку посредством цифровых технологий, только 65 % потребителей уточняют у продавца конечную стоимость товара, при оплате за него в рассрочку [16].

Вместе с тем 12 % опрошенных даже не подозревают о том, что конечная стоимость товара, приобретенного в рассрочку может отличаться от начальной цены (при оплате товара сразу полностью), предложенной на сайте продавца [16].

Как показало проведенное исследование, электронная торговля развивается стремительными темпами. При этом, как на уровне национального законодательства государств-членов, так и на уровне права ЕАЭС, пока не приняты достаточные регуляторные нормы и процедуры, способствующие формированию правил взаимодействия и обеспечения интересов всех участников электронной торговли [17].

Ключевой вызов для регуляторов в условиях цифровой трансформации розничной торговли заключается в потенциальной ограниченности возможностей по применению норм действующего законодательства, направленного на защиту прав потребителей, к существующим рыночным отношениям, носящим трансграничный характер.

Если потребитель и хозяйствующий субъект, являются резидентами разных государств-членов, а сделка совершена в Интернете (т. е. нет так называемого «заземления», а именно – привязки к территории государства, где фактически заключено соглашение), в таком случае объем прав потребителей и механизмы их защиты зависят от определения правовых норм, применимых к таким правоотношениям (право страны потребителя или право страны предпринимателя).

При этом, как указано ранее, правовые нормы государств-членов, действующие в данной сфере, имеют определенные различия, что не дает возможности обеспечить равные условия для защиты потребительских прав граждан на пространстве Союза.

Данная ситуация создает объективные затруднения для реализации гражданских прав в сфере электронной торговли, а также затруднения в выстраивании взаимоотношений между субъектами предпринимательской деятельности и потребителями.

Для защиты потребителей в электронной торговле Евразийской экономической комиссией были разработаны основные подходы, закрепленные соответствующей рекомендацией для стран Союза (см. рекомендация Коллегии ЕЭК от 11 мая 2023 г. № 10) [12].

Основная задача документа – в условиях отсутствия единого правового поля Союза, которое бы устанавливало правила взаимодействия потребителя и бизнеса в электронной торговле, выработать общие подходы, которые позволят обеспечить защиту прав граждан и учесть интересы добросовестного бизнеса.

В рекомендации среди прочего содержится посыл к закреплению обязанности электронной торговой площадки и продавца, реализующего товары и услуги в Интернете соблюдать права потребителя и установления ответственности за нарушение таких прав [12].

В контексте резонансного случая, связанного с незаконным предоставлением потребителям экскурсионных услуг по подземным коллекторам, произошедшего в августе 2023 г. в Москве, положения рекомендации ЕЭК особенно актуальны в рамках формирования правового поля, связанного с регулированием деятельности информационных агрегаторов, в том числе, предоставляющих сведения об организации туристических услуг и маршрутов повышенной опасности.

В условиях недостаточности регулирования сферы электронной торговли, добросовестность, корпоративная ответственность и саморегулирование бизнеса выходят на первый план.

Евразийской экономической комиссией сделаны существенные попытки оказать поддержку работе, проводимой на уровне государств-членов, связанной с развитием институтов саморегулирования и внедрением принципов добросовестной деловой практики. Принят ряд рекомендаций по данному вопросу. Положения некоторых рекомендаций Комиссии успешно имплементируются в нормы национального права.

Так, в соответствии с положениями рекомендации Коллегии Комиссии от 12 января 2021 г. № 1 «О принципах и критериях добросовестной деловой практики в отношении потребителей в сфере розничной торговли товарами» перечень недопустимых условий договора с потребителем включен в Закон Российской Федерации «О защите прав потребителей» (изменения внесены Федеральным законом от 1 мая 2022 г. № 135-ФЗ).

В Республике Беларусь положения данной рекомендации ЕЭК были приняты судом по иску Регионального общества защиты потребителей в качестве обоснования требований истца о защите прав потребителей (Решение Суда Ивьевского района Гродненской области от 16 сентября 2022 г. к частному торговому унитарному предприятия «З» о признании действий противоправными и прекращении этих действий).

Основой для дальнейшего развития отраслевого взаимодействия стран Союза в период непростой экономической ситуации стала принятая в 2022 г. Евразийским межправительственным советом Программа совместных действий государств – членов ЕАЭС в сфере защиты прав потребителей [19] (далее – Программа).

Реализация заложенных программой мер и механизмов должна содействовать постепенному формированию на пространстве Союза единой системы обеспечения потребительских прав граждан.

Между тем, основными проблемными вопросами, разрешение которых в рамках действующего права Союза невозможно являются:

– для граждан: проблематичность определения права, применимого в случаях споров, возникающих между потребителем и продавцом в условиях трансграничной сделки;

– для бизнеса: отсутствует возможность обеспечить равные условия ведения предпринимательской деятельности в виду различий в национальном правовом поле стран Союза;

– для государственных органов: в условиях трансграничной торговли отсутствуют механизмы принятия мер административного воздействия к нарушителям.

Стоит отметить, что реализуемые в данной сфере решения являются частью Стратегических направлений развития евразийской экономической интеграции до 2025 г. (далее – Стратегия–2025) [10].

Стратегия-2025 содержит конкретные мероприятия, направленные на дальнейшее развитие интеграции государств-членов до 2025 г., и предусматривает реализацию концептуального преобразования отраслевых направлений совместной политики государств-членов.

Вместе с тем Стратегия-2025 была сформирована в иных экономических внешнеполитических условиях, в связи с чем, не может в должной степени обеспечить эффективное противостояние новым вызовам и устойчивость интеграционного объединения в современный период.

Проведенный анализ текущего состояния дел показывает, недостаточность существующего механизма обеспечения потребительских прав граждан, основанного только лишь на реализации норм национального права для создания равных условий правовой защиты граждан на территории ЕАЭС.

Современный период развития Союза приходится на экономически сложный период. Ввиду глубокой взаимосвязанности экономик государств-членов, введенные ограничительные меры, безусловно отражаются на развитии Союза.

Однако по мнению многих российских ученых, при наличии прочных социально-экономических связей между участниками интеграции, кризисы в экономике могут явиться эффективными катализаторами для упрочения и развития интеграционных процессов [3].

При разработке сценариев дальнейшего развития ЕАЭС в контексте сферы зашиты прав потребителей, должны быть учтены проблемные аспекты, выявленные за предыдущий период совместного развития государств-членов.

Принципиальными направлениями в деятельности ЕАЭС, способствующими эффективной реализации задач по защите прав потребителей в современных

условиях могут явиться дальнейшее поступательное расширение права ЕАЭС и формирование международной евразийской системы защиты прав потребителей, основанной на национальных институтах и единых (общих) международных правилах взаимоотношений участников потребительского рынка.

В этой работе важным будет учитывать возможность разработки и применения международных механизмов разрешения трансграничных споров с участием потребителей.

Для практического разрешения указанных направлений важным также является укрепление правомочного положения Евразийской экономической комиссии в части обеспечения ее соответствия основному содержанию процесса управления и повышение ответственности за подготовку и принятие решений в рамках установленных полномочий.

Заключение. Современные условия, в которых страны ЕАЭС осуществляют международное взаимодействие по направлению защиты прав потребителей сопряжены с отсутствием единых наднациональных норм и правил, обеспечивающих равные условиях для граждан стран Союза по реализации их прав, как потребителей. Разрыв между нормами национального права, посредством которых обеспечивается защита потребительских прав граждан постепенно увеличивается.

Особенно остро эти вопросы проявляются в условиях электронной торговли. Основная проблематика заключается в потенциальной ограниченности возможностей по применению действующего национального регулирования в сфере защиты прав потребителей к существующим рыночным отношениям, носящим трансграничный характер.

Указанное создает объективные затруднения в выстраивании взаимоотношений между субъектами предпринимательской деятельности и потребителями.

Решением обозначенной проблематики станет формирование наднационального (единого) правового поля в сфере защиты прав потребителей в Союзе с передачей Комиссии полномочий по утверждению соответствующих документов, направленных на выработку:

– единых норм и правил защиты прав потребителей при дистанционном способе их продажи с акцентом на трансграничные формы торговли, учитывая необходимость выстраивания международного сотрудничества национальных компетентных органов для разрешения споров в подобных случаях;

– правил и механизмов разрешения трансграничных споров с участием потребителей на наднациональном уровне.

Дальнейшее расширение экономического взаимодействия стран в рамках ЕАЭС, имеет важное значение в контексте противостояния углубляющимся кризисным тенденциям в мировой экономике. Углубление интеграции по всем ключевым направления развития Союза также явилось основной темой послания к главам государств-членов ЕАЭС, озвученного Президентом Российской Федерации В. В. Путиным, приуроченного году председательства Российской Федерации в Союзе в 2023 году [15].

Таким образом, на основании обозначаемых государствами-членами ожиданий от развития евразийской экономической интеграции, вполне вероятно

предполагать оптимизацию существующей модели, при которой страны Союза будут определять новые сферы и углублять существующие направления международного взаимодействия, в которых важное место займет работа по формированию единой нормативной правовой базы для защиты прав потребителей.

Список литературы

1. Бекяшев К. А. ЕАЭС: международная (межгосударственная) организация или международное (межгосударственное) интеграционное объединение? // Евразийский юридический журнал. 2014. № 11. С. 14–16.

2. Вестник ученых-международников IR SCIENTISTS' HERALD // Научный электронный журнал. 2022. № 1.

3. Винокуров Е. Ю., Цукарев Т. В. Что нужно сделать для достижения максимального положительного эффекта ЕАЭС? Какова «повестка дня» на ближайшие годы? // Евразийская экономическая интеграция. 2015. № 4(29). С. 7–21.

4. Гаевский И. В. Проблемы и приоритетные задачи дальнейшего интеграционного развития стран Евразийского экономического союза// Международное правосудие и укрепление интеграционных процессов: Междунар. конф. (18–19 окт. 2018 г., г. Минск): сб. материалов / отв. ред. А. С. Бугаева, К. В. Энтин. Минск: Четыре четверти, 2018. С. 255–258.

5. Декларация о дальнейшем развитии интеграционных процессов в рамках Евразийского экономического союза Евразийская экономическая комиссия. URL: https://docs.eaeunion.org/docs/ru-ru/01420213/ms_10122018

6. Договор о Евразийском экономическом союзе. URL: https://docs.eaeunion.org/docs/ru-ru/0003610/itia_05062014

7. Евразийская экономическая интеграция. Теория и практика: учебное пособие. Москва: Проспект, 2023. 648 с.

8. Мясникович М. В., Ковалев В. С. Миссия ЕАЭС-2025: региональный центр экономического развития и опора Большой Евразии // Наука и инновации. 2021. 1(215). С. 4–11.

9. О защите прав потребителей: Закон Республики Казахстан от 4 мая 2010 г. № 274-IV. URL: https://adilet.zan.kz/rus/wniobzor

10. О Стратегических направлениях развития евразийской экономической интеграции до 2025 года: Решение Высшего Евразийского экономического совета от 11 декабря 2020 г. № 12. URL: https://docs.eaeunion.org/ docs/ru-ru/01428320/err_12012021_12

11. О плане мероприятий («дорожной карте») по созданию благоприятных условий для развития электронной торговли в рамках Евразийского экономического союза: Решение Евразийского межправительственного совета от 19.11.2021 № 10. URL: https://docs.eaeunion.org/docs/ru-ru/01430580/err_22112021_10

12. Об общих подходах к защите прав потребителей в электронной торговле: Рекомендация Коллегии Евразийской экономической комиссии от 11.05.2023 № 10 Правовой портал Евразийского экономического союза. URL: https://docs.eaeunion.org/docs/ru-ru/01439691/err_15052023_10

13. Об Основных направлениях экономического развития Евразийского экономического союза: Решение Высшего Евразийского экономического совета от 16 октября 2015 г. № 28. URL: https://docs.eaeunion.org/docs/ru-ru/0148763/scd_19102015_28

14. Обзор ключевых мер и решений. Евразийская экономическая комиссия. URL: https://eec.eaeunion.org/increasing_stability_economies/obzor-klyuchevykh-mer.php

15. Обращение Президента Российской Федерации В. В. Путина к главам государств – членов Евразийского экономического союза. URL: http://www.kremlin.ru/events/president/news/70380

16. Общественное мнение населения стран ЕАЭС о правах потребителей в электронной торговле. Евразийская экономическая комиссия. Официальный сайт. URL: https://potrebitel.eaeunion.org/ru-ru/Pages/Obschestvennoe-mnenie-naseleniya-stran-EAES-o-pravah-potrebitelej-v-elektronnoj-torgovle.aspx

17. Осауленко Л. Н. ЕАЭС: Права потребителей в электронной торговле// Стандарты и качество. 2023. № 1. С. 128–130.

18. Потребитель – центр евразийской интеграции. Как работает Евразийская экономическая комиссия в сфере защиты прав потребителей. URL: https://potrebitel.eaeunion.org/ru-ru/Pages/eec.aspx

19. Распоряжение ЕМПС от 21.06.2022 г. № 12 «О программе совместных действий государств-членов ЕАЭС в сфере защиты прав потребителей». URL: https://docs.eaeunion.org/docs/ru-ru/01434129/err_22062022_12

М. Ю. Осипов,
кандидат юридических наук,
Международная полицейская академия ВПА

К ВОПРОСУ ОБ ОСОБЕННОСТЯХ СОЗДАНИЯ И ИСПОЛЬЗОВАНИЯ АВТОМАТИЗИРОВАННЫХ КОНСТРУКТОРОВ В ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Статья посвящена особенностям создания и использования автоматизированных конструкторов как вида информационных технологий в юридической деятельности. Цель исследования состоит в том, чтобы рассмотреть особенности создания и использования автоматизированных конструкторов в юридической деятельности. Предметом исследования, результаты которого изложены в настоящей статье, выступают особенности и закономерности создания и использования автоматизированных конструкторов в юридической деятельности. К числу методов исследования можно отнести: анализ, синтез, индукцию, дедукцию, абстрагирование, обобщение, моделирование. В ходе исследования было установлено, что под автоматизированными конструкторами в юридической деятельности следует понимать специализированные программные комплексы, при помощи которых можно составлять документы юридического характера,

проводить различного рода юридические экспертизы, осуществлять юридическое консультирование. При этом в основе автоматизированных конструкторов должен лежать определенный алгоритм осуществления юридической деятельности. Также в статье на конкретных примерах показываются особенности создания автоматизированных конструкторов, могущих быть использованными при осуществлении юридической деятельности, и раскрывается технология создания подобного рода конструкторов.

Ключевые слова: право, цифровые технологии, автоматизированные конструкторы, программы, алгоритмы, правовые документы, юридические консультации, юридические экспертизы, юридическое консультирование, юридическая наука

THE QUESTION OF THE FEATURES OF CREATION AND USE OF AUTOMATED DESIGNERS IN LEGAL ACTIVITY

Abstract. The article is devoted to the features of the creation and use of automated constructors as a type of information technology in legal activities. The purpose of the study is to consider the features of the creation and use of automated constructors in legal activities. The subject of the study, the results of which are presented in this article, are the features and patterns of creation and use of automated constructors in legal activities. The research methods include: analysis, synthesis, induction, deduction, abstraction, generalization, modeling. In the course of the study, it was found that automated constructors in legal activity should be understood as specialized software systems that can be used to draw up legal documents, conduct various kinds of legal expertise, and provide legal advice. At the same time, automated constructors should be based on a certain algorithm for the implementation of legal activities. Also in the article, specific examples show the features of creating automated constructors that can be used in the implementation of legal activities, and reveals the technology for creating such constructors.

Keywords: law, digital technologies, automated constructors, programs, algorithms, legal documents, legal advice, legal expertise, legal consulting, legal science

Введение. Одной из актуальных проблем, стоящих перед современной юридической наукой, является проблема создания и использования автоматизированных конструкторов в юридической деятельности. Эта проблема является достаточно новой для отечественной и мировой юридической науке, поэтому работы, затрагивающие данную проблему в России и в мире появились достаточно недавно [1–6; 11–13; 15–17; 20; 21; 23; 24] и другие. В указанных работах рассматриваются различные аспекты применения автоматизации в юридической деятельности. Однако вопросам создания автоматизированных конструкторов в сфере юридической деятельности, т. е. специализированным программным комплексам, при помощи которых юрист может эффективно осуществлять свою деятельность уделяется недостаточное внимание как в отечественной, так и в зарубежной

юридической литературе. В связи с этим возникает необходимость проведения специального исследования, посвященного созданию и использованию автоматизированных конструкторов в юридической деятельности. При этом предметом исследования в настоящей статье выступают особенности и закономерности создания и использования автоматизированных конструкторов в юридической деятельности. Цель исследования состоит в том, чтобы рассмотреть особенности создания и использования автоматизированных конструкторов в юридической деятельности. К числу методов исследования, которые были использованы входе исследования, результаты которого изложены в настоящей статье можно отнести следующие: анализ, синтез, индукцию, дедукцию, абстрагирование, обобщение, моделирование.

При этом методы исследования, такие как анализ, синтез, индукция и дедукция, использовались для формулирования основных понятий, связанных с темой данного исследования; метод же моделирования использовался для создания и описания моделей работы автоматизированных конструкторов в юридической деятельности.

К числу же основных задач исследования, результаты которого были изложены в настоящей статье можно отнести следующие:

1) определение понятия «автоматизированный конструктор в юридической деятельности»;

2) осуществление классификации автоматизированных конструкторов в юридической деятельности;

3) описание алгоритмов создания и работы автоматизированных конструкторов в юридической деятельности;

4) определение факторов, влияющих на создание и работу автоматизированных конструкторов в юридической деятельности;

5) разработка мероприятий по повышению эффективности внедрения автоматизированных конструкторов в юридической деятельности.

Решение указанных задач составило отдельный этап исследования.

Основная часть. 1. Понятие и классификация автоматизированных конструкторов в юридической деятельности. Как уже отмечалось ранее на первом этапе исследования решалась задача, связанная с определением понятия «автоматизированный конструктор в юридической деятельности». Необходимо отметить, что в юридической науке, несмотря на многочисленные статьи, посвященные вопросам автоматизации юридической деятельности определение понятия «автоматизированный конструктор в юридической деятельности отсутствует.

Попробуем вывести его самостоятельно, проанализировав основные признаки понятия «автоматизированный конструктор в юридической деятельности».

При этом как известно в основных признаках понятия концентрируются те или иные закономерности того или иного явления, которое отражает данное понятие [18; 19].

Исходя из указанных методологических установок, можно выделить следующие основные признаки понятия «автоматизированный конструктор в юридической деятельности».

Во-первых «автоматизированный конструктор в юридической деятельности представляет собой определенную программу для ЭВМ или комплекс программ, которые предназначены для достижения какой – либо цели.

Во-вторых, автоматизированный конструктор в юридической деятельности представляет собой не просто программу для ЭВМ, но специализированную программу, которая призвана решать определенные задачи юридической деятельности. К числу таких задач можно отнести, в частности, следующие задачи:

– задачи, связанные с составлением юридических документов;

– задачи, связанные с проведением различного рода юридических экспертиз;

– задачи, связанные с осуществлением юридического консультирования.

В-третьих, в основе любого автоматизированного конструктора юридической деятельности лежит определенный алгоритм осуществления юридической деятельности.

Таким образом на основании всего вышеизложенного можно определить автоматизированный конструктор в юридической деятельности как специализированный программный комплекс, при помощи которого можно составлять документы юридического характера, проводить различного рода юридические экспертизы, осуществлять юридическое консультирование, в основе которого заложен определенный алгоритм осуществления юридической деятельности.

Анализ данного понятия позволяет выделить следующие критерии классификации автоматизированных конструкторов в юридической деятельности.

В зависимости от типа задач, которые могут быть решены при помощи автоматизированного конструктора в юридической деятельности, можно выделить следующие виды конструкторов:

– автоматизированные конструкторы составления юридических документов (примером таких конструкторов могут выступать «конструкторы договоров [7], конструкторы учетной политики» и т. д.);

– автоматизированные конструкторы проведения различного рода юридических экспертиз (примером таких конструкторов может быть «Конструктор НПА», «Правовая экспертиза», «Антикоррупционная экспертиза», «Мониторинг», «Иск», «Межведомственные соглашения МВД России» [5];

– автоматизированные конструкторы, позволяющие осуществлять юридическое консультирование (примером такого конструктора может служить разработанный автором данной статьи конструктор «Оценка перспектив судебного разбирательства, описание работы которого приведено ниже.

В зависимости от способа распространения конструктора можно выделить а) свободно распространяемые конструкторы; б) проприетарные конструкторы, распространяемые за отдельную плату среди неограниченного числа потенциальных пользователей); в) проприетарные конструкторы, распространяемые за отдельную плату среди ограниченного числа пользователей; в) проприетарные конструкторы закрытого типа, которые используются разработчиками для собственных нужд.

Таковы основные критерии классификации автоматизированных конструкторов в юридической деятельности.

Следующим этапом исследования является описание алгоритмов создания и работы автоматизированных конструкторов в юридической деятельности.

2. Описание алгоритмов создания и работы автоматизированных конструкторов в юридической деятельности. Как уже было установлено ранее любой автоматизированный конструктор в юридической деятельности представляет собой определенный специализированный программный комплекс, который функционирует по определенному алгоритму. При этом юридическая деятельность также осуществляется по определенному алгоритму [8–9]. Но поскольку юридическая деятельность осуществляется по определенному алгоритму, следовательно становиться возможным создание программы для ЭВМ в форме автоматизированного конструктора юридической деятельности, при помощи которого можно решать те или иные задачи, на решение которых направлена та или иная юридическая деятельность.

Что же эти алгоритмы собой представляют и как их можно использовать для создания и обеспечения эффективной работы автоматизированных конструкторов в юридической деятельности?

Для того, чтобы ответить на данный вопрос, необходимо вспомнить о том, что в основе любой юридической деятельности лежит определенный диалог в виде вопросов и ответов на них [14]. Следовательно, теоретически можно построить направленный граф, вершинами которого будут вопросы и ответы на них, а ребрами переходы от ответов к вопросам, и от вопросов к ответам, которые связаны с решением тех или иных задач, связанных с юридической деятельностью [22].

Каким же образом мы можем построить данный граф.

Для этого вначале рассмотрим следующую таблицу.

Таблица 1

Описание графа построения алгоритма юридической деятельности

Вопрос	**Ответ**	**Результат**	**Переход**
Вопрос 1	Ответ 1	Результат 1.1	Вопрос 2.1.
	Ответ 2	Результат 1.2	Вопрос 2.2.
	Ответ 3	Результат 1.3	Вопрос 2.3
Вопрос 2.1	Ответ 2.1.1	Результат 2.1.1	Вопрос 3.1.m
	Ответ 2.1.2	Результат 2.1.2	Вопрос 3.1.m
	Ответ 2.1.3	Результат 2.1.3	Вопрос 3.1.m
Вопрос 2.2	Ответ 2.2.1	Результат 2.2.1	Вопрос 3.2.m
	Ответ 2.2.2.	Результат 2.2.2	Вопрос 3.2.m
	Ответ 2.2.3	Результат 2.2.3	Вопрос 3.2.m
Вопрос 2.3	Ответ 2.3.1	Результат 2.3.1	Вопрос 3.3.m
	Ответ 2.3.2	Результат 2.3.2	Вопрос 3.3.m
	Ответ 2.3.3	Результат 2.3.3	Вопрос 3.3.m
	Ответ 2.3.4	Результат 2.3.4	Вопрос 3.3.m
……..	…….	……	…….
Вопрос JK	Ответ JmKn	Результат JmKn	Завершение диалога и отправка результатов его по электронной почте

Таким образом направленный граф вопросов и ответов при построении автоматизированного конструктора юридической деятельности будет выглядеть следующим образом:

Вопросn– Ответ nm – Результат nm –Вопросn+1m – Ответn+1m– Результатn+1m -…….. Вопрос JK – Ответ JmKn– Результат JmKn – Завершение диалога и отправка результатов его по электронной почте

Теперь покажем, как это работает на практике на примере разработанного автором данной статьи автоматизированного конструктора «Оценка перспектив судебного разбирательства»

Для этого представим все вопросы и варианты ответа, используемые в данном автоматизированном конструкторе, а также переходы в виде следующей таблицы.

Таблица 2

Описание графа построения автоматизированного конструктора «Оценка перспектив судебного разбирательства»

Запрос персональных данных пользователя ФИО и адреса электронной почты				
Ознакомление пользователя с правилами обработки персональных данных				
Ввод соответствующих персональных данных в соответствующую форму				
№ вопроса	**Вопрос**	**Ответ**	**Результат**	**Переход**
Вопрос 1	У нас предстоит суд. Мы бы хотели оценить перспективы судебного разбирательства. Не могли ли бы Вы помочь нам?	Мы готовы помочь Вам. Для этого необходимо Вам ответить на ряд вопросов. Если Вы готовы, тогда нажмите продолжить	Мы готовы помочь Вам. Для этого необходимо Вам ответить на ряд вопросов. Если Вы готовы, тогда нажмите продолжить	Вопрос 2
Вопрос 2	Вам ясно из каких правоотношений возник спор	Да ясно	Нам ясно из каких правоотношений возник спор	Вопрос 3
		Нет, не ясно	Нам не ясно из каких правоотношений возник спор	В таком случае Вам надо определиться из каких правоотношений у Вас возник спор. Как только Вы определитесь нажмите продолжить Вопрос 2

Вопрос 3	Какую роль Вы будете играть в данном споре: истца или ответчика?	Истца	Истца	Вопрос 4
		Ответчика	Ответчика	Вопрос 8
Вопрос 4	Вам ясно, какие Ваши права были нарушены?	Да, ясно	Да, ясно	Вопрос 5
		Нет, не ясно	Нет, не ясно	Вам необходимо определится с тем, какие Ваши субъективные права были нарушены. Как только Вы определитесь с этим нажмите продолжить Вопрос 4
Вопрос 5	Располагаете ли Вы доказательствами того, что Ваши права нарушены?	Да располагаем	Да располагаем	Вопрос 6
		Нет, не располагаем	Нет, не располагаем	В таком случае, прежде чем предъявлять иск в суд, Вам надо убедиться в том, что Вы располагаете необходимыми доказательствами нарушения Ваших прав. В противном случае суд откажет Вам в удовлетворении заявленных требований Продолжить. Вопрос 5
Вопрос 6	Не истек ли срок исковой давности по Вашим требованиям?	Нет, не истек	Нет, не истек	Вопрос 7
		Да, истек	Да, истек	В таком случае существует очень большой риск что в удовлетворении Ваших требований будет отказано в суде, поскольку истек срок исковой давности. Извините, больше ничем помочь не могу Финиш

Вопрос 7	Не имеется ли каких-либо иных препятствий к удовлетворению заявленных требований?	Да имеются	Да, имеются	В таком случае увы скорее всего суд откажет Вам в удовлетворении заявленных требований Извините, больше ничем помочь не могу Финиш
		Нет, не имеется	Нет, не имеется	Ну что же если все что Вы мне сообщили это правда, у Вас хорошие перспективы выиграть дело в суде Финиш
Вопрос 8	Вы нарушали права истца своими действиями или бездействием?	Да, нарушали	Да, нарушали	В таком случае скорее всего суд встанет на сторону истца. Вопрос 9
		Нет, не нарушали	Нет, не нарушали	Если Вы не нарушали права истца, и Вы мне сказали правду, то скорее всего суд откажет в удовлетворении заявленных требований истца. Финиш
Вопрос 9	Но как Вам кажется истец располагает необходимыми доказательствами нарушения Вами его прав?	Да, располагает	Да, располагает	В таком случае, если не истек срок исковой давности по делу суд скорее всего удовлетворит требования истца, уж извините. Финиш
		Нет, не располагает	Нет, не располагает	В таком случае скорее всего суд откажет в удовлетворении заявленных требований истца Финиш
Финиш				
Отправка результатов выполнения конструктора на электронную почту пользователя				

Аналогичным образом могут и должны строиться графы построения других автоматизированных конструкторов для юридической деятельности.

Наиболее удобной программой для построения подобного рода конструкторов выступает отечественная программа Ispring Talk Master9 из комплекса Ispring Suite 9.

Анализ данного графа показывает, что в основе любого автоматизированного конструктора, используемого в юридической деятельности, лежит следующая концепция построения алгоритмов работы автоматизированных конструкторов в сфере юридической деятельности. Вопрос-ответ на вопрос – действие в зависимости от ответа на вопрос – переход к следующему вопросу. При этом вопросы и ответы на них должны иметь юридическое значение.

Таковы основные особенности алгоритмов создания и работы автоматизированных конструкторов в юридической деятельности.

Следующим этапом исследования является описание факторов, влияющих на создание и работу автоматизированных конструкторов в юридической деятельности.

3. Описание факторов, влияющих на создание и работу автоматизированных конструкторов в юридической деятельности. Как уже отмечалось ранее на процесс создания и работы автоматизированных конструкторов в юридической деятельности влияет множество факторов, под которыми следует понимать конкретные явления социальной действительности, которые непосредственно (прямые факторы) или опосредованно (косвенные факторы) позитивно (позитивные факторы) либо негативно (негативные факторы) влияют на процесс создания и работы автоматизированных конструкторов в юридической деятельности.

Основными критериями классификации указанных факторов выступают следующие.

В зависимости от процесса, на который они влияют можно выделить: а) факторы влияющие на процесс разработки автоматизированных конструкторов в юридической деятельности; б) факторы влияющие на процесс внедрения автоматизированных конструкторов в юридической деятельности; в) факторы, влияющие на работу автоматизированных конструкторов в юридической деятельности.

В зависимости от механизма влияния все факторы, влияющие на процесс создания и работы автоматизированных конструкторов в юридической деятельности, можно подразделить на: а) прямые факторы – факторы, которые непосредственно влияют на процесс создания и работы автоматизированных конструкторов в юридической деятельности; б) косвенные факторы – факторы, которые опосредованно (через другие факторы) влияют на процесс создания и работы автоматизированных конструкторов в юридической деятельности.

В зависимости от характера влияния все факторы, влияющие на процесс создания и работы автоматизированных конструкторов в юридической деятельности, можно подразделить на: а) позитивные факторы – факторы, которые способствуют созданию и работе разработки автоматизированных конструкторов в юридической деятельности; б) негативные факторы – факторы, которые препятствуют созданию и работе разработки автоматизированных конструкторов в юридической деятельности.

В зависимости от природы можно выделить «психологические, социальные, экономические, политические, правовые и иные факторы» [10].

Рассмотрим некоторые из этих факторов более подробно.

1. Степень понимания целей и задач юридической деятельности заинтересованными субъектами права. Данный фактор показывает, насколько заинтересованные субъекты права понимают правильно цели и задачи юридической деятельности. Если степень понимания целей и задач юридической деятельности достаточно низкая, то и построение автоматизированных конструкторов в юридической деятельности будет идти с трудом, поскольку если не ясны цели и задачи юридической деятельности, то очень трудно найти пути их решения.

2. Степень понимания путей решения целей и задач юридической деятельности заинтересованными субъектами права. Данный фактор показывает, насколько заинтересованные субъекты права понимают правильно пути решения целей и задач юридической деятельности. Если степень понимания путей решения целей и задач юридической деятельности достаточно низкая, то и построение автоматизированных конструкторов в юридической деятельности будет идти с трудом, поскольку если неясны пути решения целей и задач юридической деятельности, то, следовательно, также неясны возможности и пути автоматизации решения задач юридической деятельности.

3. Степень понимания возможностей и путей автоматизации решения задач юридической деятельности. Данный фактор показывает, насколько заинтересованные субъекты права понимают правильно возможности и пути автоматизации решения задач юридической деятельности. Если степень понимания возможных путей автоматизации решения задач юридической деятельности достаточно низкая, то и построение автоматизированных конструкторов в юридической деятельности будет идти с трудом, поскольку неясны возможные пути автоматизации решения задач юридической деятельности при помощи данных конструкторов.

4. Наличие необходимых ресурсов в достаточном количестве для осуществления процесса создания и работы автоматизированных конструкторов в юридической деятельности. Данный фактор показывает, насколько у заинтересованных субъектов права есть необходимые ресурсы (актуальные или потенциальные), которые необходимы для успешного создания и работы автоматизированных конструкторов в юридической деятельности. Если необходимых ресурсов нет, то и создание и работа автоматизированных конструкторов в юридической деятельности. будет невозможной или существенно затруднена при недостаточности ресурсов, поскольку для создания и эффективной работы автоматизированных конструкторов в юридической деятельности требуются необходимые ресурсы.

5. Умение заинтересованными субъектами права определять необходимые ресурсы в достаточном количестве для осуществления процесса создания и работы автоматизированных конструкторов в юридической деятельности. Данный фактор показывает, насколько заинтересованные субъекты права могут определить необходимые ресурсы (актуальные или потенциальные), которые необходимы для успешного создания и работы автоматизированных конструкторов в юридической деятельности. Если такого умения нет, то создание и работа автоматизированных конструкторов в юридической деятельности. будет невозможной или существенно затруднена поскольку заинтересованные субъекты права не могут определять

необходимые ресурсы в достаточном количестве для осуществления процесса создания и работы автоматизированных конструкторов в юридической деятельности.

6. Умение заинтересованными субъектами права осуществлять выбор необходимых автоматизированных конструкторов в юридической деятельности, а также предлагать их на рынок и оперативно реагировать на изменение рынка. Данный фактор показывает, насколько заинтересованные субъекты права могут осуществлять выбор необходимых автоматизированных конструкторов в юридической деятельности, а также предлагать их на рынок и оперативно реагировать на изменение рынка.

7. Иные факторы.

Следующим этапом исследования является описание разработанных автором данной статьи мероприятий повышению эффективности внедрения автоматизированных конструкторов в юридической деятельности

4. Описание мероприятий по повышению эффективности внедрения автоматизированных конструкторов в юридической деятельности. Под мероприятиями по повышению эффективности внедрения автоматизированных конструкторов в юридической деятельности следует понимать действия или систему действий, которые направлены на повышение эффективности внедрения автоматизированных конструкторов в юридической деятельности.

К числу таких мероприятий можно отнести следующие:

1. Мероприятия, направленные на осознание заинтересованными субъектами права целей и задач юридической деятельности;

2. Мероприятия, направленные на осознание заинтересованными субъектами права возможных путей решения целей и задач юридической деятельности.

3. Мероприятия, направленные на осознание заинтересованными субъектами права возможных путей автоматизации в области решения целей и задач юридической деятельности.

4. Мероприятия, направленные на осознание заинтересованными субъектами права возможных путей разработки автоматизированных конструкторов юридической деятельности.

5. Мероприятия, направленные формирование умений у заинтересованных субъектов права определять необходимые ресурсы в достаточном количестве для осуществления процесса создания и работы автоматизированных конструкторов в юридической деятельности, а также умений определять осуществлять выбор необходимых автоматизированных конструкторов в юридической деятельности, а также предлагать их на рынок и оперативно реагировать на изменение рынка.

Представляется, что данные знания, умения и навыки могут быть сформированы в ходе курсов повышения квалификации, а также в ходе освоения соответствующих магистерских программ в области информационных технологий в сфере юридической деятельности.

Мы рассмотрели основные вопросы, входящие в предмет данного исследования.

Заключение. В ходе данного исследования было установлено следующее.

1. Автоматизированный конструктор в юридической деятельности – это специализированный программный комплекс, при помощи которого можно

составлять документы юридического характера, проводить различного рода юридические экспертизы, осуществлять юридическое консультирование, в основе которого заложен определенный алгоритм осуществления юридической деятельности.

2. В качестве критериев классификации автоматизированных конструкторов в юридической деятельности выступают: а) особенности целей и задач юридической деятельности; б) способ распространения конструктора.

3. В основе любого автоматизированного конструктора, используемого в юридической деятельности, лежит следующая концепция построения алгоритмов работы автоматизированных конструкторов в сфере юридической деятельности. Вопрос-ответ на вопрос – действие в зависимости от ответа на вопрос – переход к следующему вопросу. При этом вопросы и ответы на них должны иметь юридическое значение.

4. На процесс создания и работы автоматизированных конструкторов в юридической деятельности влияет множество факторов, под которыми следует понимать конкретные явления социальной действительности, которые непосредственно (прямые факторы) или опосредованно (косвенные факторы) позитивно (позитивные факторы) либо негативно (негативные факторы) влияют на процесс создания и работы автоматизированных конструкторов в юридической деятельности.

5. В качестве критериев классификации указанных факторов могут выступать: а) особенности процесса, на который они влияют; б) механизм влияния; в) характер влияния; в) природа фактора.

Также в статье были рассмотрены отдельные факторы и приведен перечень мероприятий, необходимый для повышения эффективности внедрения автоматизированных конструкторов в юридической деятельности.

Дальнейшее направление исследований автор склонен связывать с рассмотрением особенностей создания и использования автоматизированных конструкторов в отдельных сферах юридической деятельности.

Список литературы

1. Азаров М. С. Гачина А. А. Потенциал автоматизации практической деятельности юриста [Дневник] // Актуальные проблемы правоведения. 2022. Т. 66. № 2. С. 45–50.

2. Башков Д. С Legal Tech: автоматизация юридической деятельности («за» и «против») // Правовая коммуникация государства и общества: отечественный и зарубежный опыт: Сборник трудов международной научной конференции, Воронеж, 11–12 сентября 2020 года. Воронеж: Автономная некоммерческая организация по оказанию издательских и полиграфических услуг «НАУКА-ЮНИПРЕСС», 2020. С. 395–399.

3. Бшоян Л. Д. Автоматизация работы юриста: использование информационных технологий в юридической деятельности // Традиции и новации в системе современного российского права: Материалы XXI Международной конференции молодых ученых. В 3-х томах, Москва, 15–16 апреля 2022 г. М.: Московский

государственный юридический университет имени О. Е. Кутафина (МГЮА), 2022. Т. 3. С. 417–418.

4. Варламов В. А., Местников С. В. Проектирование приложения для автоматизации ведения учета договоров и документов в юридической деятельности // Современные информационные технологии, инновации и молодежь – «СИТИМ–2023»: Материалы Всероссийской студенческой научно–практической конференции с международным участием, Якутск, 27–29 марта 2023 г. Ульяновск: Зебра, 2023. С. 95–97.

5. Глебов Д. А, Кононов А. М Правовое регулирование и юридическое сопровождение деятельности МВД России в условиях цифровой трансформации правоохранительной сферы [Дневник] // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2022. Т. 64, № 4. С. 64–70.

6. Грязнов С. А. К вопросу об автоматизации и юридической деятельности // Юридическая наука в XXI веке: актуальные проблемы и перспективы их решений: Сборник научных статей по итогам работы круглого стола №2 со Всероссийским и международным участием, Шахты, 27–28 февраля 2022 года. Шахты: КОНВЕРТ, 2022. С. 177–178.

7. Джумагулов Д. Д. Конструктор договора с опциональными условиями. Свидетельство о государственной регистрации программы для ЭВМ № 2020615873.

8. Завгородний А. М., Шабалина Л. В., Шавкун Г. А. Алгоритм получения юридическими лицами исключительных прав на результаты интеллектуальной деятельности и распоряжение ими в Донецкой Народной Республике // Вести Автомобильно-дорожного института. 2022. № 2 (41). С. 63–70.

9. Комин А. В. Применение алгоритмов в юриспруденции // Вестник Южно-Уральского государственного университета. Серия: Право. 2023. Т. 23, № 2. С. 74–79.

10. Косых А. А Интеллектуальные аспекты идеи законопроекта // Труды Академии управления МВД России. 2022. № 4(60). С. 60–67.

11. Котов А. А. Автоматизация обработки юридических документов на примере правового сопровождения издательской деятельности: задачи и перспективные технологии // Экономика. Информатика. 2022. Т. 49, № 2. С. 394–-402.

12. Котов., А. А. Ронжин,А. Л. Моделирование процесса автоматизации создания, проверки и актуализации текста договоров // Известия Юго-Западного государственного университета. 2022. Т. 26, № 2. С. 87–105.

13. Круть Л. С. Legal Tech: друг или враг юриста? // Технологии XXI века в юриспруденции: Материалы Третьей международной научно–практической конференции, Екатеринбург, 21 мая 2021 года / ред. Д. В. Бахтеева Екатеринбург: Уральский государственный юридический университет, 2021. С. 306–312.

14. Кургаева О. Л. Особенности юридического дискурса и его дидактические параметры // Kant. 2018. №1 (26). С. 61–64.

15. Маркова, Т. Ю., Максимова Т. Ю. Трансформация профессиональных навыков в условиях цифровизации уголовного судопроизводства // Право и политика. 2023. № 6. С. 25–37.

16. Нестеров. А. В. Цифровая трансформация юридической деятельности и законодательства // Правовое государство: теория и практика. 2018. Т. 62, № 4–1. С. 43–53.

17. Чайковский Д. С. Системы автоматизации юридической деятельности // Информационные технологии в юридической науке и образовании. Сборник научных статей по материалам II Всероссийской научной конференции, Саратов, 27 апреля 2018 года. Саратов: Саратовская государственная юридическая академия, 2018. С. 59–65.

18. Alnaim M. M. Understanding the Traditional Saudi Built Environment: The Phenomenon of Dynamic Core Concept and Forms // World Journal of Engineering and Technology. 2022. Vol. 10, № 2. Pp. 292–321.

19. Borsotti V., Bjørn P. Humor and stereotypes in computing: An equity–focused approach to institutional accountability // Computer Supported Cooperative Work. 2022. Vol. 31, № 4. P. 771–803.

20. Dale. R Law and word order: NLP in legal tech // Natural Language Engineering. 2019. Vol. 25, № 1. Pp. 211–217.

21. Delgado., F., Barocas., S., Levy., K. An uncommon task: Participatory design in legal AI // Proceedings of the ACM on Human–Computer Interaction. 2022. Vol. 6. Pp. 1–23.

22. Koehler. M Jurisprudence Meets Physics // Frontiers in Physics. 2022. Vol. 10. Pp. 760–780.

23. Pasquale. F. A rule of persons, not machines: the limits of legal automation // Geo. Wash. L. Rev. 2019. Vol. 87. Pp. 1–16.

24. Zhamshid V., Nusratilloevich Y. A. Shahida. Azamat. K. Rise of the Machines: The Legal Implications of Robotics and Automation for the Digital Workforce // International Journal of Cyber Law. 2023. Vol. 1, № 4. Pp. 1–19.

Л. В. Павлова,
кандидат юридических наук, доцент,
Национальный центр законодательства
и правовых исследований Республики Беларусь

ЦИФРОВИЗАЦИЯ КАК ПЕРСПЕКТИВА И ВЫЗОВ ПРАВОВОМУ РАЗВИТИЮ

Аннотация. Цифровые преобразования жизнедеятельности общества и государства требуют соответствующего правового регулирования, а предварительно – уяснения сущности новых явлений, их правовой природы, формулирования дефиниций, соотношения с устоявшимися институтами права. Изложенное определило цель исследования – рассмотреть цифровизацию как современный тренд и выявить обусловленные этим концептуальные вопросы развития права, подлежащие учету в научной и нормотворческой деятельности. В рамках исследования рассмотрены вопросы, касающиеся «оцифровки» традиционно складывающихся

отношений, автономности и правосубъектности системы искусственного интеллекта, роли охранительных отраслей в развитии права в условиях цифровизации.

Ключевые слова: право, цифровые технологии, цифровые инструменты, искусственный интеллект, свобода воли, криминализация деяний, осуществляемых в виртуальной среде

DIGITIZATION AS A PROSPECT AND CHALLENGE FOR LEGAL DEVELOPMENT

Abstract. Digital transformations of the life of society and the state require appropriate legal regulation, and first, an understanding of the essence of new phenomena, their legal nature, the formulation of definitions, and the relationship with established legal institutions. The foregoing determined the purpose of the study – to consider digitalization as a modern trend and to identify the resulting conceptual issues in the development of law that must be taken into account in scientific and rule-making activities. The study examined issues related to the "digitization" of traditionally developing relationships, the autonomy and legal personality of the artificial intelligence system, and the role of security industries in the development of law in the context of digitalization.

Keywords: law, digital technologies, digital tools, artificial intelligence, free will, criminalization of acts carried out in a virtual environment

Введение. Цифровые преобразования, происходящие в управлении, экономике, социальной сфере приобрели необратимый характер и претендуют на роль современного драйвера развития общества и государства. Наглядными примерами является активное внедрение информационно-коммуникативных технологий (далее – ИКТ), технологий искусственного интеллекта (далее – ИИ), робототехники, 3D-печати, что может значительно снизить затраты субъектов хозяйствования на производство. Иные положительные стороны «цифровой цивилизации» также очевидны – оперативность электронного документооборота, электронные порталы госуслуг, GPS-навигация, банковские услуги в онлайн-режиме, удобство систем «умное производство», «умный дом», «электронный дневник» и т. д.

Данного рода достижения появились в последние два десятилетия – период, характеризующийся для Республики Беларусь развитием IV и формированием V технологического уклада. Несомненно, происходящие изменения требуют соответствующего правового сопровождения, а предварительно – решения вопроса о характере требуемых корректировок и приоритетах развития.

Основная часть. 1. В Республике Беларусь внимание вопросам цифровизации уделяется в программных документах развития государства и общества, в научных исследованиях в области права. Например, издание Декрета Президента Республики Беларусь от 21.12.2017 № 8 «О развитии цифровой экономики» заложило основы нормативному регулированию обращения токенов (цифровых знаков), рассмотрению их в качестве объекта правоотношений; Указом Президента Республики Беларусь от 07.04.2022 № 136 «Об органе государственного управления

в сфере цифрового развития и вопросах информатизации» оператором государственных цифровых платформ и информационных систем определен Центр цифрового развития в составе Министерства связи и информатизации Республики Беларусь; приведены определения ряда используемых терминов.

Примечательно, что вопросы цифровизации весьма стремительно вписались в повестку дня, не оставляя времени на опережающее и постепенное их изучение представителями гуманитарных наук, соотнесение привносимых благ и угроз, возможные возражения об их преждевременности, разработку гарантий для доминирования антропологической и в целом социальной составляющих в развитии общества и государства. Особо востребованы научные исследования, направленные на правовое сопровождение качественно новых отношений, связанных с цифровым преобразованием. Активно обсуждаются предложения об обновлении статуса личности и новых – цифровых – правах, уточнении статуса систем искусственного интеллекта, появлении роботов, которые включаются в правоотношения, изучении генерирования общественной опасности в цифровой среде, монополизации информационно-коммуникационной инфраструктуры отдельными корпорациями и др. [2; 3; 4]. При этом рассмотрение спорных вопросов, прогнозирование и описание рисков, которые влечет нелинейное становление цифровизации, все еще превалирует над методологическими разработками, конкретными предложениями, упреждающим научным анализом проектов правовых норм (актов).

2. Обращение к исследованиям белорусских и зарубежных ученых позволяет выделить проблематику соотношения информационного и цифрового права, круг охватываемых отношений [2; 7], что необходимо для определения направленности и содержания правового регулирования. «Цифровая трансформация и продукт его развития – цифровое право, которое само по себе для науки еще terra incognita, порождают много вопросов и правовых проблем как теоретического, так и практического свойства…» [7. С. 81]. Например, в одном случае речь может идти только об использовании информационно-коммуникационной инфраструктуры для «оцифровки» традиционно складывающихся отношений, приобретших (параллельно с письменной) электронную форму отображения. В частности, это – «электронный рецепт», «электронный дневник», что не требует кардинального изменения правового обеспечения, но указывает на необходимость уточнения имеющихся норм или их нейтрального изложения для охвата электронных и письменных форм. Представляется, что потенциал языка права способен описать подлежащие регламентации отношения, не допуская перенасыщения законодательства техническими терминами, что при этом не исключает дальнейшего умеренного развития понятийно-категориального аппарата права.

Во втором случае актуализируется проблема правового регулирования систем ИИ, претендующих по ряду функций на замещение деятельности человека. В научной литературе имеются различные определения систем ИИ. Например, ИИ определяется как полностью или частично автономная самоорганизующая (самоорганизующаяся) компьютерно-аппаратно-программная виртуальная или киберфизическая, в том числе био-кибернитическая, система (юнит), которой свойственны ряд способностей и возможностей, в том числе которых мышление,

обучение, накопление информации, принятие решений и т. д. [4. С. 94]. Системам ИИ присущи способности не только обучаться, но и самообучаться, что позволяет адаптировать свое поведение к происходящему, и тем самым делает возможным их подражание человеку в интеллектуальной сфере. С учетом развития иных отраслей знаний, способствующих функциональному улучшению жизнедеятельности человека, возрастают пределы таких возможностей.

3. Актуальной остается проблема поиска методологической основы для решения вопроса о правосубъектности автономных самоорганизующихся систем ИИ (умных роботов). В настоящее время отсутствует согласованный подход по данному вопросу – в специальной литературе предложены варианты рассмотрения систем ИИ как объекта, субъекта (квазисубъекта) права, электронного лица. Исходя из выбираемой модели обсуждаются варианты правовой оценки деяний стоящих за системой ИИ реальных (физических, юридических) лиц, в числе которых разработчики, продавцы, владельцы, пользователи; для обеспечения возмещения время, причиненного ИИ, отмечается важность развития института страхования ответственности [4; 8]. Вариативность предложений указывает на целесообразность критического анализа теоретических положений о правоотношениях, их субъектом составе, критериях отнесения к субъекту права.

При этом выполнение «умным роботом» различных функций в течение длительного времени без участия человека вряд ли следует рассматривать как классическую автономность самого робота, поскольку в данном случае речь более об автономности (самостоятельности) действий и принятии решений, но тех, которые возможны в рамках программы для данного робота. Следует принять во внимание, что системы ИИ не обладают такими качествами, как душа, чувства и т. д., являющимися существенными для субъектности физических лиц. «Если система ИИ демонстрирует поведение, которое может быть свидетельством перечисленных качеств, это означает, что система имитирует поведение человека, «но симуляция вещи – это не сама вещь»» [3. С. 121]. Кроме того полагаем, что автономия проявляется в самосознании и свободной воле, свойственных личности и во многом определяющих поведение, что и являет свободу как личностное свойство человека и не соотносится пусть и с относительной, но все же с программной алгоритмизацией.

4. В качестве рисков в системе «человек – право – государство – техника» отмечается, что «перспективы технического развития направлены не на работу человека с самим собой, а на постепенное вытеснение ценностных, личностно-конститутивных антропологических практик из социального пространства с заменой их на технические аналоги – «цифровые двойники» («интеллектуальные агенты») [5. С. 169]. Обеспокоенность рисками, связанными с ИИ, обозначена в Декларации XIV саммита БРИКС (Пекин, 2022 г.), вследствие чего указано на необходимость разработки общего подхода в отношении этического и ответственного использования ИИ (п. 57). Неприкосновенность частной жизни, риски трудовой занятости, вопросы взаимодействия (манипулирование, привязанность, агрессивность, правомочия и ответственность) человека и умных роботов – перечисленные проблемы и сложности развития предугадывались учеными ранее и подтверждаются современными

исследованиями. Соответственно при расширении спектра использования цифровых технологий необходимо определение приоритетов цивилизационного развития.

5. Для согласования оптимальной модели направленности развития при появлении цифровых систем, способных по ряду функций заменить человека, необходимы дальнейшие познания в области философии права, социологии права, антропологии права и проведение, в отличие от технических наук, исследований с акцентом на человека. В Резолюции Европейского парламента от 16.07.2017 «Гражданско-правовые норме о робототехнике также изложен принцип этического характера, согласно которому «технологии робототехники должны разрабатываться только с целью дополнить возможности человека, а не для того, чтобы заменить его» (п. 3) [1].

Важность гуманитарного анализа цифровизации обусловлена тем, что праву как социальному институту необходимо поддерживать корреляцию между реальным человеком и окружающей (реальной, виртуальной (в том числе проекты о Metaverse)) действительностью. В этой связи поддерживаем вывод, что отсутствие ориентации на человека как правового деятеля в развитии правовой реальности может привести к искажению целей права, постепенному их исчезновению из горизонта нормотворчества [6].

Актуальны для права вопросы реализации в условиях цифровизации как регулятивной, так и охранительной функций, при чем проблематика правонарушений и ответственности за причиненный вред могут выступить триггером развития регулятивного законодательства. Например, очевидная необходимость усиления охраны персональных данных способствовала изменению и дополнению закона Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации», созданию Национального центра защиты персональных данных Республики Беларусь. Пересмотра заслуживает подход о презумпции знания рядовым пользователем техники (в частности, ИКТ) [6], что в ряде случаев автоматического и необдуманного одобрения запросов, не являющихся основным содержанием используемого программного сервиса, приводит к причинению вреда и может повлечь признание лица правонарушителем. Притерпевание лицом негативного воздействия в виртуальной среде (несанкционированный доступ к телу при «теледильдонике», чрезмерное физическое воздействие посредством костюмов «обратной связи» [7. С. 210–214] заслуживает анализа на предмет общественной опасности, что может повлечь вопрос о криминализации деяний, складывающихся в качественно новых отношениях, необходимости уточнения правил разработки игр и иных коммуникаций и др.

Заключение. С развитием научно-технического прогресса появляются новые решения, технологии, объекты отношений, что влечет необходимость соответствующего правового сопровождения, а предварительно – уяснения сущности и правовой природы новых явлений, формулирования дефиниций, встраивания в правовую систему. С учетом рассмотренных в настоящей работе вопросов полагаем возможным сделать следующие выводы:

– следует разграничивать использование информационно-коммуникационной инфраструктуры для «оцифровки» традиционно складывающихся отношений,

приобретающих электронную форму отображения, и «деятельность» систем ИИ. Учет данных особенностей значим для нормотворчества, а именно решения вопроса о необходимости корректировки имеющихся правовых актов или принятия новых, касающихся статуса систем ИИ;

– система ИИ способна замещать человека при выполнении ряда функций, в связи с чем объективно возникают вопросы о субъекте ответственности и в целом о правовом статусе системы ИИ. При нормативном описании системы ИИ важно не допустить перенасыщения законодательства техническими терминами;

– принятие предложения рассматривать систему ИИ как субъекта права влечет риски этического и антропологического характера, в связи с чем необходимо проведение социально-правовых исследований с акцентом на человеке, включая приоритеты развития, объекты, заслуживающие особой правовой охраны, значимость социального взаимодействия, культурные различия и потребности, определяющие содержательную сторону отношений, др.;

– критического анализа заслуживают теоретические положения о правоотношениях, их субъектом составе, критериям отнесения к субъекту права, а также рассмотрение применительно к данным вопросам так называемой «автономии умных роботов», которая соотносится с программной алгоритмизацией (определенной, относительно-определенной) и существенно отличается от свободной воли, присущей человеку;

– тщательного изучения требует используемый правоприменителями подход о так называемой презумпции знания рядовым пользователем ИКТ, программных сервисов, что сказывается на увеличении количества правонарушений и правонарушителей (преступников);

– возникающие качественно новые отношения, включающие цифровые инструменты, целесообразно анализировать на предмет общественной опасности, что может повлечь вопрос о криминализации некоторых деяний.

Список литературы

1. Civil Law Rules on Robotics. URL: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU %282016 %29571379_EN.pdf

2. Василевич Г. А. Технологические императивы: проблемы и риски реализации в сфере прав человека // Журнал зарубежного законодательства и сравнительного правоведения. 2023. Т. 19, № 1. С. 32–37.

3. Дремлюга Р. И., Дремлюга О. А. Искусственный интеллект – субъект права: аргументы за и против // Правовая политика и правовая жизнь. 2019. № 2. С. 120–25.

4. Морхат П. М. К вопросу о юридическом понимании искусственного интеллекта // Аграрное и земельное право. 2017. № 11(155). С. 89–95.

5. Павлов В. И. Человек – право – государство – техника: трансформация ценностных оснований правового регулирования в современном мире // Человек и право: проблема ценностных оснований правового регулирования: сб. науч. трудов (Минск, 3–4 мая 2019 г.). Минск. С. 163–176.

6. Павлов В. И. Трансформация субъекта права в условиях «цифрового поворота»: антрополого-правовой анализ // Субъект права: стабильность и динамика

правового статуса в условиях цифровизации: сб. науч. трудов. М.: Инфотропик Медиа, 2021. С. 21-33.

7. Трансформация права в цифровую эпоху: монография. Барнаул: Изд-во Алт. ун-та, 2020. 432 с.

Т. В. Пашнина,
кандидат юридических наук,
Российский государственный университет правосудия,
Уральский филиал

О СИСТЕМНОМ ПОДХОДЕ В ПРАВОВОМ РЕГУЛИРОВАНИИ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ ОБРАЗОВАНИЯ

Аннотация. Цель работы состоит в исследовании проблем и перспектив правового регулирования применения технологий искусственного интеллекта в сфере высшего образования. Подвергнуты анализу тенденции научно-технического прогресса человеческого общества и факторы, обуславливающие перспективность применения технологий искусственного интеллекта для поступательного развития государств. Констатирована необходимость скорейшей цифровой трансформации ключевых сфер и отраслей жизнедеятельности в качестве необходимого условия достижения национальных целей, поставленных стратегическими документами Российской Федерации. Обосновано, что одной из сфер, перед которой поставлена задача цифровой трансформации, является сфера образования. Доказано, что технологии искусственного интеллекта выступают обязательным условием для перехода сферы образования в смарт-форму. На примере высшей школы показано, что использование искусственного интеллекта в образовательном процессе способно как дать преимущества, так и поставить новые вызовы, в частности, связанные с широким распространением нейросети ChatGPT. Сделан вывод о необходимости системного подхода к созданию механизма правового регулирования применения технологий искусственного интеллекта в сфере образования, учитывающего не только правовые, но и этические и технические нормы и принципы.

Ключевые слова: искусственный интеллект, нейронные сети, ChatGPT, правовое регулирование искусственного интеллекта, этика искусственного интеллекта, цифровая трансформация, высшее образование

ABOUT THE SYSTEMATIC APPROACH IN THE LEGAL REGULATION OF THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THE FIELD OF EDUCATION

Abstract. The purpose of the work is to study the problems and prospects of legal regulation of the use of artificial intelligence technologies in higher education. The trends of scientific and technological progress of human society and the factors that determine

the prospects for the use of artificial intelligence technologies for the progressive development of states are analyzed. The necessity of early digital transformation of key spheres and branches of life activity as a necessary condition for achieving the national goals set by the strategic documents of the Russian Federation is stated. It is proved that one of the spheres facing the task of digital transformation is the sphere of education. It is proved that artificial intelligence technologies are a necessary condition for the transition of education to a smart form. Using the example of a higher school, it is shown that the use of artificial intelligence in the educational process can both give advantages and pose new challenges, in particular, related to the widespread use of the ChatGPT neural network. The conclusion is made about the need for a systematic approach to the creation of a system of legal regulation of the use of artificial intelligence technologies in the field of education, taking into account not only legal, but also ethical and technical norms and principles.

Keywords: artificial intelligence, neural networks, ChatGPT, legal regulation of artificial intelligence, ethics of artificial intelligence, digital transformation, higher education

Введение. Человек как представитель вида homo sapiens прошел длительный эволюционный путь, изменяясь под воздействием окружающих его природных и техногенных факторов, выступающих стимулами для его развития. В последнее десятилетие поток информации, ежегодно увеличивающийся по экспоненте, достижения научно-технической мысли XXI века, породившие создание и стремительное внедрение прорывных технологий во все сферы жизнедеятельности, стали теми «триггерами», которые не только определяют направления дальнейшей трансформации человеческой цивилизации, но и ставят перед ней принципиально новые вопросы.

При этом эксперты различных отраслей знаний роль главного технологического вызова ближайшего будущего отдают технологиям искусственного интеллекта, поскольку именно они, по обоснованному мнению А. В. Минбалеева, «рассматриваются в большинстве экономически развитых стран в качестве приоритетных на ближайшую перспективу развития, и именно с ними эксперты связывают экономический рост, конкурентоспособность государств, а также обеспечение их национальных интересов» [5. С. 1094].

Вызовы, которые искусственный интеллект ставит перед человечеством, детерминированы технической сложностью и неоднозначностью природы данной технологии, способной к «осознанно-волевой автономной деятельности» и к «поведению, не поддающемуся конструктивному прогнозированию со стороны сторонних субъектов» [1. С. 82, 83].

Сложная природа технологий искусственного интеллекта, обуславливает и трудности правового регулирования их применения, поскольку «традиционный механизм правового регулирования явно не имеет возможности оперативно воспринять особенности цифровой среды и специфику использования современных цифровых технологий, в том числе искусственного интеллекта» [5. С. 1094].

Основная часть. На сегодняшний день базовый законодательный нормативный правовой акт, максимально полно регулирующий применение искусственного интеллекта, в России отсутствует. При этом существует целый ряд правовых актов, посвященных стратегическим направлениям и практическому внедрению технологий искусственного интеллекта, начало создания которых положило принятие «Национальной стратегии развития искусственного интеллекта на период до 2030 года» (утв. Указом Президента Российской Федерации от 10.10 2019 г.).

Кроме собственно правовой регламентации, большое значение для регулирования вопросов прикладного характера сыграла разработка предварительных национальных и национальных стандартов касательно применения технологий искусственного интеллекта в конкретных сферах (аналитики больших данных, клинической медицины, навигационных системах воздушных судов гражданской авиации). Огромную позитивную роль в решении данных вопросов играет также приятие в 2021 году российского «Кодекса этики в сфере искусственного интеллекта».

Таким образом, несмотря на то, что профильный федеральный закон об искусственном интеллекте находится в стадии разработки, происходит активное внедрение данных технологий в различные сферы жизнедеятельности, сопровождаемое их точечным регулированием на уровне правовых, этических и технических документов. И здесь необходимо помнить о том, что правовое регулирование внедрения технологий искусственного интеллекта происходит в рамках более широкого процесса, связанного с цифровой трансформацией. И одной из сфер жизнедеятельности, перед которой в рамках данного процесса остро встала проблема создания адекватного механизма правового регулирования применения этих прорывных технологий, стала сфера высшего образования.

Отметим, что необходимость цифровой трансформации ключевых отраслей и сфер жизнедеятельности в качестве одной из стратегических целей развития страны была поставлена в (пп. д) п.1) Указа Президента РФ от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года», в соответствии с которым были разработаны и приняты ведомственные стратегии цифровой трансформации. В числе прочих цель цифровой трансформации была поставлена и перед сферой высшего образования, которой отводится ключевая роль в подготовке кадров, способных внести вклад в поступательное развитие страны, цифровой экономики и формирование российского общества знаний.

При этом процесс активного внедрения в образовательную деятельность цифровых технологий начался в период пандемии, когда применение ДОТ (дистанционных образовательных технологий) при осуществлении учебного процесса фактически стало обязательным условием соблюдения санитарно-эпидемиологических ограничений, продиктованных необходимостью предотвращения распространения коронавирусной инфекции COVID-19.

И. В. Ершова, Е. Е. Енькова отмечают, что «на сегодняшний день Федеральный закон от 29 декабря 2012 г. № 273 ФЗ «Об образовании в Российской Федерации» предусматривает право образовательных организаций осуществлять реализацию образовательных программ с применением электронного обучения

и дистанционных образовательных технологий. Действующие образовательные стандарты также определяют «цифровые» возможности вузов» [3. С. 25–26].

Цифровая трансформация вузов стала логическим продолжением данного процесса. В числе подзаконных правовых актов, регулирующих вопросы цифровизации сферы образования, были приняты Распоряжение Правительства РФ от 21.12.2021 № 3759-р «Об утверждении стратегического направления в области цифровой трансформации науки и высшего образования», «Стратегия цифровой трансформации отрасли науки и высшего образования» (2021); Письмо Минобрнауки России от 07.10.2021 № МН-19/697 «О направлении методических рекомендаций по разработке стратегии цифровой трансформации образовательных организаций высшего образования, подведомственных Минобрнауки России» и др. На локальном уровне также были разработаны соответствующие положения, касающиеся цифровой трансформации конкретных образовательных учреждений.

Данные документы поставили перед высшими учебными заведениями страны задачу скорейшего достижения показателей цифровой зрелости и обозначили искусственный интеллект в качестве одной из самых перспективных технологий, используемых в цифровых сервисах онлайн образования для создания максимально персонализированного обучения, в частности, рекомендованного для использования в рамках проектов «Датахаб», «Единая сервисная платформа науки», и др. В данном контексте технологии искусственного интеллекта рассматриваются как база для трансформации сферы образования в качественно иной уровень – уровень смарт-образования.

Ряд авторов отмечают, что «основное преимущество искусственного интеллекта – возможность решать некоторые задачи, для решения которых человек не обладает алгоритмами или это решение потребует огромного количества времени» [4. С. 100], что обуславливает перспективность использования данной прорывной технологии в образовании, поскольку одним из способов преодоления кризисных явлений в современном российском образовании экспертами называется переход от запаздывающего образования к опережающему [6. С. 102].

Однако при всех преимуществах, порождаемых цифровой трансформацией и использованием прорывных технологий, дающих возможность построения индивидуальных образовательных траекторий, гибких курсов и т. д., тем самым позволяющих сделать высшее образование максимально доступным, достижения в разработке технологий искусственного интеллекта поставили перед сферой образования новые вызовы, в частности, связанные с широким распространением нейросети ChatGPT, способной генерировать тексты, имитирующие созданные человеком, в свете чего перед сферой высшего образования встала проблема «академической GPT-непорядочности», связанной с выполнением образовательных работ с помощью ChatGPT, которые обучающиеся (студенты) представляют как выполненные лично [2. С. 8], что вызвало обоснованную тревогу у педагогов и привело к введению ряда ограничений на использование нейросетей в разных стран, например, в школах США и в университетах Франции.

Тем не менее, как справедливо отмечают эксперты, ограничительные меры не способны остановить применение сквозных цифровых технологий в процессе

обучения [2. С. 8–9]. Более того, умение использовать преимущества прорывных технологий на сегодняшний день становится обязательным условием подготовки высшей школой специалистов, востребованных на рынке труда в реалиях цифровой экономики.

Заключение. В данных обстоятельствах установление четких границ применения технологий искусственного интеллекта в образовательном процессе является необходимым условием гармонизации требований технического прогресса и ценностно-этическим содержанием образовательной деятельности. При этом необходим системный подход к созданию средств правового регулирования применения технологий искусственного интеллекта в сфере образования, учитывающий не только правовые, но и этические, а также технические нормы, содержащиеся в документах по стандартизации.

Правовая основа данной системы должна включать как упомянутые ранее нормативные и этические документы, регулирующие применение искусственного интеллекта в России в целом, так и специальные нормы, касающиеся использования прорывных технологий в сфере высшего образования, важнейшими из которых, на наш взгляд, на сегодняшний день должны стать положения локальных нормативных актов образовательных организаций, содержащих нормы, касающиеся этических аспектов допустимости либо недопустимости использования технологий искусственного интеллекта в процессе обучения, максимально четко определяющих пределы такого использования и устанавливающих меры дисциплинарной ответственности за их нарушение.

Также необходимым считаем включение положений, касающихся обучения с использованием нейросетей, в федеральные государственные образовательные стандарты высшего образования.

В перспективе целесообразным представляется разработка силами профессионального сообщества этического кодекса применения искусственного интеллекта в сфере отечественного образования, аналогичного «Рекомендациям об этических аспектах искусственного интеллекта» (2021), разработанного под эгидой ЮНЕСКО.

При этом упомянутые выше нормы должны согласоваться с положениями базового профильного закона образовательной сферы и способствовать скорейшему достижению целей, заданных стратегическими документами Российской Федерации.

Список литературы

1. Бегишев И. Р., Латыпова Э. Ю., Кирпичников Д. В. Искусственный интеллект как правовая категория: доктринальный подход к разработке дефиниции // Актуальные проблемы экономики и права. 2020. Т. 14, № 1. С. 79–91.

2. Гаркуша Н. С., Городова Ю. С. Педагогические возможности ChatGPT для развития когнитивной активности студентов // Профессиональное образование и рынок труда. 2023. Т. 11, № 1. С. 6–23.

3. Ершова И. В., Енькова Е. Е. Цифровая зрелость как показатель успешности цифровой трансформации университета // Вестник Университета имени О. Е. Кутафина (МГЮА). 2022. № 12 (100). С. 20–29.

4. Лукинский И. С., Горшенева И. А., Сумина А. В. Использование искусственного интеллекта в качестве инструмента оптимизации научной деятельности: pro et contra // Психология и педагогика служебной деятельности. 2023. № 1. С. 99–102.
5. Минбалеев А. В. Понятие «искусственный интеллект» в праве // Вестник Удмуртского университета. Серия Экономика и право. 2022. Т. 32, № 6. С. 1094–1099.
6. Степанова Г. А., Демчук А. В., Арпентьева М. Р. К проблеме кризиса российского образования // Проблемы современного образования. 2021. № 2. С. 102–113.

Н. В. Караваев,
кандидат юридических наук,
Волго-Вятский институт (филиал)
Московского государственного юридического
университета имени О. Е. Кутафина
С. В. Педань,
студент,
Волго-Вятский институт (филиал)
Московского государственного юридического
университета имени О. Е. Кутафина

ОСОБЕННОСТИ КОММЕРЦИАЛИЗАЦИИ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Аннотация. В статье рассматриваются проблемы реализации договора купли-продажи в популярных у современного человека маркетплейсах, выделяет основные преимущества и недостатки таких торговых площадок. Целью исследования является анализ проблемы привлечения маркетплейсов к ответственности в случае продажи контрафактных или некачественных товаров. Автор выделяет ситуации, в которых маркетплейсы либо не несут ответственности (выступают информационным посредником), либо отвечают на общих основаниях.

Ключевые слова: маркетплейс, цифровизация, купля-продажа, ответственность за некачественный товар, контрафактные товары, интернет-магазин, электронный товарооборот

FEATURES OF COMMERCIALIZATION OF INTELLECTUAL PROPERTY IN MODERN CONDITIONS

Abstract. In the article examines the problems of implementing a purchase and sale agreement in marketplaces popular with modern people, highlights the main advantages and disadvantages of such trading platforms. The purpose of the study is to analyze the problem of bringing marketplaces to responsibility in case of sale of counterfeit or low-quality goods. The identifies situations in which marketplaces either do not bear responsibility (act as an information intermediary), or respond on a general basis.

Keywords: marketplace, digitalization, purchase and sale, responsibility for low-quality goods, counterfeit goods, online store, electronic turnover

В настоящее время невозможно представить какие-либо повседневные дела без информационных разработок. В частности, заметное влияние на общество оказывает Интернет, который с каждым годом видоизменяется одновременно с ростом потребностей человека. Так, Всемирная паутина сопровождает нас везде: в Интернете люди получают образование, узнают что-то новое, общаются, передают сообщения, работают, рекламируют какой-либо вид деятельности или какую-либо организацию, совершают покупки, заключают различные гражданско-правовые договоры и т. д.

Одной из самых популярных и, пожалуй, полезных разработок является использование различных агентов-посредников, предлагающих на собственных интернет-сайтах за определенную денежную сумму предложения индивидуальных предпринимателей и юридических лиц о продаже огромного количества товаров. Роль таких посредников заключается в том, что они «соединяют самостоятельных экономических агентов – производителей и потребителей – посредством специальной инфраструктуры» [2. С. 147]. В настоящее время платформу, на которой работают такие посредники, называют «маркетплейсами». Их можно сравнить с некой «виртуальной витриной» магазина, которая позволяет покупателю в рамках одного «здания» проанализировать различные предложения, сравнить их параметры и выбрать подходящий для себя вариант как по ценовой категории, так и по внешним признакам.

В большинстве научных работ под маркетплейсами понимаются специализированные интернет-сайты, на которых можно найти товары от разных юридических лиц и индивидуальных предпринимателей, представленных на одной и той же платформе [4. С. 21–24]. На данной площадке покупатель формирует некий поисковый запрос для покупки необходимого товара, собственник и разработчик торговой площадки (посредник) отвечает за привлечение клиентов и обработку этих самых запросов и заказов, в то время как сами продавцы товаров реагируют на заказ и начинают его собирать для дальнейшей отправки покупателю. Российские суды в своей деятельности руководствуются схожим понятием: «Маркетплейс – платформы электронной коммерции, предоставляющей информацию о продукте или услуге третьих лиц, чьи операции обрабатываются оператором маркетплейса» [13]. В настоящий момент крупнейшими действующими в России маркетплейсами являются, например: «Wildberries», «Ozon», «Яндекс.Маркет», «Lamoda», «СберМегаМаркет».

Определяя понятие «маркетплейса», сразу разграничим его с понятием «интернет-магазин». Различие между ними может быть неочевидно для обычного потребителя товаров и услуг, однако у каждого из них есть свои особенности, которые необходимо знать при защите своих прав и интересов, которые были нарушены данными видами интернет-площадок. Так, интернет-магазин может быть разделен на два вида: магазин одного производителя (аналог какого-либо магазина люксовой одежды, спортивных товаров) или же магазин с широким ассортиментом товаров от различных производителей (по аналогии с гипермаркетом или универмагом). Владельцы интернет-магазина приобретают какой-либо товар у производителей и в дальнейшем осуществляют его перепродажу, устанавливая

свою ценовую политику. Маркетплейс же, наоборот, представляет собой некий торгово-развлекательный центр, который не является непосредственным продавцом товаров и услуг, а предоставляет изготовителям и поставщикам в аренду площади и помещения. Соответственно, маркетплейс сотрудничает с юридическими лицами и индивидуальными предпринимателями, осуществляющими производство и продажу товаров под своим брендом, предоставляя им в пользование так называемые лоты и личные кабинеты (нишу) на своем сайте, не являясь при этом, как правило, исполнителем услуг по продаже и обслуживанию клиентов, как это делает тот же интернет-магазин. Здесь уже не разработчик маркетплейса, а сам продавец размещает товары, формирует ценники и скидки на своей странице, продвигает и отправляет товар. Получается, в интернет-магазине идет непосредственное взаимодействие продавца и покупателя, в маркетплейсах же появляется некий посредник, который обеспечивает движение товара и привлекает новых клиентов (рис. 1).

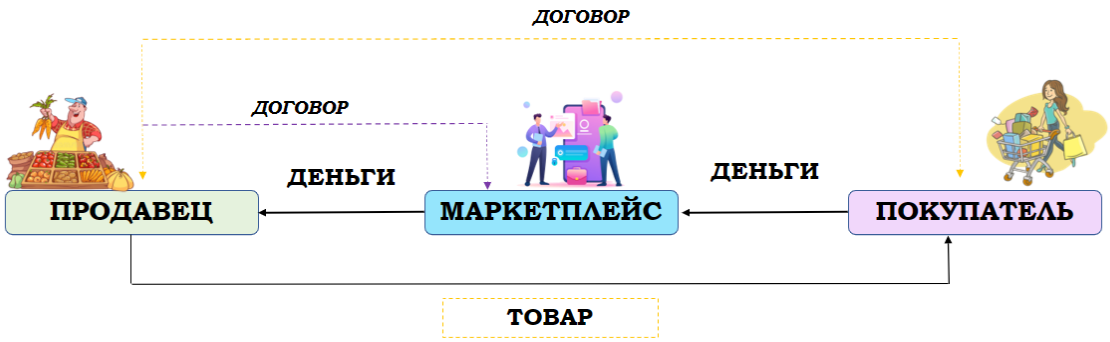

Рис. 1. Принцип работы маркетплейса.

Источник: составлено автором.

Выделим основные преимущества маркетплейсов:

– покупатели получают широкий ассортимент товаров в одном интернет-ресурсе. При таком варианте у потребителя появляется больше возможностей найти подходящую для его финансового положения цену за товар самого высокого качества при данной цене и с необходимыми характеристиками;

– формирование базы отзывов и рейтингов применимо к каждому производителю, что упрощает коммуникацию, так как помогает потребителю сделать правильный выбор, повышает доверие к продавцу и к маркетплейсу в целом;

– обновляемая в режиме реального времени информация о цене и наличии того или иного товара, что помогает покупателям находить самые выгодные предложения в зависимости от своего финансового положения;

– наличие высокой конкуренции, что способствует проведению низкой ценовой политики и появления большого количества акций и предложений, чем в традиционных магазинах;

– гарантируется безопасность личных данных пользователей, возможность конфиденциального совершения покупок через аватар.

Безусловно, данные преимущества относятся только к потребителям, так как маркетплейсы, как и обычные магазины в период рыночной экономики ориентированы именно на приобретателей товаров. Это связано с тем, что удовлетворенные потребители – это гарант длительного существования продавцов на рынке определенного сегмента, а также наличие постоянно растущей прибыли.

Безусловно, маркетплейсы заметно упрощают нашу жизнь и пользуются популярностью как у людей старшего поколения, так и у молодежи. При этом нельзя отрицать и тот факт, что некачественные товары встречаются довольно часто. В связи с этим люди задаются вопросом: несут ли маркетплейсы ответственность за попадание на их площадки контрафактной продукции перед правообладателем и перед потребителем?

Согласно п. 1 ст. 1477 Гражданского кодекса Российской Федерации (далее – ГК РФ), товарный знак – это обозначение, служащее для индивидуализации товаров юридических лиц или индивидуальных предпринимателей. Использование товарных знаков позволяет индивидуализировать товар определенного производителя или продавца, отграничить его от других товаров, создать у покупателей определенный образ товара или ассоциации, связанные с ним. Защита товарного знака особенно важна в виртуальной среде, так как на одной и той же интернет-платформе может одновременно присутствовать оригинальный товар и его подделка, которые нельзя отличить друг от друга. В связи с применением цифровых технологий и их влиянием на средства индивидуализации возникает ряд теоретических и практических проблем.

Как мы уже отметили, в настоящее время на маркетплейсах довольно часто фиксируются случаи незаконного размещения и использования некоторыми продавцами чужих товарных знаков, соответственно, и введение потребителей в заблуждение. К сожалению, во многих случаях покупатель, при выборе товара определенной марки, наталкивается на предложения недобросовестных продавцов, которые используют чужой товарный знак в своих целях. Соответственно, отличное качество, которое гарантируется правообладателем определенного товара под некой маркой, не предоставляется продавцом контрафактной продукции. Покупатель, не зная всей ситуации, разочаровывается же именно в продукции истинного правообладателя. [1. С. 133–141]. К примеру, индивидуальный предприниматель продает на «Wildberries» футболки с ручной вышивкой. Дизайн вышивки и самой футболки предприниматель придумал сам, сам вкладывал деньги в профессиональную фотосессию товара, придумывает к каждой модели продающий текст и др. Все перечисленное относится к такой категории интеллектуальной собственности, как объекты авторских прав. Данные футболки предприниматель продает под собственным брендом, который зарегистрирован в качестве товарного знака, что является средством индивидуализации.

При этом на этой же площадке появляется точно такие же футболки с вышивкой: он выставляет на продажу точно такую же одежду, копирует фото, использует для продвижения товара название и уникальный товарный знак, которые

так старательно разрабатывал создатель магазина авторской одежды, к тому же продает данный товар по более низкой цене. Вследствие такой ситуации у добросовестного предпринимателя «падает» спрос, футболки больше не продаются, он теряет прибыль. Нарушитель же, не получая разрешения использовать авторский контент в коммерческих целях, все же получает прибыль. Схожая ситуацию наблюдается и с декоративной косметикой, в частности, можно привести в качестве примера тушь для ресниц. На одном и том же сервере присутствуют сразу два бренда под наименованием «Vivienne Sabo», но ссылка на продавца имеет другой дизайн (рис. 2). Здесь же мы видим, что цены двух одинаковых продуктов значительно отличаются и спрос больше на ту тушь, где предложена более низкая цена. Потребитель, которому важно приобрести качественный и сертифицированный товар, не сможет отличить оригинал от «подделки».

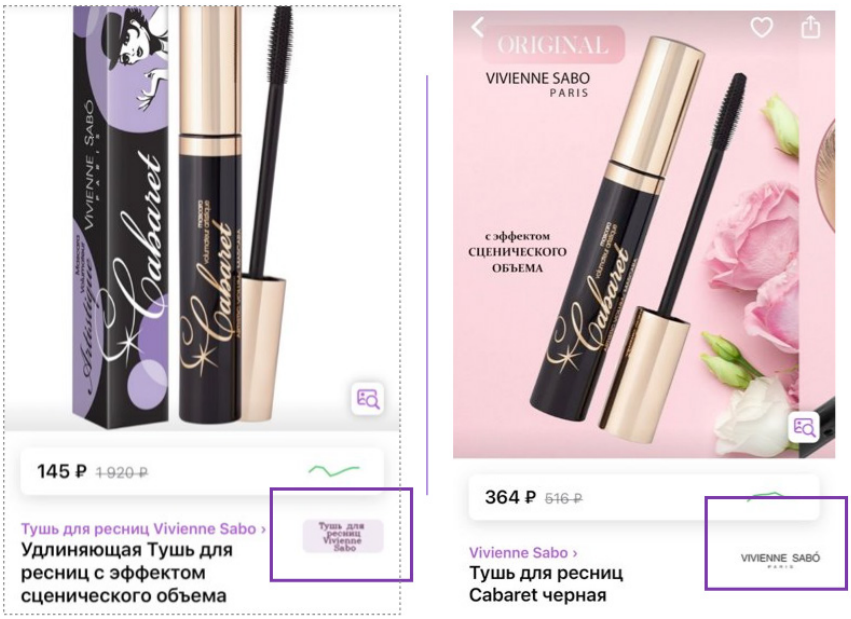

Рис. 2. Сравнение двух товаров, реализуемых под одним наименованием

Получается, мы наблюдаем случаи нарушения исключительного права правообладателя на товарный знак, а также введение потребителей в заблуждение. Так, действительный обладатель данного товарного знака может написать заявление в Антимонопольную службу или напрямую обратиться в соответствующий арбитражный суд. Но здесь необходимо знать кому именно мы будем адресовывать свои требования: другому предпринимателю или самому маркетплейсу, который позволил «зайти» на рынок недобросовестному лицу, а может направить свои требования сразу двум лицам.

Практика показывает, что в случае борьбы с контрафактом в обычных магазинах модель поведения потребителей уже сформировалась, т. е. они знают последовательность своих действий для защиты нарушенного права. В случае же с контрафактами, размещаемых на маркетплейсах, защитить права потребителей и изготовителей достаточно сложно. В частности, до сих законодательно

не разрешен вопрос о том, несут ли маркетплейсы ответственность за то, что на их сайтах предлагаются к продаже и продаются контрафактные товары.

Согласно п. 6.1 ст. 1252 Гражданского кодекса Российской Федерации (далее по тексту – ГК РФ), если одно нарушение исключительного права на результат интеллектуальной деятельности или средство индивидуализации совершено действиями нескольких лиц совместно, такие лица отвечают перед правообладателем солидарно. Здесь же интересен п. 73 Постановления Пленума Верховного Суда РФ № 10 от 23 апреля 2019 г. (далее – Постановление Пленума ВС РФ № 10), в котором говорится о том, что использование объекта интеллектуальной собственности по поручению или заданию лица, нарушившего исключительное право правообладателя, образует нарушение исключительного права [7]. Получается, маркетплейс, согласно данным положениям, может нести ответственность как некий информационный посредник между продавцом и покупателем. Но и здесь есть свои особенности.

Необходимо учитывать роль самого маркетплейса в отношениях, возникающих между продавцом и покупателем. Так, мы можем выделить две роли маркетплейса: выступление в роли самостоятельного продавца, который действует на основании агентского договора и получает определенный процент от реализуемого товара, и уже упоминаемая нами выше роль информационного посредника, который предоставляет возможность опубликовать информацию о товарах, тем самым реализовав его предложение для большой группы потребителей, при этом не участвует в продаже.

Примером первого случая является маркетплейс «Wildberries», который обязуется за вознаграждение совершать от имени продавца и за его счет сделки по реализации товаров продавца. К тому же данная платформа также вправе сама определять цены на конкретный товар или же применять скидки к цене продавца без предварительного запроса об этом [5]. Получается, при такой модели поведения маркетплейс несет ответственность за нарушение исключительных прав продавцов на товарные знаки, незаконное размещение товаров под чужими товарными знаками, за продажу контрафактного товара. Это связано с тем, что при решении вопроса о привлечении торговой площадки к ответственности по данному основанию, суды учитывают следующее:

– источник получения прибыли: получают установленный договором размер процентов от продаж;

– кто размещает информацию на сайте и осуществляет дальнейшее редактирование данных, оказывает дополнительные услуги по продвижению (рекламе) товаров.

Исходя из этого, в совокупности с данными признаками маркетплейс непосредственно участвует в сделке по реализации товара, при этом учитывается его воля. В таком случае, при нарушении исключительных прав, он несет ответственность на общих основаниях. Данное утверждение подтверждается и судебной практикой.

Так, 22 июня 2022 г. Суд по интеллектуальным правам вынес итоговое решение по иску ООО «Комфортплюс» (владелец товарного знака) к ООО «Wildberries» и ООО «Строй Материалы Холдинг» [8]. Так, Истец хотел взыскать 2 млн рублей

как с маркетплейса, так и непосредственно с продавца. Суды трех инстанций встали на сторону Истца по следующей причине: в рамках дела было установлено, что известная торговая площадка знала о содержании размещенной информации и, что самое интересное, могла вносить в нее изменения, т. е. выступала в роли редактора. Деньги, полученные от покупателей, также поступали на счет маркетплейса, что подтверждалось электронными чеками. Получается, в данном случае маркетплейс выступал не в роли информационного посредника, а в роли полноправного участника гражданских правоотношений по купле-продаже.

Подобные случаи встречаются часто. Так, индивидуальный предприниматель обратился с иском сразу к двум субъектам: к производителю вафельных трубочек и к маркетплейсу. По мнению первого, при реализации товаров были нарушены его исключительные права на товарный знак. Суд взыскал компенсацию как с производителя, так и с продавца солидарно 200 тысяч рублей. При этом Суд при вынесении решения руководствовался следующим: продавец в обязательном порядке должен осуществлять проверку закупаемой им продукции на предмет не нарушит ли реализация заграничного товара в РФ права третьих лиц в поле интеллектуальной собственности [9]. Думаем, такое решение связано не столько с тем, что маркетплейс не проверил предоставляемый товар на предмет нарушения исключительных прав, но и не ответил на претензию Истца, тем самым не попытался исправить нарушение прав последнего.

В качестве примера можно также многочисленные контрафакты посуды, которые продаются под известным брендом «Zepter». Посуда Zepter является гарантией качества для многих россиян. Наверное, поэтому подделки под эту торговую марку наводнили самый популярные маркетплейсы. При поиске по сайтам выдаются десятки предложений ножей Zepter. При этом на данных сайтах сильно рознится цена. Так, на официальном маркете Zepter набор ножей можно купить за 38 тыс. рублей, на маркетплейсах же множество продавцом предлагают такие ножи по цене не больше 5 тыс. руб.

Второй случай применим, если маркетплейс будет признан судом информационным посредником. Согласно ст. 1253.1 ГК РФ информационным посредником признается лицо, осуществляющее передачу материала в информационно- телекоммуникационной сети, в том числе в сети «Интернет», лицо, предоставляющее возможность размещения материала или информации, необходимой для его получения с использованием информационно-телекоммуникационной сети, а также лицо, предоставляющее возможность доступа к материалу в этой сети. Из данного нормативного толкования можно сделать следующий вывод: маркетплейсы могут быть отнесены к информационным посредникам только в том случае, если они предоставляют третьим лицам возможность размещения определенного материала и оказывают ряд сопутствующих услуг, не связанных с самостоятельным продвижением маркетплейсами товаров и услуг.

К примеру, платформа «Яндекс.Маркет», в соответствии со своим договором, размещает данные о товаре, предоставленные заказчиком, в своей базе данных, оказывает услуги по привлечению клиентов и формирования спроса для заключения договоров купли-продажи, оказывают услуги, связанные с реализацией

товаров, не выступая при этом самостоятельным продавцом товаров. Получается, данная платформа лишь передает информацию продавца о товарах и размещает ее на сайте [6].

В п. 78 Постановления Пленума ВС РФ № 10 указывается, что информационным посредником владелец интернет-сайта, на котором размещены материалы, включающие результаты интеллектуальной деятельности или средства индивидуализации, выступает именно тогда, когда он докажет, что материалы размещены третьими лицами, а не владельцем сайта. Получается, признание маркетплейса информационным посредником не является абсолютным основанием для освобождения его от ответственности, так как суд должен исходить из совокупности доказательств каждого конкретного дела. При этом информационный посредник, осуществляющий передачу материала в информационно-телекоммуникационной сети, не несет ответственность за нарушение интеллектуальных прав, произошедшее в результате этой передачи, при одновременном соблюдении следующих условий:

1) он не является инициатором передачи контрафактной продукции и не определяет получателя указанного материала;

2) он не изменяет указанный материал при оказании услуг связи, за исключением изменений, осуществляемых для обеспечения технологического процесса передачи материала;

3) он не знал и не должен был знать о том, что использование соответствующих результатов интеллектуальной деятельности или средств индивидуализации лицом, инициировавшим передачу материала, содержащего соответствующие результаты интеллектуальной деятельности или средства индивидуализации, является неправомерным [3].

По модели информационного посредничества маркетплейс не реализует товары от своего имени, а лишь предоставляет продавцам площадку, на которой они могут находить покупателей и реализовывать свои товары самостоятельно, т. е. не имеет напрямую отношение к осуществлению сделки купли-продажи. В таком случае информационный посредник (маркетплейс) несет ответственность за нарушение интеллектуальных прав при наличии его вины. Такая устойчивая позиция сформировалась и в судебной практике.

В одном деле Десятый арбитражный апелляционный суд отказал правообладателю товарного знака «КОФТЁНЫШИ», охраняемого в отношении одежды, в удовлетворении иска к ООО «Wildberries» о взыскании компенсации [10]. Суд посчитал, что в данном деле торговая платформа выступает в роли информационного посредника, так как ее функции сводятся только к предоставлению продавцам возможности размещать материалы или иную информацию на сайте платформы, тем самым привлекая потребителей.

Интерес представляет также дело о взыскании компенсации за нарушение исключительных прав на товарные знаки по иску индивидуального предпринимателя к ООО «Интернет решения» (маркетплейс «Озон»). Правообладатель товарного знака на восточные сладости обратился в суд за защитой своего исключительного права и с требованием выплатит ему компенсацию в размере 500 тысяч

рублей. Ответчиком в данном разбирательстве выступил «Озон». Суды также как и в предыдущем примере отказали в требовании по следующему основанию: маркетплейс только предоставил лот для размещения товаров, другие услуги им не оказывались [11]. Исходя из этого суды в первую очередь руководствуются тем, что продавцы обладают способностями и возможностями самостоятельно и без участия разработчиков маркетплейса зарегистрироваться на площадке в статусе продавца, самостоятельно указать данные о товаре, заключить договор напрямую с покупателем, в связи с чем маркетплейсы не должны нести какую-либо ответственность.

Здесь же необходимо иметь ввиду то, что, если маркетплейс нельзя привлечь к ответственности, это не значит, что исключительное право нельзя защитить. В таком случае пострадавшей стороне юристы-практики советуют напрямую обращаться к производителю товара, не тратя финансовые средства и моральные ресурсы, выясняя отношения еще и с интернет-площадкой. Так, деле индивидуального предпринимателя К. А. Богданова и ООО «ТВОЕ» поднимался вопрос о привлечении компании ООО «ТВОЕ» к ответственности за нарушение исключительных прав ввиду того, что последний производил и реализовывал на различных маркетплейсах футболки, на которых были напечатаны рисунки Истца [12]. В данном случае Суд обязал Ответчика выплатить 100 000 руб. Таким образом, ответственность за нарушение интеллектуальных прав на платформах электронной торговой площадки несут в большинстве случаев продавцы, а не информационные посредники, которыми в данном деле и были признаны маркетплейсы.

Безусловно, руководствуясь моделью информационного посредника, мы не можем привлечь различные маркетплейсы к ответственности, но это не отменяет того факта, что именно на этих платформах реализуется большинство контрафактной продукции, что вводит многих потребителей в заблуждение и влияет на репутацию и уровень прибыли производителей оригинальной продукции. В связи с этим важно разработать какой-либо действенный механизм защиты потребителей и правообладателей от контрафактной продукции, избегая при этом обращения в органы правосудия.

Считаем необходимым ввести дополнительную и основополагающую обязанность для маркетплейсов, которая будет заключаться в запрашивании у продавцов или производителей, которые хотят использовать электронную торговую площадку для размещения своих товаров, документы, подтверждающие регистрацию в установленном законом порядке принадлежащих им товарных знаков или разрешения на использование чужих товарных знаков (свидетельство на товарный знак, лицензионный договор, договор коммерческой концессии). Если же необходимых документов не предоставили – отказывать в заключении договора с продавцом.

В связи с довольно актуальной и явно «болезненной» проблемой решило бороться и Правительство, которое 29 июля 2022 г. приняло Постановление, согласно которому начиная с 1 марта 2023 г. маркетплейсы начинают нести ответственность за размещение на своих сайтах контрафактной продукции, а также немаркированного товара. Как следует из документа, маркетплейсы обязаны

передавать все необходимые сведения в специальный реестр для идентификации продавцов и изготовителей. Данная информация позволяет прослеживать движение товара от производителя продукции до момента продажи товара потребителю.

Считаем, что такая маркировка не уменьшит поток контрафактной продукции, предлагаемой маркетплейсами. В частности, вышеописанный способ борьбы с контрафактом возведет барьер для мелких фирм или начинающих индивидуальных предпринимателей, ведь любая маркировка требует от участников дополнительных финансовых затрат на закупку соответствующего оборудования, что не все компании могут себе позволить.

Правильным будет обеспечить собственный контроль маркетплейсов за своей деятельностью, а именно самостоятельная борьба с контрафактами под угрозой привлечения к ответственности вне зависимости от того, выступала площадка заинтересованным лицом либо информационным посредником. Так, на сегодняшний день самые крупные и, пожалуй, популярные торговые площадки Wildberries, Ozon и Яндекс.Маркет договорились о сотрудничестве. Они начали создавать свою базу данных для регистрации обнаруженных ими контрафактных товаров с целью приостановки их движения от недобросовестного продавца к потребителю. В систему будут вноситься данные о случаях размещения контрафакта, информация о продавцах таких товаров, а также сведения из документов, подтверждающих нарушение [14].

Работа такой базы данных видится следующим образом: после отправки формы жалобы или заявления, которые формируются автоматически системой маркетплейса, от правообладателя, потребителя или представителей государственных или муниципальных органов, маркетплейс в кратчайшие сроки блокирует такие предложения на своей площадке. Информация о блокировке и о самом недобросовестном продавце выгружается в информационную систему для дальнейшего сопоставления с другими случаями продажи контрафакта. Если «подозрительный» продавец встречается в данной базе больше двух раз, у него запрашиваются необходимые документы, а при их отсутствии или недостоверности страница данного продавца удаляется. При таком методе действительно надо работать сообща, так как закрытие одного «рынка» не становится препятствием для недобросовестного продавца перейти на другой «рынок».

Здесь же отметим, что вышеназванный метод работает против тех контрафактных товаров, которые уже размещены на сайтах маркетплейсов. Так, контролировать поток контрафактной продукции необходимо еще «на входе» уполномоченными на то сотрудниками маркетплейса [15. С. 27]. Такой шаг позволит не просто предотвратить нарушение исключительного права, но и вообще не допустит любой возможности такого нарушения. Безусловно, это создаст нагрузку на работников маркетплейса, но лучше потратить свои материальные и моральные ресурсы на начальной стадии, чем потом участвовать в различных судебных разбирательствах.

Таким образом, защита прав на товарные знаки является очень важным элементом коммерческой деятельности не только для представителей предпринимательской деятельности, но и для электронных торговых площадок (маркетплейсов),

так как они также могут быть привлечены к ответственности и понести серьезные финансовые потери. Используя чужой товарный знак, нарушитель способствует оттоку основной части прибыли от оригинального продавца, наносит последнему вред репутации, так как потребитель во многих случаях ассоциирует товар именно с его производителем, а ухудшение качества товара из-за незаконных действий других лиц снижает уровень доверия покупателей к бренду в целом.

Вследствие этого законодателю стоит незамедлительно реагировать на данные случаи нарушения исключительных прав. В частности, стоит разработать перечень четких критериев, согласно которым маркетплейсы будут нести солидарную с продавцом ответственность.

Список литературы

1. Ворожевич А. С. Споры по нарушениям исключительных прав на товарные знаки в маркетплейсах // Журнал Суда по интеллектуальным правам. 2021. № 2(32). С. 133–141.

2. Иванов А. А. Бизнес-агрегаторы и право // Закон. 2017. № 5. С. 145–156.

3. Лазарева Ю. А. Защита исключительных прав на платформах электронной коммерции // Журнал суда по интеллектуальным правам. 2022. № 6. С. 18–25.

4. Мастеров А. И. Управленческий анализ смешанных затрат в условиях многономенклатурной реализации // Актуальные проблемы социально-экономического развития России. 2012. № 2. С. 21–24.

5. Оферта о реализации товара на сайте Wildberries. URL: https://mstatic.wbstatic.net/suppliers-portal-root/0.0.2/offer-ru.pdf

6. Оферта на оказание услуг «Яндекс Маркет». URL: https://yandex.ru/legal/oferta_market

7. О применении части четвертой Гражданского кодекса Российской Федерации: Постановление Пленума Верховного Суда РФ от 23 апреля 2019 г. № 10. URL: https://www.consultant.ru

8. Постановление Суда по интеллектуальным правам от 22.06.2022 г. по делу № А41-85375/2020. URL: https://www.garant.ru

9. Постановление Девятого арбитражного апелляционного суда от 06.11.2020 № 09АП-48163/2020. URL: https://www.consultant.ru

10. Постановление Десятого арбитражного апелляционного суда от 1 декабря 2021 г. № 10АП-21094/21 по делу № А41-73925/2020. URL: https://base.garant.ru

11. Постановление Суда по интеллектуальным правам от 21 февраля 2022 г. № С01-41/2022 по делу № А40-26921/2021. URL: https://www.garant.ru

12. Постановление Суда по интеллектуальным правам от 12 марта 2021 г. по делу № А40-296316/2019. URL: https://kad.arbitr.ru

13. Решение Арбитражного суда Новосибирской области от 31 мая 2022 г. по делу № А45- 35894/2021. URL: https://sudact.ru

14. Федеральная антимонопольная служба. URL: https://fas.gov.ru

15. Asta Valackienė, Stephen Yeboah. The responsibility of e-marketplaces in shaping fair e-commerce practices: a conceptual framework // Vadyba. Journal of Management. 2023. Vol. 39. No. 2. Pp. 17–19.

А. Е. Пономарченко,
старший преподаватель,
Санкт-Петербургский государственный аграрный университет

АВТОРСКИЕ ПРАВА И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: КОМУ ОНИ ПРИНАДЛЕЖАТ?

Аннотация. На сегодняшний день мы наблюдаем растущее число произведений искусства, созданных с помощью искусственного интеллекта, по мере расширения этой области и экспоненциального развития технологий. Мы видим такие примеры, как Ай-Да, робот-художник с искусственным интеллектом, музыкальные интеллекты, такие как Amper, Jukedeck и Flow Machines, Бенджамин, робот-сценарист, или даже такие работы, как «Следующий Рембрандт», все чаще присутствующие на сегодняшнем рынке и демонстрирующие различные области, в которых искусственный интеллект может создавать произведения. Цель настоящей статьи заключается в исследовании вопроса: кому в таких случаях принадлежит интеллектуальная собственность? Исследуется вопрос о необходимости внесения изменений в гражданское законодательство Российской Федерации.

Ключевые слова: искусственный интеллект, авторское право, произведение, интеллектуальная собственность, автор, юридическое лицо, владелец, робот

COPYRIGHT AND ARTIFICIAL INTELLIGENCE: WHO DOES THEY OWN?

Abstract. Today, we are seeing a growing number of works of art created with artificial intelligence as the field expands and technology advances exponentially. We see examples like Ai-Da, the AI-powered robot artist, musical intelligences like Amper, Jukedeck and Flow Machines, Benjamin, the scriptwriter robot, or even works like The Next Rembrandt increasingly featured on today's market and showcasing the various areas in which artificial intelligence can create works. The purpose of this article is to explore the question: who owns the intellectual property in such cases? The issue of the need to amend the civil legislation of the Russian Federation.

Keywords: artificial intelligence, copyright, work, intellectual property, author, legal entity, owner, robot

Введение. Благодаря ускоренному развитию технологий искусственного интеллекта (ИИ) в последние годы создание машинно-генерируемого контента стало реальностью. ИИ теперь способен создавать оригинальные произведения, такие как текст, музыка, изображения и т. д., что вызывает ряд юридических вопросов. Когда произведения искусства создаются искусственным интеллектом, алгоритмами или роботами, авторские права на такие произведения не столь очевидны. Принадлежат ли эти права ИИ или самому алгоритму, или, например, человеку, запрограммировавшему такой ИИ? На этот вопрос мы попытаемся ответить, сосредоточившись на российском законодательстве и зарубежном опыте. Важно сначала определить термин искусственный интеллект. Хотя устоявшегося определения

не существует, различные ученые пытались дать определение искусственного интеллекта, в том числе Swiss Group, которая определяет его как «объект (или коллективный набор взаимодействующих объектов), способный получать входные данные из окружающей среды, интерпретировать и учиться на таких входных данных, например, с точки зрения достижения конкретной цели или задачи» [6].

Основная часть. Искусственный интеллект относится к способности компьютерной системы обучаться и выполнять задачи, которые обычно требуют человеческого интеллекта, и может быть разделен на две основные категории: слабый ИИ и сильный ИИ. Слабый ИИ, также известный как узкий ИИ, предназначен для выполнения определенных задач на основе данных и запрограммированных алгоритмов, таких как распознавание речи, рекомендации по продукту или даже самоуправляемые транспортные средства. С другой стороны, сильный ИИ – это ИИ, обладающий когнитивными способностями, эквивалентными человеческим, и способный выполнять задачи, которые может выполнять человек. В последнее время много говорят о генеративном искусственном интеллекте – ИИ, способные создавать новый контент из существующего набора информации.

С ростом способности ИИ учиться и имитировать творческий процесс человека, создание машинного контента стало реальностью. Например, алгоритмы ИИ могут создавать тексты, стихи, сценарии фильмов и музыку, используя огромные объемы данных для изучения структуры, стиля и характеристик определенного типа работы. Кроме того, искусственный интеллект также может создавать изобразительное искусство, такое как картины и скульптуры, с использованием методов машинного обучения и нейронных сетей.

Авторское право – это отрасль права, защищающая творческие произведения, созданные человеком. Законодательство об авторском праве варьируется от страны к стране, но, как правило, дает автору исключительное право контролировать воспроизведение, распространение, выставку, публичное исполнение и т. п. Эти авторские права действуют автоматически и защищают произведения, как только они создаются в материальной форме, например, при написании текста или записи песни. Однако отсутствие ясности в законе об авторском праве на произведения, созданные ИИ, вызывает ряд этических и юридических вопросов.

Например, ИИ могут создавать работы, которые идеально имитируют существующий стиль или жанр работы, что поднимает вопрос о том, является ли это нарушением авторских прав оригинальной работы. Кроме того, тот факт, что ИИ обучаются на данных, собранных из других существующих работ, вызывает вопросы об оригинальности и плагиате работ, созданных ИИ. Другой серьезной этической проблемой является отсутствие надлежащей атрибуции истинных авторов работы, созданной ИИ. Это может привести к отсутствию реального признания и надлежащего финансового вознаграждения для тех, кто внес свой вклад в создание ИИ и алгоритмов, лежащих в его основе. Таким образом, авторское право на произведения, созданные ИИ, остается развивающейся областью, требующей пристального внимания.

В соответствии с п. 1 ст. 1225 Гражданского кодекса Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ [2] (далее – ГК РФ), произведениям

науки, литературы и искусства предоставляется правовая охрана. В соответствии со ст. 1228 ГК РФ, автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат. Следовательно, произведение должно исходить от гражданина, поскольку только физические лица могут создавать произведения, подлежащие охране авторским правом в Российской Федерации. Предпосылка человеческого вклада для получения выгоды от защиты авторских прав объясняется тем фактом, что личность автора в значительной степени присутствует в полученном произведении, и поэтому автор имеет право собственности на плоды своей работы [7].

Аналогичным образом, согласно п. «а» п. 1 статьи 3 Бернской конвенции [1], только авторы, являющиеся гражданами одной из стран Союза, пользуются защитой авторских прав на европейском уровне. Следовательно, не только юридические лица находятся за рамками европейской защиты, но и ИИ. Кроме того, Закон США об авторском праве также «явно исключает авторство не человека» [3]. Следовательно, произведения, созданные с помощью ИИ, получат защиту авторских прав только в том случае, если в процессе создания гражданин внес необходимый творческий вклад [4. С. 90].

Человеческий творческий вклад должен быть предусмотрен и отражен в итоговой работе – в произведении науки, литературы или искусства. Фактически, «творческая причинно-следственная связь» должна быть заметной между творческой работой указанного физического лица (лиц) и результирующей работой» [1]. Человеческое вмешательство должно выходить за рамки простого дизайна и программирования объекта ИИ, и его масштабы должны оцениваться в каждом конкретном случае. Швейцарская группа определила два критерия для оценки степени человеческого вмешательства: «(i) степень, в которой определение (дизайн, программирование и т. д.) кода ИИ авторами ИИ предопределяет то, какой будет новая работа; [и] (ii) возможное дальнейшее участие авторов ИИ в творческом процессе, ведущем к новой работе, помимо простого определения кода ИИ» [6].

В настоящее время в российском законодательстве не предусмотрены нормы, которые квалифицирует автора кода или программы ИИ как автора результирующей работы, поскольку их творческие решения обычно не отражаются в указанной результирующей работе. Фактически, «авторы ИИ на практике редко будут считаться авторами новой работы» [6]. Именно ценность ИИ заключается в его способности быть самодостаточным и не требовать вмешательства человека благодаря неконтролируемому обучению и машинному обучению. Авторы ИИ должны будут принять творческое решение, отраженное в новой работе, чтобы квалифицироваться как авторы указанной работы. Например, если автор ИИ специально разрабатывает свой код, чтобы ИИ рисовал изображение женщины в красном платье, потенциально это можно рассматривать как достаточную творческую причинно-следственную связь между автором ИИ и полученной работой, но это будет исследоваться в каждом конкретном случае, как упоминалось ранее. Таким образом, простого выбора данных для ИИ будет недостаточно, если только это не окажет видимого творческого влияния на итоговую работу.

Как было сказано ранее в соответствии с п. 1 ст. 1228 ГК РФ, автор произведения является гражданин, творческим трудом которого создан такой результат. Не признаются авторами результата интеллектуальной деятельности граждане, не внесшие личного творческого вклада в создание такого результата, в том числе оказавшие его автору только техническое, консультационное, организационное или материальное содействие или помощь либо только способствовавшие оформлению прав на такой результат или его использованию, а также граждане, осуществлявшие контроль за выполнением соответствующих работ. Произведения должны отражать личный отпечаток автора и его индивидуальность [5. С. 101]. Таким образом, произведение должно иметь индивидуальный и творческий характер, обусловленный вмешательством человека, чтобы иметь право на охрану авторского права. Этот элемент также не будет соответствовать произведению, созданным исключительно ИИ без вмешательства человека. Поэтому «полностью искусственное произведение» не может рассматриваться как имеющее индивидуальный и творческий характер» [8].

Однако в Швейцарии в ситуациях, когда ИИ просто используется автором произведения в качестве творческого инструмента, применяется охрана авторских прав, поскольку существует четкая идентифицируемая творческая причинно-следственная связь [6]. В музыкальной индустрии Швейцарии ИИ очень часто используется в качестве вспомогательного инструмента. В этом отношении оригинальность и творческое выражение автора по-прежнему можно было бы идентифицировать в полученном произведении, и, таким образом, оно могло бы пользоваться защитой авторских прав. Однако, как мы упоминали ранее, если автор просто запускает инструмент ИИ без какого-либо творческого вклада человека, который отражается в конечном результате, защита авторских прав не будет применяться.

Исходя из вышеизложенного можно наметить два потенциальных пути решения, кому будут принадлежать авторские права на произведения, созданные искусственным интеллектом.

1. Авторские права принадлежат владельцу ИИ. В науке преобладает мнение, что сам ИИ не может считаться автором, поскольку ему не хватает творческих способностей и правосубъектности, чтобы быть правообладателем. Вследствие этого одним из возможных решений может быть передача прав ИС, связанных с искусственно созданной работой, непосредственно владельцу ИИ, поскольку именно он программирует систему ИИ [7], что можно расценивать как авторский вклад. Это означало бы отход от концепции творческой причинно-следственной связи и строгое сосредоточение внимания на том, кто является владельцем системы ИИ. Владелец ИИ фиксирует рамки для художественного творчества ИИ и, как таковой, должен иметь возможность извлекать выгоду из плодов своего труда. Фактически, в соответствии с пунктом 3 статьи 9 Закона Великобритании об авторском праве, промышленных образцах и патентах 1988 г. (CDPA), автором компьютерного произведения «должно считаться лицо, которым приняты меры, необходимые для создания произведения» [8]. Точно так же работы, созданные ИИ, можно рассматривать как работы по найму, и, таким образом, права будут принадлежать владельцу ИИ, который заказал работу.

Если ИИ и его владелец создали совместно произведение, и мы можем разделить то, что сделал каждый из них, тогда авторские права могут принадлежать владельцу ИИ. Если вклад владельца ИИ и самого ИИ более тесно переплетен, право на авторское право на произведение зависит от того, насколько автор-человек контролировал или влиял на результаты работы ИИ.

2. Произведения, созданные технологией ИИ, не подлежат охране авторским правом. Очень интересным представляется опыт Китая. Лидерство в разработке искусственного интеллекта – это в первую очередь цель Китая, где по этому поводу было два крупных судебных процесса. В первом, известном как Feilin vs. Baidu, наблюдается тенденция: произведения, созданные ИИ должны быть отнесены к категории общественное достояние, поскольку оригинальность произведений считается недостаточной. Такой подход можно подвергнуть критике, поскольку будет препятствовать развитию новых технологий искусственного интеллекта.

Во втором деле Shenzhen Tencent v. Yingxun, окружной суд Наньшань постановил, что финансовая статья, созданная системой искусственного интеллекта, должна быть защищена авторским правом. Суд посчитал, что форма выражения отвечает требованиям интеллектуального творчества, поскольку имело место вмешательство человека в отбор, анализ и оценку информации и данных, имеющих отношение к делу, и осудил подсудимого Инсюня за нарушение авторских прав.

Таким образом, поскольку мы являемся свидетелями быстрого развития и расширения искусственного интеллекта и новых технологий, крайне важно, чтобы правовые рамки, окружающие эти области, развивались вместе с ними. Множество неопределенностей в отношении темы авторского права, права собственности и искусственного интеллекта предполагают, что для решения этих вопросов следует разработать конкретную правовую базу или, по крайней мере, добавить дополнение к существующем положения в ГК РФ. Институт интеллектуальной собственности должен развиваться одновременно с этими новыми технологиями и обеспечивать соответствующие и необходимые права ИС.

Заключение. Подводя итог вышеизложенному, отметим, что на сегодняшний день сама распространенная позиция заключается в том, что владелец ИИ считается владельцем произведения искусства, созданного ИИ. Сегодня наиболее приемлемый подход больше касается этой области, поскольку ГК РФ предусматривает, что владельцем художественного произведения является физическое лицо. Следовательно, человекоподобный робот или любой другой компьютерный художник-машинист не может быть владельцем интеллектуальной собственности на произведение искусства, поскольку они еще не получили правовой статус в российском законодательстве.

Мнение в поддержку того, что ИИ следует считать владельцем авторских прав на произведения, которые он производит, представляется применимым только при условии, что ИИ присвоен правовой статус в соответствующем законодательстве. Даже если в будущем ИИ будет предоставлена личность, мы считаем, что он может носить только символический характер, поскольку он не может заявлять о своих правах или возмещать ущерб, который он причинил.

В заключение, хотя в настоящее время в России нет четкого регулирования и судебной практики, касающихся личности ИИ, эти созданные людьми машины становятся все более и более популярными день ото дня. Поэтому интересно следить не только за развитием экосистемы ИИ, но и за меняющейся практикой судов по всему миру в отношении прав интеллектуальной и промышленной собственности.

Список литературы

1. Бернская Конвенция об охране литературных и художественных произведений (Парижский Акт, ВОИС, 24 июля 1971 г.) // Свод нормативных актов ЮНЕСКО. М., 1993. 500 с.

2. Гражданский кодекс Российской Федерации. Часть четвертая: Федеральный закон от 18.12.2006 № 230-ФЗ // Собрание законодательства Российской Федерации. 2006 г. № 52 (1 ч.). Ст. 5496.

3. Закон Соединенных Штатов Америки об авторском праве от 04 марта 1909 г. URL: https://www.copyright.gov/history/1909act.pdf

4. Протас Е. В. Правовое регулирование авторских прав на произведения, создаваемые искусственным интеллектом / Е. В. Протас, С. Е. Павлюченкова // Право и образование. 2021. № 4. С. 88–94.

5. Свиридова Е. А. Проблема определения субъекта авторских прав на произведения, созданные искусственным интеллектом / Е. А. Свиридова // Государство и право. 2021. № 2. С. 95–103.

6. Bourcier Danièle, De Filippi Primavera. Les robots seront-ils les artistes de demain. URL: https://www.latribune.fr/opinions/tribunes/les-robots-seront-ils-les-artistes-de-demain-770046.html

7. Maia Alexandre Filipe, The Legal Status of Artificially Intelligent Robots: Personhood, Taxation and Control. URL: https://ssrn.com/abstract=2985466

8. Kurki, Visa A. J., «The Legal Personhood of Artificial Intelligences», A Theory of Legal Personhood. URL: https://doi.org/10.1093/oso/9780198844037.003.0007

В. К. Раюшкин,
младший научный сотрудник,
Национальный центр законодательства
и правовых исследований Республики Беларусь

ОБРАЩЕНИЕ ВЗЫСКАНИЯ НА ПРАВА НА РЕЗУЛЬТАТЫ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ДОЛЖНИКА

Аннотация. В статье проведен анализ положений белорусского и российского законодательства об обращения взыскания на исключительные и иные права на результаты интеллектуальной деятельности и средства индивидуализации должника в исполнительном производстве. Определяется значение исключительных прав как правовой категории. Установлены существенные признаки

исключительных прав, а также проанализированы право требования по договорам об отчуждении или использовании исключительного права на объект интеллектуальной собственности, а также право использования результата интеллектуальной деятельности или средства индивидуализации. Сделан вывод об обоснованности подхода российского законодателя в вопросе отдельного от принадлежащего должнику исключительного права упоминания права требования по договорам об отчуждении или использовании исключительного права на результат интеллектуальной деятельности и средство индивидуализации, а также права использования результата интеллектуальной деятельности или средства индивидуализации, принадлежащее должнику как лицензиату. Предлагается на основе проведенного сравнительного исследования, опираясь на существующие в науке точки зрения ученых-правоведов, дополнить существующие положения белорусского законодательства в данной сфере правового регулирования.

Ключевые слова: исполнительное производство, исключительные права, интеллектуальная собственность, результаты интеллектуальной деятельности, право требования, должник, мера принудительного исполнения

FORECLOSURE OF RIGHTS TO RESULTS INTELLECTUAL ACTIVITY OF THE DEBTOR

Abstract. The article analyzes the provisions of Belarusian and Russian legislation on foreclosure of exclusive and other rights to the results of intellectual activity and means of individualizing the debtor in enforcement proceedings. The meaning of exclusive rights as a legal category is determined. The essential features of exclusive rights are established, and the right of claim under contracts for the alienation or use of an exclusive right to an object of intellectual property, as well as the right to use the result of intellectual activity or a means of individualization, are analyzed. A conclusion is made about the validity of the approach of the Russian legislator in the issue of mentioning the right of claim under contracts for the alienation or use of the exclusive right to the result of intellectual activity and a means of individualization, as well as the right to use the result of intellectual activity or a means of individualization, which belongs to the debtor as a licensee, separately from the exclusive right owned by the debtor. The article proposes, on the basis of a comparative study, based on the existing scientific points of view of legal scholars, to supplement the existing provisions of Belarusian legislation in this area of legal regulation.

Keywords: enforcement proceedings, exclusive rights, intellectual property, results of intellectual activity, right of claim, debtor, enforcement measure

Введение. На данный момент в рамках исполнительного производства Республики Беларусь происходит формирование и развитие новых мер и способов взыскательной деятельности в отношении имущества должника. Как пример такого процесса можно привести закрепленную в абз. 6 ч. 2 ст. 69 Закона

Республики Беларусь от 24 октября 2016 № 439-З «Об исполнительном производстве» (далее – Закон об ИП Республики Беларусь) норму о том, что «обращение взыскания на имущество должника, в том числе на имущественные права, а также на исключительные права на результаты интеллектуальной деятельности и средства индивидуализации является мерой принудительного исполнения, которая применяется судебным исполнителем после возбуждения исполнительного производства при принудительном исполнении исполнительного документа» [1].

Данная норма представляет особый интерес ввиду того, что является весьма новым и перспективным направлением в области правовой регламентации исполнительного производства в Республике Беларусь. Кроме того, это подтверждается тем, на сколько результаты интеллектуальной деятельности с каждым годом приобретают все более значимый вес в экономической и инновационной сферах развития государства и общества не только в нашей стране, но и в общемировом масштабе. Кроме этого, Национальный центр интеллектуальной собственности Республики Беларусь, который занимается обеспечением защиты прав на результаты интеллектуальной деятельности авторов и осуществляющий полномочия национального белорусского патентного органа, повсеместно использует информационные технологии, в том числе для осуществления договорной работы по регистрации возникновения и уступки прав на объекты интеллектуальной собственности, а также при взаимодействии с органами принудительного исполнения.

Так, построение инвестиционной экономики с переориентацией на преимущественное вложение средств в инновации, интеллектуальную собственность и другие виды нематериальных активов представляет собой в рамках Национальной стратегии устойчивого развития Республики Беларусь на период до 2035 года одну из основных целей стратегического развития Республики Беларусь. Этим же документом, задающим ориентиры развития страны более чем на десятилетие, закрепляется комплекс задач по разработке и воплощению институциональной среды, нацеленной на обеспечение создания и получение различного рода выгод и благ из нематериальных активов, к которым по смыслу данного документа относятся ноу-хау (хотя ноу-хау является объектом права интеллектуальной собственности), технологии, интеллектуальная собственность и человеческий капитал). Вдобавок предполагается, что комплекс мер и целей, установленный данной стратегией развития страны, поставит в будущем Республику Беларусь на лидирующее место в области интеллектуальной собственности среди всех государств мира [2]. Ввиду этого, считаем обоснованным закрепление в абз. 6 ч. 2 ст. 69 Закона об ИП Республики Беларусь такой меры принудительного исполнения, как обращение взыскания на исключительные права на результаты интеллектуальной деятельности и средства индивидуализации участников гражданского оборота.

Тем не менее данная формулировка не лишена и недостатков, а также, на наш взгляд, может быть расширена и дополнена.

Основная часть. В первую очередь обратимся к законодательству Российской Федерации в сфере исполнительного производства, как наиболее сходному с законодательством Республики Беларусь, в том числе и в области осуществления взыскательных мероприятий в отношении прав на результаты интеллектуальной

деятельности должника. Так, согласно п. 3 ч. 3 ст. 68 Федерального закона Российской Федерации от 2 октября 2007 № 229 «Об исполнительном производстве» (далее – Закон об ИП Российской Федерации) «обращение взыскания на исключительные права на результаты интеллектуальной деятельности и средства индивидуализации, права требования по договорам об отчуждении или использовании исключительного права на результат интеллектуальной деятельности и средство индивидуализации, право использования результата интеллектуальной деятельности или средства индивидуализации, принадлежащее должнику как лицензиату, является одной из мер принудительного исполнения, которые применяются судебным приставом-исполнителем после возбуждения исполнительного производства» [3].

Как видим из вышеизложенного, формулировка ст. 68 Закона об ИП Российской Федерации является более подробной, включающей в себя больший перечень прав, связанных с интеллектуальной собственностью, чем формулировка абз. 6 ч. 2 ст. 69 Закона об ИП Республики Беларусь.

Для большего уяснения вышеприведенных различий в формулировках представленных норм российского и белорусского законодательств об исполнительном производстве необходимо разобраться в сути такой правовой категории, как исключительные права на результаты интеллектуальной деятельности и средства индивидуализации участников гражданского оборота.

Исключительные права как юридическая конструкция относятся к категории материальных прав, причем абсолютного порядка, а свою реализацию они находят через пользование и распоряжение ими со стороны их правообладателя. Исключительное право на результаты интеллектуальной деятельности и средства индивидуализации – это отдельный уникальный вид гражданских прав, в силу своей правовой природы предоставляющий правообладателям произведением литературы, науки, искусства, средств индивидуализирующих участников гражданских правоотношений и т. д., как правообладателям объектов воплощения интеллектуальной деятельности, особое правомочие пользования, владения и распоряжения объектами интеллектуальной собственности в установленный период времени, а также на определенной территории в соответствии с положениями норм законодательства.

П. П. Баттахов выделяет следующие существенные признаки исключительных прав: «исключительность, срочность, имущественный характер, абсолютность, территориальный характер, юридические факты, которые необходимы для его возникновения, полный отрыв интеллектуальных прав в отношении объекта интеллектуальной собственности от права собственности на материальный носитель» [4].

Таким образом, уникальный статус правообладателя, в отношении результатов интеллектуальной деятельности и средств индивидуализации участников гражданского оборота обеспечивается именно его исключительными правами на объект интеллектуальной собственности. Только правообладатель имеет право по своему личному разумению использовать и разрешать другим лицам использовать свой объект интеллектуальной собственности, касательно которого он имеет

исключительное право. Исключительное право на результаты интеллектуальной деятельности может быть ограничено территориальной зоной, в которой оно зарегистрировано. Это означает, что правообладатель получает охрану только в той стране, где исключительное право на результаты интеллектуальной деятельности было зарегистрировано государством в установленном законодательством страны порядке. Исключительные права имеют ограниченный срок действия, устанавливаемый соответствующим законодательством страны в области регистрации результатов интеллектуальной деятельности и средств индивидуализации о государственной процедуре. В большинстве стран этот срок составляет от одного десятилетия, до нескольких десятилетий, в соответствии с видом интеллектуальной собственности. Исключительные права могут быть уступлены третьим лицам. Это позволяет правообладателю получать доход от результата интеллектуальной деятельности путем передачи исключительных прав, а также залога исключительных прав или предоставления лицензий и др.

Наряду с этим, права требования по договорам об отчуждении или использовании исключительного права на результат интеллектуальной деятельности и средство индивидуализации, а также право использования результата интеллектуальной деятельности или средства индивидуализации, указанные в п. 3 ч. 3 ст. 68 Закона об ИП Российской Федерации, вытекают из договорных отношений в сфере создания и использования объектов интеллектуальной собственности. В свою очередь, такие договорные отношения всецело соответствуют правилам оборотоспособности гражданских прав, закрепленных в гражданском законодательстве обоих государств. Так, согласно как белорусскому, так и российскому гражданскому законодательству в процессе осуществления правоотношений по универсальному правопреемству, к которым обычно относят реорганизацию юридических лиц и наследственные отношения, может происходить свободное отчуждение или переход гражданских прав от одного лица к другому. Доступны и другие способы, при условии, что объекты гражданских прав не изъяты из оборота и не ограничены в обороте.

В то же время С. С. Лосев справедливо относит исключительные права к автономному виду гражданских прав, которым присущ характер имущественных правоотношений, «при этом само исключительное право не является объектом гражданских прав, а является частью правового режима охраняемых результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации» [5].

На наш взгляд, раздельное указание исключительных прав, а также прав требования по договорам об отчуждении или использовании исключительного права и прав использования результата интеллектуальной деятельности или средства индивидуализации, принадлежащее должнику как лицензиату в формулировке п. 3 ч. 3 ст. 68 Закона об ИП Российской Федерации обусловлено тем, что права сторон любых гражданско-правовых договоров, к которым относятся и вышеназванные, являются по своей юридической природе обязательственными правами требования, а не исключительными правами, хоть обе эти группы гражданских прав относятся к имущественным правам.

Исходя из этого следует, что исключительное право не входит в состав обязательственных правоотношений ввиду того, что является отдельным уникальным видом гражданских прав имущественного характера. Тем самым и обусловлено отдельное от исключительного права упоминание права требования по договорам об отчуждении или использовании исключительного права на результат интеллектуальной деятельности или на средство индивидуализации, а также прав на использование результата интеллектуальной деятельности или средства индивидуализации, принадлежащее на правах лицензиара должнику.

Необходимо разобраться в основных чертах договора уступки исключительного права и лицензионного договора. Договор уступки является по своей природе гражданско-правовым договором, а значит предполагает возникновение, изменение или прекращение гражданских прав и обязанностей. Данный тип гражданско-правового договора опосредует полную передачу от одной стороны, принадлежащих ей прав на объекты интеллектуальной собственности и средства индивидуализации участников гражданского договора, товаров, работ или услуг, указанные в договоре, другой стороне. Лицензионный договор также является гражданско-правовым по своей правовой природе, однако имеет свои характерные особенности, отличающие его от договора уступки. Лицензиар, обладающий исключительным правом в отношении результата интеллектуальной деятельности, передает лицензиату (лицу, которое получает данное право) правомочие на использование конкретным, определенным в договоре способом, результаты интеллектуальной деятельности.

Отсюда следует, что должником в правоотношении о применении взыскания в отношении исключительных прав на объект интеллектуальной собственности является правообладатель результата интеллектуальной деятельности самолично, а получившее право требование в рамках договорных правоотношений об отчуждении или использовании данного исключительного права на продукты интеллектуальной деятельности и средства, индивидуализирующие участников рыночных отношений, лицо является должником при взыскании, нацеленном на права требования по договорам такой категории. При осуществлении взыскательных мер в отношении прав использования результата интеллектуальной деятельности или средства индивидуализации, возникшее как следствие заключения лицензионного договора, должником является лицензиат.

Таким образом, благодаря в достаточной мере широкой формулировке такой нормы российского законодательства об исполнительном производстве дополнен перечень лиц, которых судебные приставы-исполнители могут отнести к должникам, на исключительные и обязательственные права в области результатов интеллектуальной деятельности которых может быть обращено взыскание.

Согласно статистическим данным Национального центра интеллектуальной собственности Республики Беларусь в 2022 г. «всего было зарегистрировано 898 договоров о передаче и предоставлении прав на объекты права промышленной собственности (увеличение на 18,5 % по сравнению с 2021 г. – 758 договоров). Из них лицензионных договоров о предоставлении прав использования объектов права промышленной собственности за 2022 г. было заключено больше на

46,7 % по сравнению с 2021 г.» [6]. Такие статистические данные свидетельствуют о положительной динамике увеличения количества лиц, обладающих правами требования по договорам о передаче и предоставлении прав на объекты права промышленной собственности.

При обращении к статистическим данным Российской Федерации становится возможным проследить тенденцию ежегодного увеличения количества запросов в Федеральную службу по интеллектуальной собственности Российской Федерации из Федеральной службы судебных приставов Российской Федерации. Так, количество обращений и запросов Федеральной службы судебных приставов Российской Федерации в Федеральную службу по интеллектуальной собственности Российской Федерации составило: «в 2019 г. – 1 857 обращений, в 2020 г. – 2 029 обращений, в 2021 г. – 3 115 обращений» [7]. Целями обращений и запросов были: «предоставление информации о наличии зарегистрированных объектов интеллектуальной собственности, предоставление информации о наличии обеспечительных мер на объекты интеллектуальной собственности, наложение ареста на объекты интеллектуальной собственности, снятие ареста с объектов интеллектуальной собственности, предоставление сведений и документов о распоряжении правами на объекты интеллектуальной собственности» [7]. Как видим, предоставление сведений и документов о распоряжении правами на объекты интеллектуальной собственности, в качестве одной из целей обращений и запросов Федеральной службы судебных приставов Российской Федерации в Федеральную службу по интеллектуальной собственности Российской Федерации, свидетельствует о фактическом применении на практике судебными приставами-исполнителями нормы об обращении взыскания на права требования по договорам об отчуждении или использовании исключительного права на результат интеллектуальной деятельности и средство индивидуализации и право использования результата интеллектуальной деятельности или средства индивидуализации, принадлежащее должнику как лицензиату в качестве мер принудительного исполнения.

Заключение. В результате проведенного исследования, считаем необходимым, в развитие уже существующих положений об обращении взыскания на исключительные права на результаты интеллектуальной деятельности и средства индивидуализации должника в рамках исполнительного производства в Республике Беларусь, учесть положительный опыт Российской Федерации в вопросах правовой регламентации такой меры принудительного исполнения и внести изменения в Закон об ИП Республики Беларусь относительно предмета данного исследования, а именно, предлагаем изложить абз. 6 ч. 2 ст. 69 Закона об ИП Республики Беларусь в следующей редакции:

(Мерами принудительного исполнения являются:)

«обращение взыскания на имущество должника, в том числе на имущественные права, а также на исключительные права на результаты интеллектуальной деятельности и средства индивидуализации, права требования по договорам об уступке исключительного права на результат интеллектуальной деятельности и средство индивидуализации, право использования результата интеллектуальной

деятельности или средства индивидуализации, принадлежащее должнику как лицензиату;».

Список литературы

1. Об исполнительном производстве [Электронный ресурс]: Закон Респ. Беларусь, 24 окт. 2016 г. № 439-З // ЭТАЛОН. Законодательство республики Беларусь / нац. Центр правовой информ. Респ. Беларусь. Минск, 2023.

2. Национальная стратегия устойчивого развития Республики Беларусь на период до 2035 года. URL: https://clck.ru/36p4BQ

3. Федеральный закон «Об исполнительном производстве» от 02.10.2007 № 229-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_71450

4. Баттахов П. П. Существенные признаки исключительных прав в сфере права интеллектуальной собственности // Право и государство: теория и практика. 2018. № 2(158). С. 63–66.

5. Лосев С. С. О понятии исключительного права. URL: enter.gov.by/articleLosev2.html

6. Годовой отчет Национального центра интеллектуальной собственности за 2022 год. URL: https://clck.ru/36p4Cy

7. Годовой отчет Федеральной службы по интеллектуальной собственности за 2021 год. URL: https://clck.ru/bkwPX

Т. В. Рехачева,
преподаватель,
Омский государственный университет
имени Ф. М. Достоевского

РЕГИОНАЛЬНАЯ МЕДИЦИНСКАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ОМСКОЙ ОБЛАСТИ

Аннотация. Статья посвящена анализу постановления «О государственной информационной системе в сфере здравоохранения Омской области». Рассматривается порядок создания региональной медицинской информационной системы Омской области, анализируются пункты положения, определяются нормы, вызывающие трудности правоприменения и описываются предложения по устранению возникших коллизий. В заключение определяется место региональной медицинской информационной системы в системе актов Омской области.

Ключевые слова: право, медицинское право, информационное право, цифровые технологии, информационная система, региональная медицинская информационная система

THE REGIONAL MEDICAL INFORMATION SYSTEM OF OMSK REGION

Abstract. The article analyzes the Omsk's government decree «On the state information system of health care of Omsk region». The article addressees the procedure

of creation of the regional medical information system of Omsk region, analyzes the legal provisions, identifies provisions that may cause difficulties in law enforcement and describes proposals for them elimination. In the summary, the author determines place of the regional medical information system in the system of acts of the Omsk region.

Keywords: law, medical law, information law, digital technologies, information system, regional medical information system

Введение. В августе 2023 года Правительством Омской области было принято постановление «О государственной информационной системе в сфере здравоохранения Омской области» [2]. Хотя ранее о внедрении региональной медицинской информационной системы Омской области (далее – РМИС Омской области) упоминалось в постановлении Правительства Омской области 2016 года [8], в распоряжении правительства Омской области 2019 года и в распоряжении Правительства Омской области 2022 года [4], но юридическое закрепление получила только в этом году.

Данная система не является уникальной на территории Российской Федерации, в отдельных субъектах уже успешной функционируют подобные программы. Например, в Нижегородской области РМИС уже действует. Стратегию приняли в 2018 году, поэтому к настоящему времени уже есть определенные успехи, вроде реализации подсистемы «Программно-технических комплексов удаленных телемедицинских консультаций медицинских учреждений» (СПТК УТК МУ), и создания центрального архива медицинских изображений (ЦАМИ) [10].

В Нижегородской области в РМИС интегрировано уже 137 учреждений [7], которые обеспечивают персонифицированный учет оказанной медицинской помощи, работу электронной регистратуры, формирование отчетности и управление взаиморасчетами за оказанную медицинскую помощь, а к концу 2023 года планируется подключение всех медицинских учреждений к РМИС Нижегородской области.

Основная часть. В Омской области постановление о создании РМИС появилось лишь в 2023 году. В документе не называется конкретных сроков создания РМИС: пункт 1 говорит только о создании, пункт 2 – об утверждении положения о РМИС Омской области, пункт 3 устанавливает оператора РМИС, пункт 4 определяет сведения и порядок ежегодного отчета о работе системы, а пункт 5 возлагает контроль за исполнением постановления на Министра труда и социального развития Омской области. В то же время в постановлении Правительства Российской Федерации от 09.02.2022 № 140 «О единой государственной информационной системе в сфере здравоохранения» [3] в пункте 4 указывается срок вступления в силу положения и срок его действия. Положение о ГИС Здравоохранение действуют до 1 марта 2028 года.

Отсутствие четкого срока создания РМИС в Омской области может породить проблемы в правоприменении и создать коллизии. Например, региональная программа Омской области по здравоохранению 2022 г. предполагала внедрение автоматизации процессов управления качеством и контроля качества оказания медицинской помощи по медицинской реабилитации на основе данных электронной

медицинской карты пациента в региональной медицинской информационной системе с 01.07.2023 по 31.12.2024 путем модернизации и автоматизации в действующей РМИС процессов управления качеством и контроля качества оказания медицинской помощи по медицинской реабилитации [4].

Другая региональная программа к 2024 г. планирует снижение младенческой смертности до 5,6 новорожденных на 1 000 родившихся живыми, этот показатель будет достигнут путем организации и проведения мониторинга состояния здоровья беременных женщин с использованием модулей региональной медицинской информационной системы «Мониторинг беременных» [5].

До 17 августа 2023 года в Омской области отсутствовал нормативный акт, регулирующий работу РМИС, поэтому говорить о высокой эффективности функционирования систем до этого времени не приходится.

Положение определяет назначение РМИС Омской области, ее задачи и функции, порядок взаимодействия с медицинскими информационными системами и иными информационными системами, участников информационного взаимодействия, порядок и сроки предоставления информации, порядок доступа и порядок защиты информации.

Система была разработана на основе раздела III «Требования к ГИС субъектов Российской Федерации» приказа Минздрава России от 24.12.2018 N 911н [11] и не противоречит ему.

Правительство Омской области ставит перед РМИС восемь основных задач, которые реализуют функции, указанные в Постановлении Правительства Российской Федерации № 447 [9]. Тем не менее количество задач РМИС Омской области может быть увеличено, например за счет ведения реестра медицинских работников, который существует при федеральной ГИС Здравоохранение.

Принятое Постановление Правительства Омской области № 443 совместно с положением содержит ряд пунктов, вызывающих вопросы с точки зрения правоприменения.

Пункт 10, содержащий структуру РМИС Омской области является отсылочным, поскольку «перечень подсистем Системы с указанием их назначения и функций совместно с перечнем реализованных функциональных возможностей и процессов в разрезе подсистем Системы ведется в составе реестра оператора Системы «Состав единого цифрового контура в здравоохранении Омской области»» [2]. В настоящий момент подобный перечень отсутствует, хотя выше уже упоминались как минимум две возможные подсистемы, а в Постановлении Правительства Российской Федерации № 140 перечислены все подсистемы, которые входят в единую государственную информационную систему в сфере здравоохранения, например подсистема ведения реестров лекарственных препаратов для медицинского применения или федеральная электронная регистратура.

Пункт 15 обязывает медицинские организации, подведомственные уполномоченному органу, передавать информацию в полном объеме по всем источникам финансирования и по всем случаям оказания медицинской помощи любым категориям пациентов [2]. Наличие подобного пункта подразумевает необходимость изменения формы согласия на обработку персональных данных, добавлением

пункта, согласно которому медицинские организации имеют права передавать персональные данные граждан, а также результаты их обследования третьим лицам, иначе подобная передача невозможна. Более того само предоставление информации о случаях оказания медицинской помощи любым категориям пациентов противоречит пункту 1 части 13 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» [6], сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну.

Пункт 21 о порядке и сроках предоставления информации в РМИС Омской области четко не определен, а содержит отсылочное положение, поскольку порядок и сроки определяет оператор Системы по согласованию с уполномоченным органом в реестре оператора Системы «Состав информации, размещаемой в РМИС Омской области». Постановление Правительства Омской области № 443 было принято недавно и точные сроки создания РМИС не определены, поэтому в настоящее время можно говорить, что это норма является мертвой.

Подпункт 6 статьи 41 обязывает РМИС Омской области функционировать в бесперебойном круглосуточном режиме, за исключением установленных периодов проведения работ по обслуживанию информационных систем и устранению неисправностей в работе, суммарная длительность которых не должна превышать 4-х часов в месяц (за исключением перерывов, связанных с обстоятельствами непреодолимой силы), но при этом никакой ответственности за неисполнение данного положение на оператора не возлагается.

Пункт 50 посвящен защите информации, содержит типовые положения и полностью возлагается на оператора РМИС Омской области. Однако пользователями системы, согласно пункту 30 являются: уполномоченный орган; оператор Системы; медицинские организации; фармацевтические организации в Омской области; территориальный фонд обязательного медицинского страхования Омской области; организации, являющиеся операторами иных информационных систем; граждане и органы исполнительной власти Омской области на основании соглашения об информационном взаимодействии. Утечка информации возможно не только от оператора РМИС Омской области, но и от других пользователей, которым не вменяется в обязанность защита персональных данных [2].

Однако несмотря на ряд спорных пунктов, акт содержит несколько хорошо проработанных положений о РМИС Омской области.

Пункт 27 об обязанностях оператора РМИС Омской области содержит 33 требования, охватывающих довольно широкий спектр обязательств, от функционирования всей системы и порядка доступа к личному кабинету иных пользователей до технической поддержки и ликвидации последствий компьютерных атак.

Пункт 33 о доступе к информации в РМИС Омской области осуществляется с помощью единой системы идентификации и аутентификации; квалифицированного сертификата ключа проверки электронной подписи; и уникального логина и пароля в соответствии с установленными оператором правами доступа. Использование всех трех способов защиты значительно повышает безопасность

РМИС, поскольку основывается на современных технологиях, которые затрудняют несанкционированное получение доступа. Конечно, от полной утечки информации данные способы не защитят, ведь сотрудник может просто сфотографировать экран компьютера с необходимой информацией, однако наличие сразу трех способов защиты говорит о том, что Правительство Омской области считает данную проблему серьезной и уделяет ей особое внимание. Дальнейшее описание порядка доступа подробно регламентировано, как и требования к программно-техническим средствам. Для всех информационных систем информационных систем, и РМИС Омская область исключением не является, обязательно нахождение серверов на территории Российской Федерации, не обязательно в пределах региона, где данная система эксплуатируется [2].

Заключение. Исходя из анализа положений, принятое постановление в первую очередь нацелено на систематизацию отдельных информационных систем медицинских учреждений, их информационное взаимодействие, сбор, хранение, обмен и представление медицинской документации и сведений в форме электронных документов и электронных медицинских записей, обеспечение электронного медицинского документооборота между медицинскими организациями [2].

Говорить об информировании граждан в новой системе РМИС Омской области пока рано, поскольку в настоящее время многие не знают даже о возможности записи к врачу» или получения информации об оказанных медицинских услугах и их стоимости через портал «Госулуги, поэтому для выполнения задач по информированию населения по вопросам охраны здоровья и ведения здорового образа жизни и обеспечению доступа граждан к услугам в сфере здравоохранения в электронной форме необходимо приложить усилия. Последнее становится еще более актуальным, поскольку с 1 сентября 2024 года обязательно ведение медицинских книжек только в электронном варианте [1].

В завершении необходимо отметить, что несмотря на ряд вопросов к принятому постановлению и положению, Омская область создает РМИС, который закроет одну из существующих правовых лакун на региональном уровне и даст возможность совершенствованию цифрового и информационного регулирования в сфере здравоохранения.

Список литературы

1. О внесении изменений в приказ Министерства здравоохранения Российской Федерации от 18 февраля 2022 г. № 90н «Об утверждении формы, порядка ведения отчетности, учета и выдачи работникам личных медицинских книжек, в том числе в форме электронного документа» // СПС КонсультантПлюс.

2. О государственной информационной системе в сфере здравоохранения Омской области «Региональная медицинская информационная система Омской области» (вместе с «Положением о государственной информационной системе в сфере здравоохранения Омской области «Региональная медицинская информационная система Омской области»): Постановление Правительства Омской области от 17.08.2023 № 443-п. // СПС КонсультантПлюс.

3. О единой государственной информационной системе в сфере здравоохранения (вместе с «Положением о единой государственной информационной системе в сфере здравоохранения»): Постановление Правительства РФ от 09.02.2022 № 140 // СПС КонсультантПлюс.

4. О региональной программе Омской области Оптимальная для восстановления здоровья медицинская реабилитация в Омской области: Распоряжение Правительства Омской области от 31.05.2022 № 100-рп // СПС КонсультантПлюс.

5. О региональной программе Омской области «Программа развития детского здравоохранения Омской области, включая создание современной инфраструктуры оказания медицинской помощи детям: Распоряжение Правительства Омской области от 27.06.2019 № 114-рп // СПС КонсультантПлюс.

6. Об основах охраны здоровья граждан в Российской Федерации: Федеральный закон от 21.11.2011 № 323-ФЗ // СПС КонсультантПлюс.

7. Об утверждении Государственной программы «Развитие здравоохранения Нижегородской области: Постановление Правительства Нижегородской области от 26.04.2013 № 274 // СПС КонсультантПлюс.

8. Об утверждении государственной программы Омской области «Информационное общество Омской области: Постановление Правительства Омской области от 15.10.2013 № 253-п // СПС КонсультантПлюс.

9. Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями: Постановление Правительства РФ от 12.04.2018 № 447 // СПС КонсультантПлюс.

10. Об утверждении Стратегии социально-экономического развития Нижегородской области до 2035 года: Постановление Правительства Нижегородской области от 21.12.2018 № 889 // СПС КонсультантПлюс.

11. Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций» (Зарегистрировано в Минюсте России 19.06.2019 N 54963): Приказ Минздрава России от 24.12.2018 № 911н // СПС КонсультантПлюс.

М. А. Садиков,
старший преподаватель,
Ташкентский государственный юридический университет

РАЗВИТИЕ LEGAL TECH В УЗБЕКИСТАНЕ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Аннотация. В статье приводится правовой и организационный анализ, а также развитие Legal tech в Узбекистане. Отмечаются существующие проблемы

и перспективы в развитии Legal tech в Республике Узбекистан. Кроме того, особое место в научной работе отводится новому визовому исследованию и обучению студентов по теоретико-правовым наукам в связи с цифровизацией общества. Сделанные предложения направлены на устранения актуальных проблем и развития Legal tech в Узбекистане.

Ключевые слова: право, Legal tech, обучение, цифровизация, проблемы, перспективы

DEVELOPMENT OF LEGAL TECH IN UZBEKISTAN: PROBLEMS AND PROSPECTS

Abstract. The article provides a legal and organizational analysis, as well as the development of Legal tech in Uzbekistan. The existing problems and prospects in the development of Legal tech in the Republic of Uzbekistan are noted. In addition, a special place in scientific work is given to a new visa study and teaching students in theoretical and legal sciences in connection with the digitalization of society. The proposals voiced in the scientific article are aimed at eliminating actual problems and developing Legal tech in Uzbekistan using the experience of developed countries.

Keywords: Legal tech, law, training, digitalization, problems, prospects

Цифровизация общественных процессов стала объективным требованием которому все подчиняются без исключения. Государства и правительства, осознающие необходимость перехода к цифровизации важнейших сфер деятельности в правовой сфере в течении небольшого времени, объективно вырвутся в число развитых во всех сферах жизнедеятельности стран, такова правда истории. Так как актуальность цифровизации экономики и социальной сфере очевидна, приведем факты из практики Узбекистана. В нашей стране в цифровой формат переведено 370 из 715 государственных услуг, в прошлом году электронными услугами воспользовались 12 миллионов человек. В результате цифровизации отменено истребование от населения более 70 видов справок и документов [1].

В Узбекистане 2020 г. был объявлен «Годом развития науки, просвещения и цифровой экономики». С этого года были приняты основополагающие правовые акты, которые являются фундаментом цифровых реформ в нашей стране.

В 28 апреля 2020 г. было принято Постановление Президента Республики Узбекистана «О мерах по широкому внедрению цифровой экономики и электронного правительства». В акте Президента определены актуальные вопросы, связанные с внедрением цифровых технологий в деятельности как государственных, так и негосударственных учреждений. Кроме того, 5 октября 2020 г. был принят Указ Президента Республики Узбекистан «Об утверждении Стратегии «Цифровой Узбекистан – 2030» и мерах по ее эффективной реализации». Данный документ включает в себя «дорожные карты» по цифровой трансформации приоритетных экономических отраслей и регионов [2].

В целях дальнейшего совершенствования деятельности органов и учреждения юстиции по качественной организации единой государственной правовой

политики 19 мая 2020 г. было принято Указ Президента Республики Узбекистан «О мерах по дальнейшему совершенствованию деятельности органов и учреждений юстиции в реализации государственной правовой политики» [3].

Согласно Указа Президента Республики Узбекистан от 29.04.2020 «О дополнительных мерах по кардинальному совершенствованию юридического образования и науки в Республике Узбекистан» в Ташкентском государственном юридическом университете создана лаборатория Legal Tech.

Данное учреждение служит центром бизнес-инкубации и акселерации стартап-проектов в университете. Лаборатория постоянно следит за развитием и достижениями в области информационных технологий, включая технические решения, которые могут быть использованы при разработке информационных и правовых технологий и систем; обеспечении развития информационных и правовых технологий. Цель данной лаборатории – пробудить интерес студентов к информационным технологиям и системам и привлечь их к этой области.

С этой целью студенты, докторанты и независимые соискатели ТГЮУ участвуют в конкурсах новых стартапов «Лучший инновационный проект», «Самый молодой ученый» и «Лучшая независимая работа», «Лучший творческий подход», «Лучшая инновационная идея» и «Конкурсы в номинации «Инновационное образование». В конкурсах приняли участие более 40 работ.

Все работы подробно обсуждались и определялись победители в каждой номинации. В конкурсе участвовали проекты на общую сумму 550 млн сум, такие как: «Укрепи свою жизнь правом!», «Transfers», «ID on the phone», «MyLaw», «Рынок онлайн-юридических консультаций», «Unistore.uz», «Kazus.uz» и Legally24.Uz.

Для реализации этих проектов созданы веб-платформа и мобильное приложение «Legal City». 7 октября 2020 года состоялась презентация веб-платформы. Мобильное приложение размещено на платформе Google Play Market и доступно для скачивания.

В настоящее время ведется работа по эффективной реализации стартап-проектов. Для привлечения студентов к этой деятельности и формирования проектных групп в соответствии с портфолио стартапов на официальном сайте ТГЮУ и в социальных сетях были размещены объявления. В результате сформирована база резидентов лаборатории, состоящая из более чем 40 студентов [4].

В августе 2022 года Министерство юстиции Республики Узбекистан запустил новый проект для «юридического самообслуживания». Сервис находится по адресу yurxizmat.uz. На портале доступны более 800 образцов договоров, обращений, заявлений и других юридических документов – как корпоративных, так и для физических лиц. Все документы можно заполнить нужными данными онлайн. Благодаря сервису граждане и предприниматели смогут подготавливать необходимые документы без участия юристов и адвокатов. Все образцы на сайте доступны бесплатно [5].

Республики Узбекистан утверждена стратегия «Цифровой Узбекистан 2030» и меры по ее эффективной реализации. Во всех госучреждениях всех отраслей экономики активно внедряются цифровые технологии. К системе Цифрового правительства подключены более 100 информационных систем. Системы,

разработанные Центром цифрового правительства, такие как Система биллинга, Межведомственная информационная платформа, One ID и другие играют огромную роль в цифровизации всех сфер Узбекистана [6].

В связи с тем, что за последнее 5 лет в Узбекистане наблюдается гражданская активность, портал коллективных обращений «Mening fikrim» – «Мое мнение» (meningfikrim.uz), стал новым толчком при организации выдвижении гражданских инициатив. Благодаря этому механизму активные граждане и общественные организации могут стать инициаторами решения различных проблем. Таким образом, на деле будет реализован принцип «Важнейшие решения, касающиеся жизни страны, принимаются на основе непосредственного диалога» [7].

Несмотря на то, что многое проделано в Республике Узбекистан для развития Legal Tech сферы, все же существует ряд проблем, препятствующих развитию этой сферы в нашей стране. Самое значительное среди этих проблем – это огосударствление цифровизации. Государство в основном уделяет особое значение на работу по реформирование в сфере цифровизации. Соответственно, нужно отметить практическое отсутствие конкуренции Legal Tech рынка. Все крупные платформы разработаны государственными учреждениями [8].

Далее немаловажным фактом является отсутствие наложенной взаимосвязи между специалистами информационных технологий и юристов. Поскольку проекты в области правовой практики не рентабельны как коммерческие, по этой причине, специалисты не берутся за это дело.

Отсутствие единой системы взаимосвязи между компетентными органами по разработке Legal Tech проектов тормозит усовершенствование данной сферы. Существующие центры по разработке цифровых продуктов не получают заказов в области Legal Tech. Каждое государственное учреждение разрабатывает собственный проект, исходя из своих функций, что приводит частым коллизиям между ними. В результате гражданам от использования подобных продуктов, явно становится неудобно. Примером может послужить, заявление на подключение холодной воды, которое подается через центр единых интерактивных услуг. Заявление к водоканалу приходит не сразу. Поступившее заявление обрабатывается заново, далее, соответственно, принятие решения занимает еще определенный срок, в итоге, если раньше данная услуга оказывалась в течение максимум двух дней, затягивается на недельный срок.

Пожалуй, самой главной проблемой развития Legal Tech в Узбекистане является отсутствие частных компаний по разработке подобных проектов. Тем не менее существует огромный рынок, который еще не освоен в сфере оказания юридических услуг. Примером может послужить элементарное обжалование штрафов за нарушение ПДД. Электронные протоколы приходят нарушителям позже установленного срока обжалования или срока, по которому можно было получить скидку со стороны государства за досрочную опалу штрафа. В результате практически все платят штрафы в полной мере.

Все это причина того, что правовая практика не тесно связана с юридическим образованием. Как наблюдается, в вузах и университетах страны до сих пор нет новых направлений по подготовке специалистов юристов, ориентированных в области цифровой экономики и цифровой юридической практики [9].

Далее нужно отметить, что в Узбекистане запущены крупные проекты с использованием цифровых технологий, с помощью которых граждане проявляют свою гражданскую активность. Речь идет о таких проектах, как meningfikrim.uz, а также openbudget.uz.

Если будем говорить о проекте meningfikrim.uz, то суть проекта проявляется в том, что с помощью этого портала граждане могут подать обращения по разным актуальным вопросам жизни общества. Инициативы, получившие достаточное количество поддержек со стороны общественности, будут рассмотрены органами законодательной власти республики. Первым «на финише» оказалась инициатива о разрешении тонировки для частных автомашин. Это обращение набрало более 11 900 голосов. Голосования по данной петиции были прекращены менее чем за месяц [9].

Следующий проект, так называемый openbudget.uz «Инициативный бюджет». На сегодняшний день за 33,6 тысячи представленных проектов свои голоса отдали уже более 10 миллионов человек. Однако, во многих густонаселенных районах можно увидеть людей, которые стоят на улице и «вылавливают» из толпы людей и просят их проголосовать за их проект. Вот таким вот образом граждане набирают голоса. Взамен они предлагают напитки или же небольшой денежный бонус. Выяснилось, что жители махалли из Дехканабадского района Кашкадарьинской области для того, чтобы добиться нового асфальта возле домов, готовы были потратить около 200 миллионов сумов из собственных денежных средств, когда как сам проект с асфальтированием обойдется в 1 миллиард сумов [10].

Приведенные проекты отражают тенденцию в Узбекистане в сфере гражданской активности, данное явление должно исследоваться юридической наукой, и при подготовке будущих юристов следует учитывать данные изменения в обществе.

Список литературы

1. Обсуждены задачи в сфере информационных технологий. URL: https://president.uz/ru/lists/view/5943

2. Новый цифровой Узбекистан: цели, задачи, перспективы. URL: https://mitc.uz/ru/news/3050

3. Национальная база данных законодательства Республики Узбекистан. URL: www.lex.uz

4. О лаборатории «Legal Tech» Центра правовых инициатив и инноваций Ташкентского государственного юридического университета. URL: https://tsul.uz/ru/general-page/laboratoriya-Legal-Tech

5. Заработал портал «юридического самообслуживания» от Минюста. URL: https://www.spot.uz/ru/2022/08/26/yurxizmat

6. Из 35 миллиона населения проживающих в Узбекистане, более 64 % являются пользователями сети интернет. URL: https://e-gov.uz/ru

7. Сегодня будет запущен портал коллективного обращения граждан. URL: https://uzreport.news/society/segodnya-budet-zapushen-portal-kollektivnogo-obrasheniya-grajdan

8. Садиков М. А. “Legal tech” в современной юридической практике. URL: https://tadqiqot.uz/index.php/law/article/download/179/168

9. Петиция за разрешение тонировки собрала более 9 тысяч подписей. URL: https://uz.sputniknews.ru/20180522/Peticiya-tonirovka-8280931.html
10. Открытый бюджет превратился в позорный бюджет. URL: https://upl.uz/policy/32504-news.html

Г. А. Саубанова,
следователь,
Отдел Министерства внутренних дел Российской Федерации
по Зеленодольскому району

ХИЩЕНИЕ ДЕНЕЖНЫХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: ВОПРОСЫ КВАЛИФИКАЦИИ

Аннотация. В статье рассматриваются вопросы квалификации хищения денежных средств с использованием информационно-телекоммуникационных технологий. Современные технологии предоставляют новые возможности для совершения мошеннических действий и краж, что создает необходимость в разработке и усовершенствовании методов определения и пресечения таких преступлений. Освещаются основные проблемы, связанные с квалификацией преступлений данного вида, а также предлагаются пути решения проблемы и обеспечения эффективной борьбы с хищением денежных средств с использованием информационно-телекоммуникационных технологий.

Ключевые слова: хищение денежных средств, информационно-телекоммуникационные технологии, мошенничество, кража, преступления, квалификация, статистика, расследование, оперативно-розыскные мероприятия

THEFT OF MONEY WITH THE USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES: QUALIFICATION ISSUES

Abstract. This article deals with the issues of qualification of theft of funds with the use of information and telecommunication technologies. Modern technologies provide new opportunities for committing fraudulent actions and thefts, which creates the need to develop and improvement of methods of determination and suppression of such crimes. The article highlights the main problems associated with the qualification of crimes of this type, as well as proposed ways of solving the problem and providing an effective fight against theft of funds using information and telecommunication technologies.

Keywords: embezzlement of funds, information and telecommunication technologies, fraud, theft, crime, qualification, statistics, investigation, operational and investigative measures

На сегодняшний день в России участились случаи совершения хищений денежных средств с использованием информационно-телекоммуникационных

технологий (далее – ИТТ). Данный вид преступлений становится все более распространенным благодаря развитию Интернета, электронной коммерции и цифровых технологий. Многие люди предпочитают совершать покупки онлайн, оплачивать счета и осуществлять финансовые операции через мобильные приложения, что стало не только удобным, но и предоставляет новые возможности для киберпреступников [2].

Как отметил президент Российской Федерации В. В. Путин на расширенном заседании коллегии Министерства внутренних дел (далее – МВД), состоявшемся 20 марта 2023 г., число преступлений в ИТТ-сфере составили четверть от всех уголовных правонарушений в России в 2022 г., превысив полмиллиона. Глава государства добавил, что борьба с преступностью с использованием информационных технологий – один из безусловных приоритетов работы МВД России. Согласно статистическим данным ГИАЦ МВД России в январе-июне 2023 г. количество преступлений, совершенных с использованием ИТТ стало больше на 27,9 % по сравнению с прошлым годом. За указанный отчетный период всего зарегистрировано 318 466 преступлений. Из которых большая часть совершается с использованием сети «Интернет» и средств мобильной связи. [6] Наиболее часто регистрируются преступления, связанные с хищением денежных средств с банковских счетов потерпевших, ответственность за которое наступает по ст. 158 Уголовного Кодекса Российской Федерации (далее – УК РФ), и мошенничества по ст. 159, 159.3, 159.6 УК РФ [7].

Вопрос квалификации данной категории преступлений является одной из ключевых проблем уголовного права. Проблема заключается в том, что квалификация преступления напрямую влияет на определение наказания и меры пресечения. Квалификация может быть основана на целом ряде факторов, таких как умысел, характер причиненного вреда, обстоятельства и способ совершения преступления.

Развитие IT-технологий предоставил новые возможности для совершения преступлений, что является серьезной угрозой для финансовой безопасности банков, организаций и отдельных лиц. Все это сказывается на многих сферах жизни общества, в том числе экономической системы государства, в которую входит экономическая безопасность. В связи с этим актуальным является вопрос квалификации данных преступлений и разработка эффективных мер по их предотвращению и пресечению.

Для определения правильной квалификации преступления и успешного расследования киберпреступлений немалую роль играет проведение качественных безотлагательных оперативно-розыскных мероприятий.

Изучение правовых аспектов, связанных с киберпреступлениями, включая разработку эффективного законодательства, а также анализ подходов правоохранительных органов к расследованию и предотвращению киберпреступлений является важным направлением научных исследований в современной науке.

Так, 14 августа 2023 года на общественное обсуждение был представлен законопроект Федерального закона «О внесении изменения в статью 6 Федерального закона «Об оперативно-розыскной деятельности», в котором предлагается внести

новый вид оперативно-розыскных мероприятий, предусматривающих проведение исследования информации, в том числе содержащейся в технологических системах ее передачи, включая информационно-телекоммуникационную сеть «Интернет». Законопроект направлен на совершенствование деятельности по выявлению, пресечению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-коммуникационных технологий, что позволит в режиме реального времени, исследовать разрозненные компьютерные данные, включающие в себя не только текстовую, аудио- и/или видеоинформацию, но также технические данные о событии, времени, месте удаленного подключения к информационным ресурсам, используемом оборудовании, включая его модель, сетевой и физический адрес, серийный номер, а также о взаимодействии пользователя с информационными системами и их реакции на запросы пользователей в определенный период времени [14].

Нельзя не согласиться с предложенными изменениями в указанный Федеральный закон, так как действительно расследование большинства совершенных противоправных деяний начинается с проведения оперативно-розыскных мероприятий. Эти мероприятия проводятся для обеспечения наиболее полного и объективного выявления всех обстоятельств противоправного деяния. Киберпреступления часто оставляют цифровые следы, которые могут быть использованы в качестве доказательств. Оперативно-розыскные мероприятия помогают сохранить эти цифровые следы, проанализировать их и использовать в судебном процессе для установления фактов и обстоятельств преступления.

С учетом сложности данной категории преступлений имеется смысл применять при получении и сборе информации технологии искусственного интеллекта (далее – ИИ), которые как указано в работе М. С. Спиридонова будут проводить определенную обработку сведений и данных, имеющих существенное значение для расследования, и которые в дальнейшем могут быть оформлены в качестве доказательства по уголовному делу. [13].

Того же мнения придерживается Е. Ю. Антонова, говоря о важности использования ИИ оперативно-разыскными подразделениями (например, система распознавания лиц, идентификация личности, номеров транспортных средств, мониторинг социальных сетей и т. д.) [17].

Основные сложности при определении квалификации у следственных и судебных органов возникают при разграничении кражи и мошенничества в сфере компьютерной информации. В большей степени это связано с отсутствием физического объекта, который можно украсть. Вместо этого речь идет о несанкционированном доступе к данным или компьютерным системам, использовании чужой информации без разрешения в криминальных целях.

В российском уголовном законодательстве существует только поверхностное отражение регулирования киберпреступлений (глава 28 УК РФ «Преступления в сфере компьютерной информации» и статьи, расположенные хаотично в разных разделах УК РФ, что затрудняет их систематизацию и понимание) [15].

В науке уголовного права вопросу квалификации придается большое значение, поскольку правильная юридическая оценка совершенного лицом деяния

является необходимым условием достижения законности при отправлении правосудия в уголовного судопроизводстве. Ошибка в квалификации может повлечь за собой необоснованное осуждение лица или необоснованное ее оправдание, или применения к виновному нормы УК, не содержащей всех уголовно-правовых признаков совершенного виновным деяния [5].

Проблему квалификации хищений денежных средств с использованием информационно-телекоммуникационных технологий затрагивают в своих работах и обсуждениях И. А. Александрова, П. С. Яни, Е. А. Русскевича и др.

Как утверждает И. А. Александрова, хищение имущества в виде денежных средств, находящихся на счете, путем «взлома» защиты охраняемой компьютерной информации следует квалифицировать как кражу, поскольку компьютер – не физическое лицо, а, фактически устройство, как и банкомат [1].

По мнению профессора кафедры уголовного права и криминологии юридического факультета МГУ имени М. В. Ломоносова, члена научно-консультативного совета (далее – НКС) при Верховном Суде РФ П. С. Яни, если предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные, то по смыслу положений п. 1 примечаний к ст. 158 УК и ст. 128 ГК РФ содеянное должно квалифицироваться как хищение чужого имущества [16].

Е. А. Русскевич, напротив, считает, что отличием общеуголовного мошенничества с использованием методов так называемой социальной инженерии он лично или через третьих лиц передает денежные средства или иное имущество злоумышленнику. Например, если тем самым самостоятельно перевел денежные средства на счет злоумышленника, содеянное образует признаки общеуголовного мошенничества. В тех же случаях, когда лицо обманным путем лишь получает сведения о платежной карте либо другую критически значимую информацию, касающуюся работы сервисов дистанционного банковского обслуживания то содеянное необходимо квалифицировать по п. «г» ч. 3 ст. 158 УК РФ. [11. С. 59–64].

В науке отсутствует единообразный подход к вопросу квалификации вышеуказанной категории преступлений.

В свою очередь, законодатель в постановлении Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» говорит, что если обман не направлен непосредственно на завладение чужим имуществом, а используется только для облегчения доступа к нему, действия виновного в зависимости от способа хищения образуют состав кражи или грабежа. [9]

Аналогично указано в определении Конституционного Суда РФ от 09 июля 2021 г. № 1374-О «О прекращении производства по делу о проверке конституционности пункта «г» части третьей статьи 158 и статьи 159.3 Уголовного кодекса Российской Федерации в связи с запросом Железнодорожного районного суда города Рязани», что кража и мошенничество являются самостоятельными видами (формами) хищений, а по отношению друг к другу образуют смежные составы преступлений, основным критерием разграничения которых является способ совершения таких деяний [8].

Также анализ судебной практики по мнению Т. Н. Долгих показывает, что, если виновный открыто похищает непосредственно банковскую карточку, знает или при помощи применения насилия к потерпевшему узнает пин-код, такие действия, несмотря на последующее снятие денежных средств посредством банкомата в отсутствие потерпевшего, надлежит квалифицировать в зависимости от конкретных обстоятельств по ст. 161 или 162 УК РФ [4].

Чтобы избежать смешения в правовой системе необходимо постоянное обновление и пересмотр законов. Как подчеркивает Е. А. Русскевич востребованность и качество нормы довольно скоро будут верифицированы практикой. И в этом отношении стоит только полагаться на время. Доктрина же в свою очередь должна вырабатывать возможные перспективные шаги по изменению закона и преодолению проблем правоприменения. [12. С. 650–672].

Так, предлагается исключить из УК РФ п. «г» ч. 3 ст.158, ст. 159.3 и ст. 159.6 и ввести отдельную главу под названием: «Преступления с использованием информационно-телекоммуникационных технологий», что позволит полностью систематизировать и регулировать киберпреступления в российском законодательстве.

Для большей точности и ясности рекомендуется дать на законодательном уровне определения таким понятиям как: «информационно-телекоммуникационные технологии», «сеть-Интернет», «IT-технологии», «киберпространство», «киберпреступность» и многое другое. Например, одно из указанных понятий раскрывается в работе А. М. Райеджиана, где указано, что «киберпреступность определяется как преступная деятельность с использованием технологий и цифровизации. Она включает незаконные деяния и действия, в том числе доступ к информации, перехват или повреждение данных, вмешательство в работу компьютерных систем или устройств и т. д. Обычно киберпреступность подразделяют на преступления, связанные с информацией, и преступления, связанные с компьютерными сетями» [10].

Если говорить про киберпреступления в общем, то, например, А. А. Дмитриева и П. С. Пастухов предлагают внести изменения в Уголовно-процессуальный кодекс РФ (далее – УПК РФ), а именно добавить такое понятие как «цифровое доказательство». Как указано в их работе цифровые данные являются основой большинства расследований киберпреступлений [3].

Также необходимо определиться с предметом, местом и способом совершения киберпреступлений. Что же касается меры принуждения, как показывает практика сроки за совершение компьютерных преступлений мягкие и условные. В связи с чем правильнее будет внести новый вид дополнительного наказания в виде ограничения пользованием информационно-телекоммуникационными технологиями на определенный срок. Дать на законодательном уровне разъяснения по составам преступления, совершенным с использованием информационно-телекоммуникационных технологий, а именно: по субъекту, объекту, субъективной и объективной стороне. При расследовании преступлений использовать технологии искусственного интеллекта.

В конечном итоге проблема квалификации преступлений требует дальнейшего исследования и обсуждения со стороны ученых, юристов, правоведов,

судебных и правоохранительных органов, а также общественности в целом. Ведь от правильной квалификации преступления зависит какое наказание получит преступник.

Список литературы

1. Александрова И. А. Новое уголовное законодательство о мошенничестве // Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2013. № 21. С. 54–62.

2. Антонова Е. Ю. Преступления террористической направленности в эпоху цифровизации: формы деятельности и меры по противодействию // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 251–269. EDN: HFPMTN.

3. Дмитриева А. А. Концепция электронного доказательства в уголовном судопроизводстве / А. А. Дмитриева, П. С. Пастухов // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 270–295. EDN: SGAOKS.

4. Долгих Т. Н. Ответственность за хищение денежных средств с банковского счета // СПС КонсультантПлюс.

5. Закомолдин Р. В., Кондратюк С. В. К вопросу о нормативном определении понятия и сущности квалификации преступлений // Юридические науки. 2020. № 1(7). С. 89–92.

6. Министерство внутренних дел Российской Федерации. Состояние преступности в Российской Федерации за январь-июнь 2023 года. URL: https://мвд.рф/reports/item/40116049

7. Об ответственности, установленной законодательством за хищения, совершаемые с использованием современных информационно-телекоммуникационных технологий. URL: https://clck.ru/36p4RY

8. Определение Конституционного Суда РФ от 09 июля 2021 года № 1374-О «О прекращении производства по делу о проверке конституционности пункта «г» части третьей статьи 158 и статьи 159.3 Уголовного кодекса Российской Федерации в связи с запросом Железнодорожного районного суда города Рязани» // СПС КонсультантПлюс.

9. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС КонсультантПлюс.

10. Асли М. Р. Цифровые тренды криминологии и уголовного правосудия XXI века / М. Р. Асли // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 235–250. EDN: ZMIRLT.

11. Русскевич Е. А. Отграничение кражи с банковского счета или в отношении электронных денежных средств от смежных составов преступлений // Уголовное право. 2019. № 2. С. 59–64.

12. Русскевич Е. А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности / Е. А. Русскевич // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 650–672. EDN: FISEET.

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

14. Текст законопроекта Федерального закона «О внесении изменения в статью 6 Федерального закона «Об оперативно-розыскной деятельности» и материалами к нему на федеральном портале проектов нормативных правовых актов». URL: https://regulation.gov.ru/Entities/Npa_Text

15. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

16. Яни П. С. Лекция профессора кафедры уголовного права и криминологии юридического факультета МГУ им. М. В. Ломоносова, члена НКС при Верховном Суде РФ Павла Яни на обучающем вебинаре федеральной палаты адвокатов. URL: https://www.advgazeta.ru/novosti/advokatam-rasskazali-ob-osobennostyakh-kvalifikatsii-moshennichestva-i-vzyatochnichestva

Р. Р. Сверигина,
соискатель,
Казанский (Приволжский) федеральный университет

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ БЛОКЧЕЙН-ТЕХНОЛОГИЙ

Аннотация. В статье раскрывается проблематика регулирования в российском законодательстве отношений, связанных с использованием блокчейн технологий. Осуществляется поиск путей решения возникающих проблем и коллизий в связи с многогранностью использования данной технологии. Обозначены перспективы внедрения блокчейн технологии в разные сферы деятельности, учитывая сложности законодательного регулирования данных отношений.

Ключевые слова: блокчейн, технологии блокчейн, смарт-контракты, NFT, технология распределенного реестра, недействительность сделок и блокчейн, невзаимозаменяемый токен, цифровые финансовые активы, цифровые права

PROBLEMS OF LEGAL REGULATION OF RELATIONS ASSOCIATED WITH THE USE OF BLOCKCHAIN TECHNOLOGIES

Abstract. This article reveals the problems of regulation in Russian legislation, relations associated with the use of blockchain technologies, searches for ways to solve these problems and conflicts due to the versatility of using this technology, and also provides prospects for the introduction of blockchain technology in various fields of activity, given the emergence of difficulties for regulation data relations for the legislator

Keywords: blockchain, blockchain technology, smart contracts, NFT, distributed ledger technology, transaction invalidation and blockchain, non-fungible token, digital financial assets, digital rights

Весь мир стремительно уходит в цифровую плоскость. Все наши персональные данные, доходы, книги и даже письма есть в сети интернет. Появление новых технологий – это этап развития цивилизации. Мощным рывком стало появление технологии блокчейн, которая в значительной степени расширила возможности во многих отраслях жизнедеятельности, и не только в финансовой отрасли, как полагает большинство. В связи новизной данного явления и отсутствия аналогичных норм, многие правовые аспекты на данном этапе развития пока не поддаются регулированию. Наличие проблем правового регулирования становится невозможно скрыть, эта тема все чаще является основной повесткой дня юристов всех отраслей. Подпитывает проблему и тот факт, что технологической сущностью блокчейна является распределенность реестра данных, неизменяемость внесенных записей, что противоречит многим основам цивилистики.

Блокчейн (с англ. Blockchain- цепочка блоков)- хранения данных, непрерывная последовательная цепочка блоков, которая содержит информацию о транзакциях и выстроенная по определенным правилам. Этот общедоступный реестр, основанный на алгоритмах криптографической системы, хранит в себе данные обо всех изменениях и операциях, произошедших в системе. Согласно докладу Международной ассоциации юристов (International Bar Association) реестр, созданный на базе блокчен технологий, хранит и отслеживает данные и стоимость, создавая защищенные записи транзакций. Записи невозможно изменить. Каждая транзакция заверяется криптографическими подписями участников и после этого добавляется в реестр в качестве нового “блока” (block) в цепочку записей (chain). Вся зашифрованная цепь данных видна участникам, что делает ее прозрачной, но в то же время сохраняет персональные данные закрытыми. С этой позиции для цивилистики нужно выделить два ключевых аспекта: 1) невозможность изменить информацию; 2) анонимность. При этом саму блокчен технологию условно можно разделить на 3 сферы применения:

1. Финансовые транзакции (CBDC – Central Bank Digital Currency (цифровая валюта Центрального Банка) или криптовалюта));
2. Контракты (применение технологии в сфере экономики);
3. В области государственного управления, науки, образования.

Важно отметить, что законодатель видит перспективы данной технологии и активно ищет ей применение. Стремление законодателя в развитии данного вопроса отражается в законах ФЗ от 14.07.2022 № 339-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», ФЗ от 24.07.2023 № 340-ФЗ и ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ – свежих и неоднозначных, но тем не менее государство понимает необходимость правового регулирования и активно работает в этом направлении.

Среди преимуществ нужно сказать о прозрачности для пользователей, т. е. весь ход событий (транзакций) виден участникам платформы. Децентрализованность – данные не прикреплены к какому-то определенному серверу, они хранятся на нескольких серверах. Перманентность – данные изменять нельзя. А также строгая очередность транзакций.

Существующее положение о неизменяемости сделки остро противоречит уже закрепленным нормам гражданского права. Рассмотрим ситуацию со сделками. Сделка есть действие лица, которое подконтрольно его воле и совершается лишь постольку, поскольку имеется воля и волеизъявление этого лица на совершение сделки. В случае совершения сделки, при бесконфликтных обстоятельствах, проблем с гражданским законодательством нет, однако, в случае если появляется какой-либо спор, и как результат решение суда, то вопрос решения крайне неоднозначен, в виду того, что само определение блокчейн не позволяет вносить изменения в код, без подтверждения всех участников, а, следовательно, положение статей требует внесения изменений. Аналогий, которые можно было бы применить, нет. Законодателю придется искать новые пути решения возникшего противоречия. Одним из варианта решения проблемы, можно создать дополнительную запись в блокчейн, которая позволит перекрыть предыдущие записи в системе новыми вводными данными. В свою очередь, стоит законодательно закрепить, что фактическую и юридическую силу приобретает именно последняя внесенная запись, тем самым мы сможем аннулировать значение первоначальной сделки. Стоит здесь еще вспомнить об операторах системы. Здесь очень важно не потерять основную суть и ценность технологии. Законодателю стоит задуматься о создании отдельного Федерального Закона, в котором будут прописаны соответствующие права и обязанности будущих операторов блокчейн-платформ, как например в Федеральном Законе от 27.06.2011 №-161ФЗ «О национальной платежной системе» (ст. 15). Необходимо указать, что операторы Российских блокчейн-платформ (а также, зарубежных, которые будут работать с Российскими физическими и юридическими лицами), подчиняются законам РФ и судебным постановлениям, и закрепить ответственность за невыполнение существующих предписаний. Схожее противоречие возникает и с п.1 ст.450.1 ГК РФ. Технические особенности системы блокчейн не позволят внести в систему изменения, даже если односторонний отказ от сделки был совершен правомерно. Возникает ситуация, когда участники оказываются в новых условиях рынка, которые государство пытается урегулировать традиционными способами. Но новую возникшую парадигму можно приспособить, только внеся изменения в существующие, уже укоренившиеся нормы гражданского права. Тут по той же аналогии можно внести изменения путем новой записи.

Еще одной существенной проблемой выступает выявление сделок, противоправных закону, основам правопорядка или же нравственным началам. Такие сделки, в соответствии со ст. 169 ГК РФ, являются ничтожными и влекут последствия, установленные статьей 167 ГК РФ. Такого рода сделки должны пресекаться и не иметь никакой юридической силы, так как они входят в категорию повышенной опасности для государственного строя и общества в целом. Тут суть заключается именно в том, что такие сделки не должны нести за собой никаких юридических последствий, так как это является приоритетом государства и общества. Но, как мы уже поняли, сделки, проведенные в блокчейне отмене, не подлежат. То есть, предположим сделки с различными анонимными криптовалютами (Monero, Zec) проводят для сбыта наркотических веществ, и даже при

полном понимании, что данная транзакция – это оплата за наркотические вещества в Monero (Предположим сходится время, дата, сумма при конвертации, а также по данному была наводка от уже пойманного дилера), сделать ничего невозможно. К сожалению, установление в системе алгоритма или фильтра, позволяющего отследить подобные сделки, пока технически не выполнимо. В таком случае нужно модернизировать данную технологию. Как пример, хочу проанализировать недавнее высказывание А. Г. Аксакова, который заявил, что цифровой российский рубль (CBDC) можно будет программировать под определенные траты с помощью смарт-контрактов: «Как ни велико будет желание школьника использовать мамин цифровой рубль на вредные сладости, применить деньги не по назначению не получится. Целевое назначение выделенных родителями ребенку денег будет прописано в специальном смарт-контракте». Для работы российских блокчейн платформ необходимо упоминание в законе о запрете привязки криптовалют к смарт контрактам. Отечественные блокчейн-операторы должны привязывать смарт контракты только к дебютирующему цифровому рублю.

Обсудим упомянутые смарт-контракты. Феномен, изобретенный в 1994 г., придуман для автоматизации действий, которые в быту совершаются с привлечением третьих лиц. К примеру, за простой оплатой электроэнергии стоят бухгалтеры, аудиторы, чьи осмысленные формальные действия можно автоматизировать, используя блокчейн технологии. Но на сегодняшний день существуют локальные нормативно правовые акты в области электроэнергии усложняющие заключения подобных контрактов в данной области. Внесение изменений в данных НПА позволит сделать заключение подобных договоров более прозрачным и без использования аналогии права, которая может быть весьма субъективна и неоднозначна.

Преимуществами смарт контрактов являются:

– Независимость. Нет необходимости искать специалиста для заключения сделки;

– Контракт храниться в зашифрованном виде в распределенном реестре;

– Все документы многократно продублированы в блокчейне;

– Экономия. Нет необходимости оплачивать услуги посредников;

– Точность. Не нужно заполнять вручную множество форм, с риском ошибиться [1].

Ник Сабо, изобретатель «умного контракта», хотел создать цифровую торговую площадку, которая основывается на автоматических и криптографически защищенных процессах. Смарт контракт содержит традиционные предпосылки договора: обязательство, условия оплаты, штрафы, но тем не менее форму юридического документа собой не представляет. Сделки, совершенные посредством смарт-контрактов, не требуют участия посредников для контроля процесса, так как предписанные действия (оплата) осуществляются автоматически при исполнении обязательства.

Проблематика смарт-контракта для гражданского права выражается в его абсолютном характере. Однако зачастую исполнение обязательства проходит совсем не так, как этого мог ожидать кредитор. Разные условия сделки нередко понимаются сторонами по-разному, что приводит к коллизиям. Ведь вопросы качества

товара или услуги нельзя запрограммировать. Надлежащее исполнение обязательства складывается из двух элементов: 1) своевременное исполнение (факт фиксирования может быть интегрирован в смарт контракт) и 2) соответствие оказанной услуги условиям сделки (что нельзя перенести в компьютерный код). На мой взгляд, для регулирования отношений, связанных со смарт контрактами нужны изменения и дополнения в Гражданский кодекс РФ. Во-первых, новая форма договоров полностью не заменит традиционные методы их заключения, но при этом смарт контракты кардинально меняют всю суть совершения договоров, они автоматизируются. То есть процесс раскрывается совершенно под другим углом и требует специального регулирования отношений. Во-вторых, это технология позволяет избавиться от третьих лиц при заключении договоров, однако кто же будет прописывать условия совершения договоров? Для этого также нужны люди с определенными навыками, а значит это также нужно прописать в новом законе, чтобы была определенная регуляция. И в-третьих определенные типы сделок прописать в смарт контрактах просто нереально, так как необходимо физическое присутствие людей к примеру, при проверке поставки, следовательно, в законе должен быть прописан список договоров, которые можно регулировать с помощью смарт-контрактов.

Применение смарт контактов может быть очень удобном в такой сфере как страхование, в сферах где наступление страхового случая не носит оценочный характер. К примеру страховка Путешественника при задержке рейса. То есть путем принудительного выполнения определенных обязанностей страховой компании при наступлении определенных обстоятельств. Например, задержка или отмена вылета самолета, в коде смарт контракта прописываются время задержки вылета. Каким образом технология распознает задержку рейса? Тут есть несколько вариантов. Один из них – это привязка контракта к онлайн табло в аэропорту, так как именно там человек узнает о своем рейсе информацию. Данный смарт контракт значительно облегчит процесс выплат и бюрократию при наступление страхового случая. Тут более того будет удобен цифровой рубль, так как именно он предназначен для смарт-контрактов

Необходимо отметить концепцию цифрового рубля, ведь она основывается на базе технологии блокчейн. Однако тут проблем правого регулирования значительно меньше, ведь 24 июля 2023 года были подписаны Президентом РФ и опубликованы Федеральный закон от 24 июля 2023 г. № 339-ФЗ «О внесении изменений в ст. 128 и 140 части первой, часть вторую и ст. 1128 и 1174 части третьей Гражданского кодекса Российской Федерации» и Федеральный закон от 24 июля 2023 г. № 340-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», регулирующие правовые основы введения цифрового рубля. Эти изменения и дополнения позволят ввести в России новую форму денег. Технология цифрового рубля, как и иных платежных систем на территории РФ находится под контролем государства. То есть, по сути, технология блокчейн децентрализованная, но не в случае цифрового рубля. В данном случае регулятор может контролировать, блокировать и взыскивать денежные средства без проблем. С точки зрения правового регулирования, вопросов меньше, нужно смотреть на дальнейшее развитие данной концепции и способы ее применения.

Не менее затруднительно обстоит дело с регулированием невзаимозаменяемых токенов (NFT). NFT это уникальная, неделимая и невзаимозаменяемая цифровая запись непосредственно в блокчейне. Эта запись хранит в себе конкретный цифровой объект, к примеру картина, или же ссылку на него, что, в свою очередь, подтверждает право на такой цифровой объект и более того доказывает его подлинность. Невзаимозаменяемый токен может быть связан и с уникальным физическим объектом, но тут возникают правовые коллизии. Согласно ст 128 ГК РФ NFT не могут быть причислены к вещам, но относятся к иному имуществу, перечень которого в Гражданском праве является не закрытым. Но ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» достаточно однозначно отнес это к иному имуществу и применяет все нормы как к имуществу, тем самым значительно облегчив его оборот на территории РФ. Это не ценная бумага, которая должна проходить учет через депозитарий и не валюта, а имущество. Самая главная особенность заключается в том, что невзаимозаменяемый токен может отражать абсолютно любые права, начиная правом на картину неизвестного художника и заканчивая правом на саму картину или обязанностями по определенным договорам. Хочется отметить, что сентябре 2021 года на государственном уровне был проведен аукцион NFT токенов картин музея Эрмитажа. Музей Эрмитаж создал 5 NFT токенов картин и продал их на аукционе крупной крипто-бирже в мире-Binance. Самой дорогой NFT токен картины стала отцифрованная картина «Мадонна Литта» великого Леонардо да Винчи. Она была продана более чем за 150 тысяч долларов США, на по курсу на тот момент это около 10 миллионов рублей. Это яркий пример того, как блокчейн технологии расширяют возможности. Аукцион был инициирован государственным музеем, это большой шаг в развитии и внедрении технологии, связанной с NFT.

Информация об NFT содержится в децентрализованной базе данных, которая хранится одновременно на нескольких компьютерах (серверах). Это обеспечивает ее защищенность от уничтожения, а также внесения в нее каких-либо изменений. Вывод – функцию реестродержателя выполняет сама технология блокчейн. NFT – запись в блокчейне, которая удостоверяет права на цифровые активы [2]. Но по Российскому законодательству такая запись юридической силы не имеет. Приобретатель NFT получает право на владение реестровой записью в децентрализованном реестре, а исключительное право на результаты интеллектуальной деятельности- нет. Все это лишь показывает, что законодателю предстоит проработать данные юридические аспекты и внести изменения в текущее законодательство, ведь сама по себе идея NFT является перспективной.

Одной из проблем правового регулирования данного вопроса является его взыскание. Получить доступ к такому имуществу возможно только при активном содействии самого должника. Без предоставления им логина и пароля не получится получить доступ к его активам. В данном вопросе активно обсуждаются необходимость внести изменения в НК РФ, где в перспективе каждый владелец кошелька должен информировать ФНС о его открытии, с указанием идентификационных данных. По аналогии, открытия расчетных счетов гражданами РФ

на территории иных государств. Несмотря на то, что в Налоговом кодексе уже установлен особый порядок налогообложения операций с цифровыми финансовыми активами и гибридными цифровыми правами (Федеральный закон от 14 июля 2022 г. № 324-ФЗ «О внесении изменений в часть вторую Налогового кодекса Российской Федерации»), ряд сопутствующих вопросов еще не урегулирован законодательно – например, в части гармонизации порядка налогообложения «гибридных» цифровых прав с порядком налогообложения токенизированных активов (товаров (работ, услуг), являющихся предметом исполнения таких цифровых прав. В связи с этим Банк России предлагает продолжить проработку налоговых поправок.

Очень интересная сфера применения блокчейн технологий, по моему мнению, политическая сфера, где можно модернизировать процесс выборов, путем голосования граждан, с помощью технологии блокчейн. В этом случае фальсификации будет исключена и более того голоса будут сохранены и неизменны, и при необходимости могут быть проверены. Это повысит лояльность граждан к кандидатам и к избирательной системе страны в целом. Также при должном правовом регулировании данная технология окажет существенное положительное влияние в сфере государственного управления и контролирования. К примеру, государственная регистрация сделок с недвижимостью может быть более простой нежели сейчас, а также, что немаловажно, более открытой и надежной, в случае ее децентрализации.

О том, как Российское законодательство будет изменяться в новых цифровых реалиях нам покажет время. Но факт необходимости коренных изменений в сложившихся правовых нормах ярко выражен. Преобразования, которые несет блокчейн в мир нашего права не просто эволюционные, а поистине революционные. Более того, на конференции «Технологии блокчейн, криптовалюта и другие продукты как объекты интеллектуальной деятельности», прошедшей в Москве, прозвучали высказывания о необходимости создания отдельного «технологического кодекса», который поставит под сомнение саму концепцию римского права: «фактически римское право как то право, по которому мы живем, ставится под сомнение. А это делать крайне сложно, потому что это изменяет статус нашего социально-экономического уклада».

Список литературы

1. Дудихин В. В. Некоторые социальные последствия использования криптоплатформ второго поколения // В сборнике: Государственное управление Российской Федерации: повестка дня власти и общества. материалы XVI Международной конференции. 2019. С. 74–79.

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

Л. В. Сокольская,
кандидат юридических наук, доцент,
Государственный гуманитарно-технологический университет

ЦИФРОВИЗАЦИЯ ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Сегодня юридическая сфера деятельности стоит на пороге больших стратегических преобразований, вызванных цифровой революцией. И уже на старте важно понимать, какие методы, инструменты приведут к скорейшей ее реформации, какие знания, умения и навыки будут востребованы среди юристов новой реальности. В статье анализируется личный опыт преподавания юридических дисциплин в вузе, на основании чего предлагается актуализировать действующие рабочие программы в контексте формирования у будущих юристов необходимых цифровых навыков.

Ключевые слова: право, цифровые технологии, формирование цифровых умений и навыков, преподавание, юридическая деятельность, искусственный интеллект, юридическое образование

DIGITIZATION OF LEGAL ACTIVITY

Abstract. Today, the legal industry is on the verge of a major strategic transformation brought about by the digital revolution. And already at the start, it is important to understand what methods and tools will lead to its speedy reformation, what knowledge, skills and abilities will be in demand among lawyers of the new reality. The author of the article, having analyzed her own experience of teaching legal disciplines at a university, proposes updating existing work programs in the context of developing the necessary digital skills in future lawyers.

Keywords: law, digital technologies, formation of digital skills, teaching, legal activity, artificial intelligence, legal education

Сегодня фактически все отрасли экономики, начиная от здравоохранения, заканчивая добывающей промышленностью, претерпевают цифровую трансформацию [1, 2]. Многие процессы автоматизируются, у человека появляются новые инструменты для осуществления своей деятельности, поэтому меняются сами профессии, появляются новые специальности на стыке отраслевых специальностей с ИТ-сферой. Как правило, при приеме на работу работодатель тестирует своего будущего работника на умение работать в экосистеме программного обеспечения организации, т. е. работодатель требует от своего работника не просто знаний конкретных программных продуктов, а именно овладение ими [3].

В юридической деятельности уже применяются следующие цифровые программы, проекты и инструменты:

1. Электронный документооборот. Почти все современные компании и организации сегодня используют электронный документооборот и ведут делопроизводство в электронном формате. Умение работать с документацией компании – это основной вид деятельности всех работников аппарата управления от высших

руководителей до технических исполнителей. Внедрение цифровых технологий позволяет компании повысить эффективность управления, сделать прозрачнее процесс менеджмента. Преимущества электронного делопроизводства:

– быстрая регистрация и обработка документов;

– автоматическое заполнение всех реквизитов при обмене документами с контрагентами;

– обмен электронными документами между контрагентами занимает секунды;

– подключение к системе электронного документооборота через веб-доступ или мобильное приложение;

– возможность удаленно работать с документом, подписывать его, выносить по нему распоряжения и резолюции;

– простота ознакомления с распорядительными и организационными документами всеми сотрудниками компании;

– возможность руководителя онлайн отслеживать и контролировать работу над документами сотрудниками компании. Электронная система определит кто и когда открыл данный документ, кто прочитал его, а кто еще не ознакомился с ним и т. д. [4].

В настоящее время под индивидуальные потребности организации создается своя система электронного документооборота (СЭД), которая дает возможность организовать работу с электронными документами и наладить связь между сотрудниками компании. ECM-система – это управление корпоративными информационными ресурсами. Это уже не просто СЭД, это уже сканирование, хранение документов и обеспечение их безопасности. В системе управления бизнес процессами (BPM) акцент делается не на самом документе, а на процессе и действии лиц, ответственных за выполнение определенных действий. Например, как осуществляется электронное делопроизводство с Case.pro.

Case.pro – основной рабочий инструмент юриста, который предоставляет готовый набор функций для автоматизации юридической деятельности: управление делами и проектами, хранение документов, учет и фиксация событий, управление задачами с возможностью контроля сроков исполнения, подготовка отчетов, учет расходов и затраченного времени, подготовка счетов, оперативный доступ к актуальным статусам и изменениям по делам заказчиков через клиентский портал.

Case.pro успешно помогает решать следующие проблемы: трудности в передаче дел от одного юриста другому без потери данных; неоправданная трата времени на типовые рутинные процессы – поиск процессуальных документов, ручной ввод данных для типовых документов (заявлений/отзывов/ходатайств и др.); оперативная оценка эффективности работы каждого сотрудника и юридической функции в целом; отслеживание изменений по десяткам проектов и сотням дел в режиме реального времени; тайминг и билинг дел с учетом различных ставок исполнителей, скидок и фиксированных ставок для разных клиентов; пропущенные встречи, процессуальные сроки подачи документов в суд, пропущенные заседания из-за отсутствия единого календаря и т. д.

2. Информационные справочные системы содержат полную систематизированную и оперативно-обновляемую информацию по законодательству, судебной

практики, комментариям, разъяснениям и другим материалам, а также программные средства поиска, анализа и обработки этой информации. Caselook (кейслук) – сервис для поиска и анализа судебной практики арбитражных судов и судов общей юрисдикции для формирования правовой позиции. URL: https://www.youtube.com/watch?v=1ltC8yHS418

3. Текстовые аналитики. Программа Гарант Коннект позволяет готовить юридические документы в современном формате с ссылками на действующие правовые нормы, а также поддерживать в актуальном виде документы, используемые в компании на сайте.

4. Интеллектуальные системы. По распознаванию лиц и силуэтов людей, автомобилей и номерных знаков FindFace – выявляет нарушителей и позволяет принять меры до совершения противоправных действий; помогает узнать о ваших клиентах, что улучшае качество обслуживания и повышайте продажи; обеспечивает быстрый проход через турникет; осуществляет полный контроль посещений и учет рабочего времени; оповещает о появлении лиц из «черных списков»; уведомляет службу охраны; с помощью системы распознавания лиц собирает статистику по полу, возрасту, эмоциям о клиентах; предоставляет консультацию эксперта по видеоаналитике. URL: https://ntechlab.com/ru/

По подбору судебной практики. Правобот – первый сервис, который думает как юрист, помогает подобрать необходимую судебную практику, сохраняет историю запроса и все просмотренные дела.

5. Автоматизация юридической деятельности. Гарант – LegalTech. Автоматизация правовых задач.

6. Дистанционная поддержка. Правовед.ру – юридическая консультация онлайн.

Все вышеперечисленные цифровые технологии успешно применяются на российском рынке, и задача высшей школы способствовать формированию у будущих юристов необходимых навыков или как мы сегодня говорим компетенций.

Цифровая грамотность будущего юриста состоит из следующих навыков:

– информационная грамотность – отражает навыки человека по поиску информации в интернете, компетенции по работе с различными видами данных и оценке достоверности сообщений в сети;

– коммуникативная грамотность – включает умение человека пользоваться различными видами онлайн-сервисов и электронных устройств, соблюдение норм общения в сети;

– создание цифрового контента – демонстрирует компетенции человека по созданию и редактированию цифрового контента, навыки по работе с авторскими правами в сети;

– цифровая безопасность – показывает умения человека оценивать риски социальной инженерии и онлайн-мошенничества при работе в цифровом пространстве, знание мер по обеспечению безопасности персональных данных, а также понимание негативного влияния, которое цифровые устройства оказывают на окружающую среду, физическое и психическое здоровье человека;

– навыки решения проблем в цифровой среде – определяются навыками человека по пользованию мобильными приложениями и компьютерными программами для

выполнения повседневных задач, постоянным расширением знаний в сфере цифровых технологий, возможностью решать аппаратные и программные проблемы [5].

В федеральном стандарте высшего юридического образования закреплена только одна общепрофессиональная компетенция, связанная с формированием IT – навыков (ОПК-8). И то согласно учебным планам многих вузов, выпускающих юристов-бакалавров данная компетенция формируется в рамках 1 или 2 учебных дисциплин. Например, в ГГТУ.

Что же делать если в учебном плане нет специальных дисциплин, или их недостаточно. Опираясь на собственный практический опыт преподавания на юридическом факультете можно рекомендовать коллегам предпринять следующие шаги:

– при невозможности изменить матрицу компетенций в учебном плане, можно в любой компетенции преподаваемого вами предмета расширить: знания, умения, навыки;

– обозначить новые темы лекций или расширить название существующих тем с применением информационных и «сквозных» технологий. Как например, я сделала при чтении курса АПТГП;

– изменить содержание практический занятий и самостоятельной работы студентов;

– расширить фонд оценочных средств [6, 7].

Исходя из вышеизложенного можно сформулировать вывод о том, что активная цифровая трансформация несет в себе множество вызовов для юридической сферы деятельности, в том числе и для юридического образования. Появление объектов, созданных с применением искусственного интеллекта, аддитивные технологии, распространение цифрового производства, цифровых каналов дистрибуции контента и т. д. требуют определенных изменений в процессе подготовки кадров высшей квалификации. Сегодня те уникальные знания и умения, которыми обладали люди раньше, заменяются на умения и знания в ИТ области. Например, юрист в сфере ИТ-технологий.

По мнению автора статьи, IT-юрист в цифровой компании – это перспективное направление в сфере современного права. За последний год спрос на юристов в IT вырос на 40 %. Корпорациям не хватает специалистов, знающих право информационных технологий, интеллектуальной собственности и цифровых платформ. Поэтому уже сегодня необходимо выпускать юристов, которые могут с уверенностью сказать о себе:

– знаю формы и особенности договорных отношений и защиты исключительных прав в IT;

– понимаю способы цифровой трансформации бизнес-процессов и правового сопровождения;

– знаю особенности государственного регулирования IT-компаний;

– анализирую бизнес-задачи в IT с правовой точки зрения;

– собираю и анализирую применимый правовой материал;

– готовлю базовое правовое заключение по вопросу;

– умею готовить предложения по корректировке законодательства;

– составляю исковое заявление с корректной фактологической основой.

Список литературы

1. Об утверждении Положения о формировании и функционировании евразийских технологических платформ: решение Евразийского межправительственного совета от 13.04.2016 № 2. URL: http://www.consultant.ru

2. Об утверждении Стратегии пространственного развития Российской Федерации на период до 2025 года: Распоряжение Правительства РФ от 13.02.2019 № 207-р. URL: http://www.consultant.ru

3. Смородинская Н. В. Сетевые инновационные экосистемы и их роль в динамизации экономического роста // Инновации. 2014. № 7 (189).

4. Иванова Ж. Б. Информационные технологии документационного обеспечения управления в неосударственных организациях. Ульяновск, 2020.

5. Ляпушкин П. В, Сокольская Л. В. К вопросу о цифровизации юридического образования // Новая наука – новые возможности. Сборник статей IV Международного научно-исследовательского конкурса. Петрозаводск, 2022. С. 90–94.

6. Сокольская Л. В. Проблемы модернизации образовательных программ при переходе на ФГОС ВО 3++ в контексте цифровизации юридической деятельности // Проблемы и перспективы развития государства и права в XXI веке. Материалы XII-й Международной научно-практической конференции, посвященной 15-летию Юридического факультета. Улан-Удэ, 2021. С. 64–70.

7. Сокольская Л. В. Особенности обучения в высшем учебном заведении студентов поколения Z // Юридическое образование и наука. 2021. № 7. С. 17–23.

Е. А. Мамай,
кандидат юридических наук, доцент,
Национальный исследовательский университет
«Высшая школа экономики»

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СИСТЕМЕ ПРАВОВЫХ ОТНОШЕНИЙ: ПРИМЕРЫ ИЗ СУДЕБНОЙ ПРАКТИКИ ЗАРУБЕЖНЫХ СТРАН И РОССИИ

Аннотация. В статье исследуется современная судебная практика в США, Европе, Китае и России по делам, связанным с использованием систем искусственного интеллекта. Изучены особенности правовых позиций судов по делам, в которых ИИ вовлечен в принятие юридически значимых решений, обработку персональных данных, а также создание произведений интеллектуальной собственности. Учет указанного опыта позволяет наметить перспективные направления развития отечественной судебной практики, которая на данный момент существенно отстает от общемировых тенденций.

Ключевые слова: право, интеллектуальная система, искусственный интеллект, судебная практика, принятие решений, персональные данные, авторство, маркетплейс

ARTIFICIAL INTELLIGENCE IN THE SYSTEM OF LEGAL RELATIONS: EXAMPLES FROM JUDICIAL PRACTICE OF FOREIGN COUNTRIES AND RUSSIA

Abstract. The article examines modern judicial practice in the USA, Europe, China and Russia in cases involving the use of artificial intelligence systems. The author studies the peculiarities of the legal positions of courts in cases in which AI is involved in making legally significant decisions, processing personal data, as well as creating works of intellectual property. The study of this experience allows to outline promising directions for the development of Russian judicial practice, which at the moment lags significantly behind global trends.

Keywords: law, intelligent system, artificial intelligence, judicial practice, decision making, personal data, authorship, trading platform

Введение. В современном мире вовлеченность интеллектуальных систем в разнообразные процессы, протекающие в обществе, становится все более разнообразной и всеобъемлющей. Возможности систем искусственного интеллекта в достигнутом ими на данный момент темпе развития вызывают большое опасение как в среде широкой общественности, так и специалистов. Еще в сентябре 2021 г. Верховный комиссар ООН по правам человека Мишель Бачелет призвала ввести мораторий на использование технологий искусственного интеллекта, которые потенциально могут нарушать и нарушают права человека [1]. В марте текущего года более 1000 экспертов в сфере информационных технологий, в числе которых упоминались И. Маск, Э. Шарп, С. Возник, в своем открытом письме, предупредили человечество о том, что неконтролируемое развитие искусственного интеллекта несомненно повлечет за собой негативные последствия для всего мира. В этой связи они настаивают на необходимости введения надежной системы сертификации ИИ, создания регулирующих органов, а также надзоре за высокопроизводительными системами искусственного интеллекта [2].

На передовом крае развития права нередко оказываются судебные инстанции, которые впервые сталкиваются с ситуациями, требующими правового разрешения. Представляется интересным и научно-необходимым рассмотреть текущую, передовую практику разрешения судами споров, связанных с использованием систем искусственного интеллекта в современном мире.

Основная часть. Обращаясь к вопросам современной судебной практики по делам, связанным с системами искусственного интеллекта, следует сделать несколько предварительных замечаний. Прежде всего, отметим, что в современном мире суды в своей деятельности в первую очередь сталкиваются с наиболее очевидными «болевыми точками» соприкосновения права и технологий, подразумевающими критичное восприятие людьми, распространенность явления, его большую резонансность в медийном пространстве и тому подобное, однако это не означает отсутствие подобных проблем в иных сферах общественной жизни. Также важно понимать, что многие технологические новшества имеют комплексный характер, сопряжены с вовлечением разнообразных информационных

и технологических решений, которые могут быть системами искусственного интеллекта, так и не являться таковыми, однако иметь общие проблемы и ограничения в правовом регулировании. Не последнюю роль в выявлении слабых мест в юридической регламентации общественных отношений имеют институты гражданского общества, нацеленность населения на защиту своих прав и свобод. С другой стороны, им нередко противостоят предпринимательская инициатива, открывающая новые технологии и продвигающие их на рынки сбыта, а также конкуренция в бизнес-среде («судиться может быть коммерчески выгодно»). В этом смысле системы искусственного интеллекта дают бизнесу преимущества, например, помогают в оптимизации расходов на отдельные производственные процессы, однако одновременно и создают потенциальные и фактические уязвимости правового статуса пользователей соответствующих продуктов. Наконец, не последнюю роль в правовом регулировании технологических новшеств имеют особенности организации самой судебной системы, которая должна позволять гибко реагировать на развитие современных технологий, находя необходимый баланс публичных и частных интересов.

Изучив массив судебных дел, сопряженных с использованием систем искусственного интеллекта (которых на данный момент уже без преувеличения тысячи), мы можем отметить, что наибольшее их количество распределено по трем главным категориям:

1) споры, сопряженные с принятием значимых решений системами искусственного интеллекта, чьи алгоритмы могут быть непрозрачны, предвзяты, иметь дискриминационный характер или не быть полностью подконтрольны человеку;

2) споры, связанные с нарушениями неприкосновенности частной жизни, обработкой персональных данных пользователей и их защитой от несанкционированного использования;

3) споры, сопряженные с производством системами ИИ результатов интеллектуальной деятельности, сопоставимых с результатами интеллектуальной деятельности людей. Перейдем к анализу названных категорий.

Принятие юридически значимых решений с помощью ИИ. Огромный пласт современных судебных дел поднимает вопрос о неправомерности использования технологий искусственного интеллекта для оценки социально значимого поведения человека. На текущий момент таковые уже используются в уголовном правосудии [3], налоговой сфере [4], социальном страховании, социальных услугах [5] и других сферах.

Еще в 2016 году в ходе проведенного журналистского расследования исследователи подвергли критике одну из таких систем. Дело в том, что с 1998 года в ряде штатов США (Нью-Йорк, Висконсин, Калифорния, и др.) судами использовалась интеллектуальная система COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) для прогнозирования вероятности повторного совершения осужденными лицами новых преступлений в случае применения к ним санкций, альтернативных лишению свободы, или досрочного освобождения. Исследование показало, что программа, использующая технологии искусственного интеллекта, выдавала вдвое больше ложных прогнозов в отношении

чернокожих людей по сравнению с белыми, при этом число таких ошибок превышало 7000 случаев [6].

Другим примером нарушения прав человека, обусловленного использованием систем ИИ, стало дело Баузерман (Bauserman) против Агентства по страхованию от безработицы (Unemployment Insurance Agency) [7], дошедшем до Апелляционного суда и Верховного суда штата Мичиган, США. В нем обжаловалась правомерность использования властями штата автоматизированной системы принятия решений MiDAS (Michigan Integrated Data Automated System). Указанная система по определенному алгоритму определила факты мошенничества со стороны тысяч людей, которые были дисквалифицированы и лишены права на получение пособия по безработице. В результате этого у истцов принудительно изымались возмещенные подоходные налоги и выплаченные пособия, а также удерживалась заработная плата, даже если «задолженностей на самом деле не было». Необходимо отметить, что в своих заключениях суды не пришли к выводу о неправомерности использования самой автоматизированной системы принятия решений, однако выявили нарушение в отсутствии уведомлений о таких действиях, автоматическом характере их исполнения, а также отсутствии возможности обжалования.

Отдельно отметим пусть и небольшую группу судебных процессов, в которых использование ИИ применялось для оценки обстоятельств спора, в том числе экспертной работе. На наш взгляд, названная категория дел имеет наибольший потенциал роста в виду возможностей ИИ производить комплексные исследования, оперируя большими объемами данных.

В деле Бертучелли (Bertuccelli) против Юниверсал Сити Студиос (Universal City Studios LLC) рассматривалась допустимость в качестве доказательства в исковом производстве о нарушении авторских прав показаний эксперта, основанных на анализе распознавания лиц с использованием искусственного интеллекта. Суд постановил, что показания доктора Эдварда Р. Гриффора, приглашенного истцом в качестве свидетеля-эксперта, допустимы. Предметом спора стало использование кинокомпанией изображения, защищенного авторским правом, в черной комедии 2017 года «Счастливого дня смерти» (англ. «Happy Death Day»), снятого режиссером Кристофером Бо Лэндоном на студии Blumhouse Productions.

Джонатан Бертучелли создал визуальное произведение, известное как «King Cake Baby» (KCB), которое представляет собой изображение младенца, используемое в виде пластиковой игрушки на празднике Марди Гра (фр. Mardi gras, аналог Масленицы в православии), отмечаемом во многих странах Европы, в США и в других странах. В своем исследовании доктор Гриффор провел анализ с помощью математического и целевого алгоритмов, используемого системой распознавания лиц, изображения младенца «King Cake Baby» и маски маньяка из вышеуказанного фильма с целью оценки того, являются ли с точки зрения человеческого восприятия представленные работы существенно похожими. Судом показания данного эксперта были приняты к рассмотрению, однако в конечном итоге стороны пришли к мировому соглашению, и дело было прекращено.

Обработка персональных данных с помощью систем искусственного интеллекта. Большой объем судебной практики составляют дела, в которых

наряду с вопросом о технологиях принятия решений системами искусственного интеллекта ставится также и вопрос о правомерности обработки ими персональных данных. К примеру, в деле Carpenter против McDonald's Corporation предметом обсуждения стал голосовой помощник, используемый в различных ресторанах McDonald's, в котором реализована технология распознавания голоса [8]. Значение судебного решения по этому делу состоит в установлении факта возможного нарушения прав человека подобными ассистентами, поскольку алгоритмы их работы позволяют собирать, сопоставлять или иным образом использовать образцы голосов пользователей.

Еще одним интересным делом, поднимающим вопрос о правомерности обработки персональных данных, является дело компании «Deliveroo Italy s.r.l.», оказывающей услуги по доставке еды и принадлежащей британской фирме Roofoods LTD. Итальянское управление по защите данных (Garante per la protezione dei dati Personali) в августе 2021 г. наложило на компанию штраф в размере 2,5 млн евро, установив в ее действиях факт незаконной обработки персональных данных примерно 8 000 курьеров, а также многочисленные нарушения Общего регламента ЕС по защите данных (GDPR). К основным нарушениям, допущенным Deliveroo, относились непрозрачность алгоритма управления рабочими сменами курьеров и непропорциональный сбор их личных данных, в том числе о платежных данных, сведений о транспортном средстве, а также местоположении курьера каждые двенадцать секунд [9].

ИИ и авторское право. Большую группу судебных споров, получающих распространение по всему миру и имеющих огромный потенциал роста в связи с распространением соответствующих технологий, образуют споры, относительно авторских прав на произведения, создаваемые с помощью систем искусственного интеллекта. Анализ массива изученных дел позволяет говорить, что предметом обсуждения может становиться как само авторство ИИ, так и неправомерное использование им чужих объектов интеллектуальной собственности, защищенных авторским правом. На текущий момент зарубежная судебная практика в этом отношении неединообразна.

В 2019 г. в Китае было принято судебное решение, подтвердившее, что созданное интеллектуальной системой текстовое произведение защищается как предмет авторского права. В деле Tencent против Shanghai Yingxun Technology Company [10] оспаривалась неправомерность использования статьи о состоянии фондового рынка, сгенерированной системой искусственного интеллекта «Dreamwriter». Ответчик, который опубликовал статью с таким же названием и примечанием в конце, указывающим на авторство ИИ, обосновывал, что произведение создано программой искусственного интеллекта, поэтому оно образует общественное достояние и может свободно распространяться без разрешения правообладателя. Суд с аргументами ответчика не согласился, установив нарушение авторских прав.

В отечественном информационном пространстве стал широко известен и другой случай: графический роман «Zarya of the Dawn», созданный Крис Каштановой (США) с помощью нейросети Midjourney. Текстовая и сюжетная части были полностью созданы человеком, а рисунки – вышеуказанной интеллектуальной

системой. Резонанс указанному случаю придало то, что первоначально, в сентябре 2022 года Бюро по авторским правам США защитило авторскими правами Крис Каштанову на все элементы данного графического произведения, однако позднее, в феврале 2023 года аннулировала лицензию, подтвердив право авторства за всем, кроме картинок, созданных Midjourney [11].

На данный момент в США сформировалось однозначное понимание того, что произведения, защищаемые авторским правом США, могут создаваться только человеком. В этом отношении характерны дела, инициированные д-ром Стивеном Талером в отношении Бюро по авторским правам США и Ведомства США по патентам и товарным знакам.

В первом деле 2018 года Стивен Талер обжаловал отказ Бюро по авторским правам США зарегистрировать авторские права на графическое произведение под названием «Недавний вход в рай», созданное программой искусственного интеллекта [12]. Ведомство по защите авторских прав отказалось зарегистрировать произведение на том основании, что оно не имеет авторства человека. Также был отклонен аргумент Талера о квалификации произведения, созданного ИИ, как работы, созданной по найму. Истец предпринимал попытки обжалования решения в порядке, предусмотренном Законом об административных процедурах США, однако в августе 2023 года по его делу требования также были отклонены [13].

Во втором деле д-р Стивен Талер пытался доказать и юридически закрепить в статусе изобретателя созданную им интеллектуальную систему DABUS (Device for the Autonomous Bootstrapping of Unified Sentience, устройство для автономной начальной загрузки унифицированного сознания). Истец утверждал, что в законе нет определения изобретателя или явного заявления о том, что изобретатель должен быть человеком, однако Ведомство США по патентам и товарным знакам отклонило его требование о регистрации, указав, что заявителем может быть только человек [14]. В своем решении судья отверг аргументацию истца о том, что на момент принятия закона не существовало таких технологий, поэтому и имеют место пробелы в законе [15]. Суд согласился с логикой патентного органа США, установившего неавтономность работы ИИ и аксиоматичность принадлежности изобретательства человеку.

В другом деле Andersen v. Stability AI Ltd [16], которое еще не получило своего завершения, поднимается важный вопрос о том, не нарушаются ли авторские права на произведения визуального искусства, используемых в качестве обучающих данных для инструментов создания изображений с помощью ИИ. Истцы (Sarah Andersen, Kelly McKernan, Karla Ortiz) подали коллективный иск к нескольким компаниям, создающим продукты генерации изображений (Stability AI, Ltd. Stability AI, Inc., Midjourney, Inc., and DevantArt, Inc.), заявляя о нарушении своих авторских прав. В жалобе утверждается, что ответчики скопировали изображения, чтобы использовать их в качестве обучающих данных. Полученные в результате инструменты генерации изображений с использованием искусственного интеллекта, по мнению истцов, позволяют пользователям создавать произведения искусства «в стиле» конкретных художников, что нарушает как Закон об авторском праве и право художников на гласность.

ИИ в практике российских судов. В заключение анализа современной судебной практики остановимся на опыте российских судов, сталкивающихся с подобными новшествами в своей деятельности. Отметим, что в настоящее время наработанная правоприменительная практика в России невелика, однако с каждым днем появляется все больше фактов рассмотрения дел, сопряженных с использованием интеллектуальных систем.

Нами были изучены десятки дел, рассмотренных в системе арбитражных судов России, в которых затрагивается использование искусственного интеллекта. Наибольшую долю из них составляют дела с участием ПАО «Сбербанк», связанные с использованием им «Робота-коллектора» для автоматического обзвона клиентов в целях возврата просроченной задолженности (таких дел насчитывается несколько сотен по всей России). Региональные управления Федеральной службы судебных приставов установили, что использование «Робота-коллектора» в подобных целях образует состав правонарушения, предусмотренного статьей 14.57 КоАП РФ («Нарушение требований законодательства о защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности») и наложили на ПАО «Сбербанк» административные штрафы. Во всех рассмотренных нами случаях суды встали на сторону ФССП, усмотрев в действиях истца нарушение Федерального закона от 3 июля 2016 г. № 230-ФЗ «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях». Суды не поддерживают аргументы ПАО «Сбербанк» о том, что выполнение роботом-коллектором звонков, имитирующих телефонный разговор в форме диалога, не требует заключения отдельного письменного соглашения об использовании такого способа взаимодействия, а значит, банк действовал не добросовестно и не разумно, злоупотреблял предоставленным правом [17].

Отдельную группу споров, рассмотренных отечественными судами, составляют споры, касающиеся использования субъектами предпринимательской деятельности интеллектуальных систем для автоматизации отдельных производственных процессов. В данном случае наиболее характерны, по нашему мнению, дела, инициированные истцами в отношении ООО «Вайлдберриз» в связи автоматическим назначением данной организацией и частичным удержанием штрафов в отношении предпринимателей-партнеров компании «за нарушение правил площадки» [18]. Суды усматривают в использовании систем искусственного интеллекта нарушение принципов добросовестного поведения участников коммерческих отношений, поскольку проведение проверок, наложение штрафов проводилось без учета особенностей каждого конкретного случая, при этом обжалование решений, вынесенных автоматически, было затруднительно, поскольку осуществлялось только через службу поддержки.

Наконец, еще одной характерной группой современных споров, с которыми сталкиваются отечественные суды, являются дела, связанные с продажей коммерческих продуктов, использующих технологии искусственного интеллекта для анализа больших объемов данных. Так, Арбитражным судом Республики Татарстан

только в 2023 году было рассмотрено несколько дел, в которых одним из элементов предмета спора, являлась неэффективность коммерческих программных продуктов, основанных на нейросетях и искусственном интеллекте и позиционируемых как системы прогнозирования выручки и продаж на маркетплейсах [19, 20]. Суды в рассмотренных нами делах не усмотрели оснований для признания исковых требований, установив, что в отсутствие доказательств умышленного введения ответчиками истцов в заблуждение признание неэффективности работы предлагаемой к использованию программы невозможно и соотносится с рисковым характером предпринимательской деятельности.

Заключение. Важно отметить, что количество судебных дел, связанных с использованием интеллектуальных систем, с каждым годом растет в геометрической прогрессии, однако их географическое распространение неравномерно. В первую очередь с юридическими коллизиями в указанной сфере сталкиваются государственные учреждения в странах, в которых развитие интеллектуальных систем получило наибольшее развитие, на данный момент это, прежде всего, США, страны Европейского союза, в последнее время в этом же контексте стал упоминаться и Китай.

Изучение рассмотренного нами и иного накапливающегося опыта имеет большое значение, поскольку позволяет установить потенциальные «болевые» точки как в российском законодательстве, так и в системе правового регулирования в целом. Также это позволяет установить перспективные направления развития права и юридической науки, поскольку, несмотря на особенности правовых систем отдельных государств современного мира пробелы и коллизии правового регулирования при их соприкосновении с новыми технологиями сталкиваются со схожими проблемами, требующими общего принципиального решения.

Список литературы

1. Мишель Бачелет призвала ввести мораторий на использование систем искусственного интеллекта. URL: https://news.un.org/ru/story/2021/09/1409912

2. Pause Giant AI Experiments: An Open Letter. URL: https://futureoflife.org/open-letter/pause-giant-ai-experiments

3. Borgesius F. Z. Discrimination, artificial intelligence, and algorithmic decision-making. URL: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73

4. Parks J. Nassau homeowners sue county over reassessment. URL: https://theislandnow.com/nassau-homeowners-sue-county-over-reassessment

5. Case No. 15-1390. Opinion: WALTER BARRY v. NICK LYON, in his official capacity as Acting Director, Michigan Department of Human Services. URL: https://www.courtlistener.com/opinion/4251251/walter-barry-v-nick-lyon

6. Angwin D., Larson D., Mattu S. and Kirchner L. Machine Bias. URL: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

7. Government's Use of Algorithm Serves Up False Fraud Charges. URL: https://undark.org/2020/06/01/michigan-unemployment-fraud-algorithm

8. Case: 1:21-cv-02906. COMPLIANCE WITH STATUTORY REQUIREMENTS: SHANNON CARPENTER, individually and on behalf of all similarly situated individuals, Plaintiff, v. MCDONALD'S CORPORATION, Defendant. THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS EASTERN DIVISION. URL: https://www.classaction.org/media/carpenter-v-mcdonalds-corporation.pdf

9. Algorithmic management in the gig economy. URL: https://www.michalsons.com/blog/algorithmic-management-in-the-gig-economy/66513

10. 深圳市南山区人民法院 (2019) 粤0305民初14010 ((2019) 粤0305民初14010号) //中国法律门户 CJO. URL: https://ru.chinajusticeobserver.com/law/x/2019-yue-0305-min-chu-14010

11. Cancellation Decision re: Zarya of the Dawn. URL: https://www.copyright.gov/docs/zarya-of-the-dawn.pdf

12. Case 1:22-cv-01564. COMPLAINT: Stephen Thaler, an individual Plaintiff, v. Shira Perlmutter THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF WASHINGTON D. C. URL: https://storage.courtlistener.com/recap/gov.uscourts.dcd.243956/gov.uscourts.dcd.243956.1.0.pdf

13. Case 1:22-cv-01564-BAH. MEMORANDUM OPINION: STEPHEN THALER, Plaintiff, v. SHIRA PERLMUTTER, Register of Copyrights and Director of the United States Copyright Office, et al. UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA. URL: https://storage.courtlistener.com/recap/gov.uscourts.dcd.243956/gov.uscourts.dcd.243956.24.0_2.pdf

14. Case 1:20-cv-00903-LMB-TCB. STEPHEN THALER vs. ANDREW HIRSHFELD / UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA Alexandria Division. URL: https://www.proskauerinlifesciences.com/wp-content/uploads/sites/34/2021/09/Thaler-v.-Hirshfeld.pdf

15. Karl F. Milde Can a computer be an author or an inventor? // Journal OF The Patent And Trademark Office Society. 1969. Vol 51. No 6. Рз. 378-405.

16. We've filed a lawsuit challenging Stable Diffusion, a 21st-century collage tool that violates the rights of artists. URL: https://stablediffusionlitigation.com

17. Постановление Третьего Арбитражного Апелляционного Суда от 07 сентября 2023 года по делу № А33-10303. URL: https://clck.ru/36p6WN

18. Решение Арбитражного суда Московской области от 06 сентября 2023 года по делу №А41-43556/23. URL: https://clck.ru/36p6Xm

19. Решение Арбитражного Суда Республики Татарстан от 16 августа 2023 года по делу № А65-36782/2022. URL: https://clck.ru/36p6YU

20. Постановление Одиннадцатого Арбитражного Апелляционного Суда от 03 августа 2023 года по делу № А65-6310/2023. URL: https://clck.ru/36p6Z7

А. В. Долбилов,
кандидат экономических наук,
Московский университет Министерства внутренних дел
Российской Федерации имени В. Я. Кикотя
К. А. Таран,
курсант,
Московский университет Министерства внутренних дел
Российской Федерации имени В. Я. Кикотя

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ЦИФРОВОЙ БЕЗОПАСНОСТИ В БАНКОВСКОМ СЕКТОРЕ

Аннотация. Статья посвящена проблеме обеспечения цифровой безопасности в банковском секторе и способам ее повышения. Сегодня оценка того, что киберпреступники представляют серьезную угрозу финансовой стабильности банковской системы и могут полностью ее дестабилизировать, является аксиомой – вопрос не в том, будет ли, а в том, когда. В последние десятилетия особое внимание уделяется информационной безопасности, в частности, всей банковской системы. Любая потеря данных, утечка информации, уничтожение информационных ресурсов и другие последствия кибератак, создают угрозу безопасности как граждан, так и банков, компаний, государства. Данная проблема достаточно актуальна, поскольку в условиях цифровизации общества хакеры разрабатывают различные способы хищения персональных данных и денежных средств. Также в результате исследования были представлены возможные инструменты, позволяющие минимизировать ущерб, причиненный кибератаками, путем быстрого реагирования на их возникновение.

Ключевые слова: кибербезопасность, кибератаки, преступления, банковские приложения, хакерство, цифровая безопасность, банковская деятельность, банковская операция, денежные средства, персональные данные

MODERN PROBLEMS OF DIGITAL SECURITY IN THE BANKING SECTOR

Abstract. The scientific article is devoted to the problem of ensuring digital security in the banking sector and ways to improve it. Today, the assessment that cybercriminals pose a serious threat to the financial stability of the banking system and can completely destabilize it is an axiom – the question is not whether, but when. In recent decades, special attention has been paid to information security, in particular, of the entire banking system. Any loss of data, information leakage, destruction of information resources and other consequences of cyber-attacks pose a threat to the security of both citizens and banks, companies, and the state. This problem is quite relevant, because in the conditions of digitalization of society, hackers are developing various ways of stealing personal data and money. Also, as a result of the study, possible tools were presented to minimize the damage caused by cyber-attacks by quickly responding to their occurrence.

Keywords: cybersecurity, cyber-attacks, crimes, banking applications, hacking, digital security, banking, banking operation, money, personal data

Параллельно росту числа онлайн операций и переходу к цифровым платежам увеличивается и уровень киберугроз. Указом Президента Российской Федерации № 203 была утверждена Стратегия развития информационного общества в Российской Федерации на период с 2017 по 2030 гг., которая предполагает цифровую трансформацию национальной экономики [7]. В результате чего банки становятся приоритетной целью для киберпреступников, что требует постоянного обновления мер безопасности. Банковский сектор все более полагается на новейшие технологии, такие как мобильные приложения и облачные сервисы, что, в свою очередь, увеличивает риски утечки персональных данных, повышает уровень информационной преступности, провоцирует создание новых схем мошенничества и возникновения других негативных последствий. Для подтверждения изложенного обратимся к статистическим показателям, которые были опубликованы 29 марта 2023 г. на сайте ведущего разработчика решений для кибербезопасности Positive Technologies. Так, в 2022 г. увеличилось количество инцидентов на 20,8 %, что связано с расширением теневого бизнеса, слабой цифровой безопасностью пользователей и ростом напряжения в киберпространстве. В 2023 г. эти же причины послужили еще большему росту числа атак [3].

Мировые и национальные органы начинают ужесточать требования к безопасности данных в финансовом секторе. Несоблюдение норм и стандартов может повлечь за собой серьезные юридические последствия, начиная с административной и заканчивая уголовной ответственностью. Утечки персональных данных и кибератаки серьезно подрывают доверие клиентов к банкам, в случае если это начинающий банк, то утрата доверия клиентов приведет к полному банкротству. Защита репутации стала критически важной для успешной деятельности как малых банков, так и крупных.

Для идентификации слабых мест в банковской системе России рассмотрим структуру объектов кибератак за 2016–2021 гг. (рис. 1) [1].

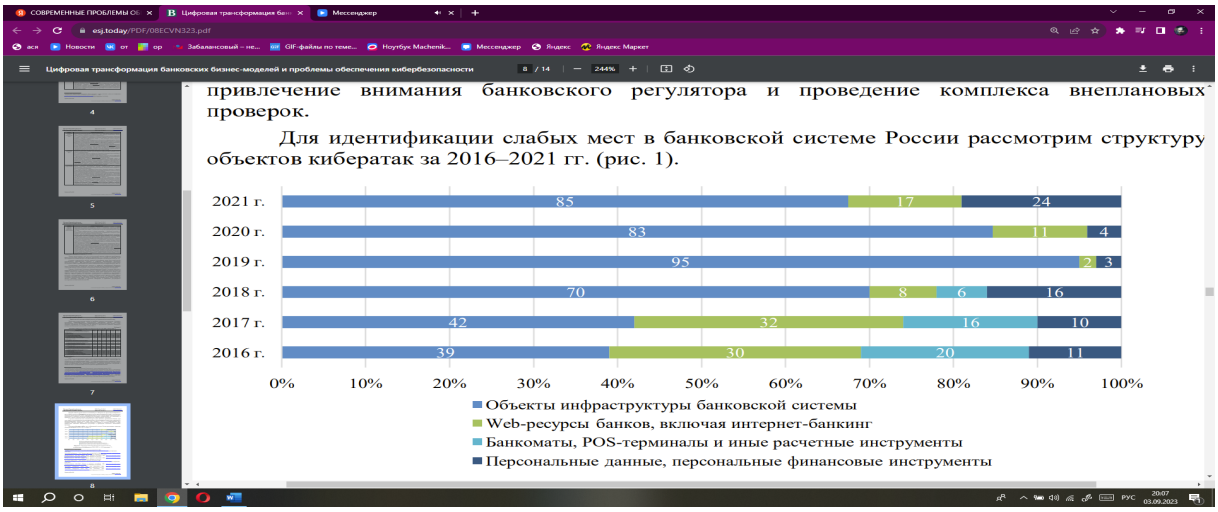

Рис. 1. Структура объектов банковской системы России, подвергавшихся кибератакам в 2016–2021 гг., в %.

Анализируя структуру объектов банковской системы, мы можем отметить, что начиная с 2017 года по 2021 год произошли значительные изменения, а именно начиная с 2018 года атакам киберпреступников стали активно подвергаться объекты инфраструктуры банковской системы. Также в последние года возрос интерес хакеров к персональным данным и Web-ресурсам банков, но интерес к объектам инфраструктуры также высок.

Выделив основные объекты банковской системы, которые подвергаются кибератакам следует рассмотреть популярные инструменты совершения исследуемых преступлений, что позволит нам выделить проблемные зоны банковского сектора (рис. 2) [2].

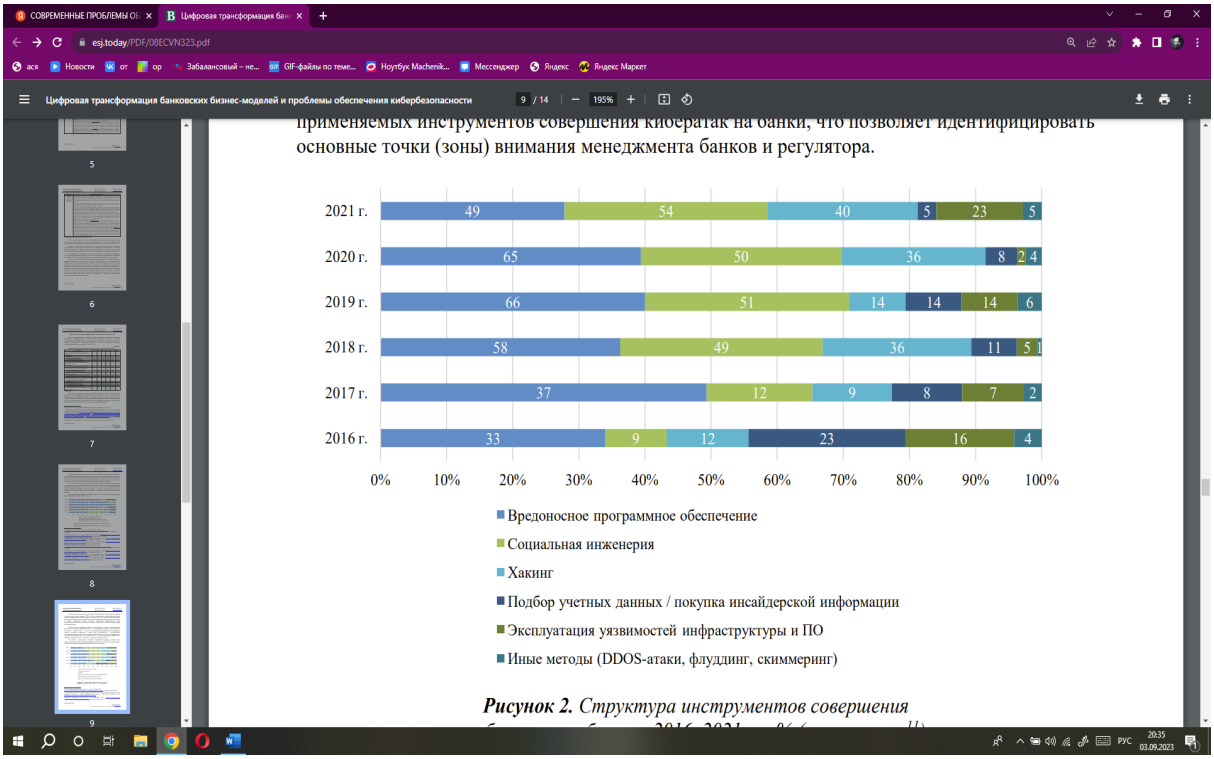

Рис. 2. Структура инструментов совершения кибератак на банки в 2016–2021 гг., %

Из предложенного рисунка следует, что основным источником угроз для российских банков является использование вредоносного программного обеспечения, которое было применено в 51 % всех атак. На втором месте находится социальная инженерия с 37 %, а на третьем месте – хакинг с 24 %. Большинство атак было направлено из США, ФРГ и Нидерландов, что может указывать на возможную политическую аффилиацию руководства этих стран.

В последнее время Центральный Банк России принимает меры для обеспечения кибербезопасности банковской системы, проводя мониторинг угроз и техническое обеспечение центра мониторинга и реагирования на компьютерные атаки, принимаются соответствующие нормативно-правовые акты, проводиться проверки, организуется сотрудничество с сотрудниками МВД России и многое

другое. Однако модель «держать врага снаружи» теряет свою эффективность в современном цифровом обществе, где практически любой гаджет, подключенный к Интернету, может стать инструментом преступления благодаря достижениям социальной инженерии [9. С. 8–9].

В результате чего, отметим, что слабых мест в банковской системе еще достаточно, требует предпринимать комплекс мер по борьбе с киберпреступностью, поэтому авторы предлагают:

1. Организовать взаимодействие банков с организациями ведущими разработку продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки. К таким организациям относятся: Positive Technologies, Iron BEES, Национальная компьютерная корпорация (НКК), Ланит, Softline и другими IT-компаниями. Такое взаимодействие позволит оснастить банковский сектор передовыми системами кибербезопасности, благодаря чему пользователи банков получат дополнительную защиту персональных данных, снизиться общий уровень утечек информации и многое другое. Благодаря общим усилиям будет развиваться социальная инженерия, будет обеспечено противодействие хакингу и действию вредоносного ПО. Также в случае, если стоимость услуг IT-компаний будет недоступно средним и малым бакам, тогда предлагается создать общую банковскую экосистему, на примере уже функционирующей в ПАО «СберБанк», и позволить средним и малым банкам вносить денежные взносы за пользование киберсистемой безопасности.

2. Одной из эффективных мер по обеспечению цифровой безопасности в банковском секторе может быть усовершенствование системы двухфакторной аутентификации (2FA, two-factor authentication) для операций, связанных с денежными переводами и платежами. Что позволит эффективно идентифицировать пользователя и защитить его от возможной утери персональной информации и других кибератак, связанных с фишингом и перехватом паролей [8. С. 1058–1059]. Совершенствовать исследуемую систему возможно посредством использования мультифакторной аутентификации. Это означает использование нескольких методов аутентификации, например, пароля и биометрической идентификации, для повышения безопасности. Также предлагается внедрить в систему двухфакторной аутентификации технологии блокчейн. Блокчейн-технология может использоваться для создания децентрализованной системы аутентификации, которая была бы более защищенной от хакерских атак.

3. Далее предлагается использовать методы анонимизации данных, чтобы предотвратить доступ к персональным данным пользователей в случае утечки информации. Важно также обеспечить регулярное обновление программного обеспечения и систем безопасности, чтобы минимизировать риски возникновения уязвимостей и предотвращать возможные атаки, благодаря чему система анонимизации пользователей будет работать эффективнее. Анонимность предполагает наличие допустимой пороговой величины для возможного сопоставления записей обезличенных и исходных данных. Дополнительными требованиями к обезличиванию относятся: возможность обратимости обезличенных данных, увеличение стойкости к деобезличиванию при увеличении объема и возможность обеспечить заданный уровень анонимности [4. С. 58].

4. Со стороны государства в лице ЦБ России предлагается разработать национальную линию информационной безопасности, в которую будут входить все банки России. Такая система должна предлагать специальное ПО и оборудование банкам по обеспечению кибербезопасности. При совместной работе банки смогут дополнительно обсуждать актуальные вызовы и угрозы, появиться возможность фиксировать все случаи информационных атак, которые некоторые малые банки скрывают. Так обратимся к мнению Г. Грефа, который отметил в своей статье о том, что более 80 % малых компаний или компаний нефинансового сектора скрывают факты кибератак и киберугроз в целях защиты авторитета [5]. Аналог такой системы – Великий Китайский файрволл, в которой около 700 тыс. пользователей и сама система базируется на анализе трафика, блокировке IP-адресов, перенаправлении поисковых запросов, блокировке виртуальных сетей и соединений (VPN) [6. С. 66].

5. Следует банковской системе обеспечить финансовую поддержку развитию инновационных технологий и развитие программ импортозамещения в сфере ИТК. Мера финансовой поддержки банками проектов по замене оборудования кибербезопасности может включать в себя предоставление кредитов на выгодных условиях, субсидирование части затрат на покупку комплектующего оборудования, а также проведение консультаций и обучения сотрудников студентов по вопросам перспективы разработки систем кибербезопасности. Кроме того, банки могут участвовать в государственных программах по поддержке цифровой безопасности и получать соответствующие гранты и субсидии. Важно, чтобы банки активно работали над улучшением своих систем безопасности и инвестировали в современные технологии, чтобы защитить своих клиентов и сохранить доверие общества к своим услугам. На практике также предлагается финансировать уже существующие проекты: АО «Российская венчурная компания», «Фонд Сколково», РФПИ с инновационной инфраструктурой.

6. На законодательном уровне предлагается разработать требования к минимальному уровню кибербезопасности участников банковской системы. Использование зарубежного опыта позволит создать эффективный правовой механизм регулирования минимальных требований к обеспечению кибербезопасности всеми банками Российской Федерации. В случае если возникает инцидент и банк не соблюдал установленные требования, следует привлекать к ответственности руководителей банка.

В заключении статьи отметим, что в современном мире цифровая безопасность является одной из ключевых проблем в банковском секторе. Кибератаки и хакерские атаки становятся все более сложными и угрожают не только конфиденциальности клиентов, но и финансовой устойчивости всей банковской системы. Поэтому, банки должны активно работать над улучшением своих систем безопасности и инвестировать в современные технологии, чтобы защитить своих клиентов и сохранить доверие общества. Взаимодействие банковской системы и IT-компаний позволит внедрить современные технологии по обеспечению кибербезопасности. Мера финансовой поддержки банками проектов по замене оборудования кибербезопасности может значительно помочь в этом процессе. Усовершенствование системы

двухфакторной аутентификации и использование методов анонимизации данных также позволят повысить эффективность защиты банковской системы от киберпреступников. Однако важно помнить, что безопасность – это постоянный процесс, который требует постоянного обновления и улучшения.

Список литературы:

1. Актуальные киберугрозы: итоги 2017-2021 годов. URL: https://www.ptsecurity.com/ruru/research/analytics/cybersecurity-threatscape-2021

2. Актуальные киберугрозы: итоги 2021 года. URL: https://www.ptsecurity.com/ruru/research/analytics/cybersecurity-threatscape-2021

3. Актуальные киберугрозы: итоги 2022 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022

4. Борисов Р. С., Ефименко А. А. протокол анонимизации наборов данных для публикации в открытых источниках // Правовая информатика. 2023. № 2. С. 54–66.

5. Греф Г. Более 80 % компаний скрывают факты кибератак. URL: https://tradersunion.ru/iaftnews/finance/news/335016

6. Иванов Д. И. Право на доступ в Интернет: модели правового регулирования // Актуальные проблемы становления и развития правовой системы российской Федерации: Сборник докладов VI Всероссийской научно-практической конференции студентов, магистрантов и аспирантов, Сыктывкар, 26–27 апреля 2022 г. Сыктывкар: Сыктывкарский государственный университет им. Питирима Сорокина, 2022. С. 65–69.

7. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента № 203 от 09.05.2017. URL: http://www.kremlin.ru/acts/bank/41919

8. Рязанова О. А., Бабикова Т. А. Новый формат работы банковского бизнеса: вызовы и перспективы // Общество. Наука. Инновации (НПК-2021): сборник статей XXI Всероссийской научно-практической конференции. В 2 т., Киров, 12–30 апреля 2021 г. Т. 1. Киров: Вятский государственный университет, 2021. С. 1055–1064.

9. Шкодинский С. В., Крупнов Ю. А., Толмачев О. М. Цифровая трансформация банковских бизнес-моделей и проблемы обеспечения кибербезопасности // Вестник евразийской науки. 2023. Т. 15, № 3. С. 1–14.

А. Е. Тарасова,
кандидат юридических наук, доцент,
Координационный совет при Правительстве Российской Федерации
по реализации Десятилетия детства

ЦИФРОВЫЕ ПРАВА И ПРАВО ПРАВ ЧЕЛОВЕКА

Аннотация. Целью исследования является определение источников международного и национального права в области прав человека и их защиты в связи с развитием цифровых технологий. Существенные особенности исследования заключаются в анализе актов мягкого права, актуальных тенденций развития

цифровых технологий и их влияния на поколения прав человека в международном праве. Приводятся примеры реализации международных стандартов в области прав человека в связи с цифровой средой на национальном уровне. Особое внимание уделяется влиянию цифровизации на права уязвимых категорий граждан, в частности несовершеннолетних, женщин, инвалидов, пожилых граждан.

Ключевые слова: право, цифровые технологии, интернет, искусственный интеллект, ребенок, уязвимые категории граждан, международные стандарты

DIGITAL RIGHTS AND HUMAN RIGHTS LAW

Abstract. The purpose of the study is to identify the sources of international and national law in the field of human rights and their protection in connection with the development of digital technologies. The essential features of the study are the analysis of soft law acts, current trends in the development of digital technologies and their impact on the generation of human rights in international law. Examples are given of the implementation of international human rights standards in relation to the digital environment at the national level. Special attention is paid to the impact of digitalisation on the rights of vulnerable categories of citizens, in particular minors, women, persons with disabilities, elderly citizens.

Keywords: law, digital technologies, internet, artificial intelligence, child, vulnerable categories of citizens, international standards

Введение. Сегодня, по оценкам, Интернетом пользуются 5,3 млрд человек, или 66 % населения Земли. В 2021 году этот показатель вырос на 6,1 % по сравнению с 5,1 % в 2020–2021 годах, самый большой процент роста 11 % составлял в 2019–2020 годах, наблюдавшийся в начале COVID-19. По данным Доклада Международного Союза электросвязи «Измерение цифрового развития: факты и цифры», 2022 г., – 2,7 млрд человек остаются без связи, что свидетельствует о том, как много еще предстоит сделать для достижения цели обеспечения универсальной и полноценной связи, которую Мир поставил перед собой на 2030 год.

В странах Европы, Содружества Независимых Государств (СНГ) и Северной и Южной Америки, Интернетом пользуется от 80 до 90 % населения, что приближается к универсальному значению (под которым в практических целях понимается уровень проникновения Интернета не менее 95 %).

Примерно две трети населения арабских государств и стран Азиатско-Тихоокеанского региона (70 и 64 % соответственно) используют Интернет, что соответствует среднемировому уровню, в то время как средний показатель для Африки составляет всего 40 % населения.

Всеобщее подключение к Интернету остается далекой перспективой и в наименее развитых странах и развивающихся странах, не имеющих выхода к морю, где в настоящее время только 36 % населения подключены к Интернету [13].

Интересным является соотношение пользователей Интернетом по возрастному критерию.

В 2022 году в мире 75 % людей в возрасте от 15 до 24 лет пользовались Интернетом, что на 10 процентных пунктов больше, чем среди остального

населения (65 %). Есть признаки того, что разрыв между поколениями сокращается. В 2020 году разница между уровнем проникновения Интернета среди молодежи (71 %) и остального населения (57 %) составлял 14 процентных пунктов. Во всех регионах мира люди в возрасте от 15 до 24 лет более подключены к Интернету, чем люди старшего или более молодого возраста (младше 15 лет). Универсальность, определяемая как более чем 95-процентное использование Интернета уже достигнута в этой возрастной группе в странах с высоким уровнем дохода и уровнем дохода выше среднего. Наибольший разрыв в относительном выражении наблюдается в странах с низкими доходами, где 39 % молодых людей пользуются Интернетом, в то время как среди остального населения этот показатель составляет лишь 23 % населения [13].

При этом на международном уровне нет специального международного договора или конвенции, определяющих международные стандарты в сфере развития и регулирования цифровых технологий, цифровых прав человека, защиты от киберпреступности и киберугроз.

Государствами ведется работа в рамках ООН по разработке конвенционных актов, достижением в этой сфере можно назвать работу над проектом всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях [2]. Конвенция разрабатывается как универсальный международный акт в связи с активным развитием информационно-телекоммуникационных технологий и различных угроз, которые цифровые достижения создают для населения государств Мира и национальной безопасности самих публичных субъектов. В проекте всеобъемлющей конвенции ее целями названы содействие принятию и укрепление мер, направленных на предупреждение киберпреступности (использования информационно-коммуникационных технологий в преступных целях) и борьбу с ней; поощрение, облегчение и укрепление международного сотрудничества в предупреждении киберпреступности и борьбе с ней; поощрение, облегчение и поддержка технической помощи в области предупреждения киберпреступности и борьбы с ней, особенно в интересах развивающихся стран, улучшение и стимулирование обмена информацией, знаниями, опытом и примерами успешной практики.

К важным аспектам проекта Конвенции относятся: принципы защиты суверенитета государств, их равенства и невмешательства во внутренние дела государств; соблюдение прав человека и всех международных обязательств государств в этой сфере. Проект Конвенции предусматривает специальные меры по защите детей от посягательств в Интернете и с помощью компьютерных систем (информационно-коммуникационных устройств).

Примечательно, что Российская Федерация в 2019 году выступила с инициативой создания профильного органа ООН для разработки всеобъемлющей международной конвенции. Была собрана поддержка мирового сообщества, предложены проекты резолюций Генеральной Ассамблеи ООН 74/247 и 75/282, регулирующие модальности Спецкомитета. Россия первой самостоятельно начала процесс разработки столь важного и требуемого временем международного договора, призванного поднять международное сотрудничество в этой сфере на качественно новый уровень [3].

По данным Министерства иностранных дел РФ работу над итоговым проектом международного соглашения планировалось завершить государствам в 2023 году в ходе 78-й сессии Генеральной Ассамблеи ООН. Уже 5 сентября текущего года 78 сессия Генассамблеи ООН начала свою работу [4] и только от совместных усилий государств зависит появление нового универсального всеобъемлющего международного документа, который может стать обязательным для стран Мира в Век цифровизации.

В настоящее время ведется продуктивная работа по согласованию государствами поправок и предложений по существу проекта конвенции, заслушиваются заявления государств, научных учреждений, организаций гражданского общества, различных структур частного сектора, о чем свидетельствуют результаты работы шестой сессии Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях ГА ООН, 21 августа – 1 сентября 2023 г.

В основном регулирующее воздействие и выработка международных стандартов в связи с развитием цифровых технологий осуществляется в рамках динамичного толкования имеющихся международных договоров в сфере прав человека, а также на уровне актов мягкого права, принимаемых международными органами в рамках международных организаций.

В связи с этим в доктрине ведется дискуссия о природе цифровых прав. Многие исследования посвящены цифровым правам на отраслевом уровне, в области частного права [8], либо регулированию цифровых технологий в институтах публичного права [12], некоторые работы посвящены проблемам защиты прав отдельных категорий граждан в цифровой среде [14]. Доктринальные исследования проводятся по теме соотношения цифровых прав и международного права [10; 11], выдвигаются позиции о формировании новых поколений и видов прав человека в международном праве прав человека, предлагаются поколения цифровых прав [9; 18].

Digital human rights предлагается относить к пятому поколению прав человека, допуская развитие существующей институциональной структуры международного права прав человека, дополнение имеющейся системы правами новых поколений. Например, наряду с первым поколением прав – «гражданские и политические права человека», получили развитие права второго поколения – «экономические, социальные и культурные права». Признается становление третьего поколения прав – коллективные права или «права солидарности» (права народов, развитие концепция международной солидарности, рассмотрение семьи как коллективного субъекта права [6]). К правам данного поколения обычно относят право на развитие, право на мир, право на самоопределение, территориальную целостность, право на здоровую окружающую среду, право на суверенитет.

Научно-технический прогресс обусловил появление четвертого поколения прав человека – «соматические права», среди которых такие биомедицинские категории, как право на донорство и трансплантацию органов и тканей, смену пола, репродуктивные права, право на смерть, на криоконсервацию.

Примечательно, что все или большинство (по этому вопросу ведется научно-практическая дискуссия) прав первого, второго, третьего и даже четвертого поколения могут быть реализованы в цифровой среде или приобрести цифровую форму. В период пандемии Covid, когда стремительно выросло число пользователей интернета, получили свою реализацию – право на online-труд, smart-родительство (общение с ребенком/детьми с помощью digital technologies не сделавшего прививку от вируса родителя или родителей в ситуации локдауна в трансграничных семьях), «дистанционное» зачатие [1].

Несмотря на активное вовлечение изначально сформировавшихся и получивших признание, на национальном и международном уровнях, как не цифровые, не предназначенные для цифровой среды и не связанные с информационно-коммуникационными технологиями прав человека в online-формат, дискуссия о развитии нового пятого поколения прав человека, именно как цифровых правах, набирает обороты.

Среди прав пятого поколения предлагается рассматривать – право на доступ в Интернет; право на конфиденциальность (шифрование); право на забвение в Интернете («the right to be forgotten»); право на защиту персональных данных, включая биометрические, в цифровой среде; право на создание, пользование и доступ к информационно-коммуникационным технологиям; право на цифровую идентификацию; цифровые права, связанные с «квази-субъектом» – искусственным интеллектом и др.

В иностранной доктрине к цифровым правам относят право на защиту человека от манипулирования его желаниями, мыслями и мнениями (to shield individuals against undue manipulation of their wishes, thoughts, and opinions) [15]; право не подчиняться алгоритмическим решениям (the right not to be subject to algorithmic decisions) [17].

Зарубежные авторы представили классификацию цифровых прав, разделяемых по нескольким поколениям, аналогично поколениям прав человека, получающим закрепление в сложившейся, на базе Всемирного Билля о правах, системе. Например, выделяют три поколения собственно цифровых прав – типология «трех поколений».

Первое поколение, по мнению авторов, предполагает радикальное переосмысление существующих прав человека, чтобы позволить им соответствовать новым условиям цифровой эпохи. Права первого поколения, согласно данной концепции, могут в некоторых отношениях быть своего рода продолжением исходных прав человека и обычно совпадают даже по названию с ними, примером служат информационные права.

Второе поколение предполагает развитие новых отличающихся цифровых прав человека, соответствующих новым потребностям и интересам онлайн-пользователей. Эти права второго поколения, в отличие от первого, не имеют близких аналогов в офлайн-мире. К данному поколению относят – право на доступ в Интернет, право на информационное самоопределение (a new right to informational self-determination), новое право не подвергаться автоматическим решениям по важным (существенным) вопросам.

Третье поколение предполагает признание новых правообладателей и новых носителей обязанностей, т. е. речь идет о новой субъектности. Признание цифровых прав такого поколения представляет собой существенную трансформацию концепции прав человека и системы международного права прав человека, поскольку речь идет о правах, принадлежащих «онлайн-людям». Указанные цифровые права отделены от прав, которыми пользуются физические лица, создавшие digital-субъектов или управляющие ими. Данный шаг в направлении изобретения новой категории «правосубъектности» должен основываться на поддержке прежде всего национальными государствами и относиться в доктрине к вопросу политического обоснования. Для сравнения авторы приводят произошедшее в свое время в частном праве (private law) наделение юридическими правами корпораций и других юридическим лиц [18], как искусственно созданных субъектов, вспомним теорию фикции.

На наш взгляд, можно было бы использовать не термин «поколение» к цифровым правам, чтобы избежать путаницы со сложившейся структурой международного права прав человека, а более подходящий термин – «измерение» для digital rights.

В соответствии с Резолюцией Генеральной Ассамблеи ООН от 25 августа 2023 г. A/RES/77/326 период 2024-2033 гг. провозглашен в качестве «Международного Десятилетия наук» в интересах устойчивого развития, чтобы предоставить человечеству уникальные возможности научных достижений для решения сложных проблем современности, обеспечения всем в будущем безопасности и процветания. По существу, это новые ориентиры для периода пост-достижений Целей устойчивого развития (напомним, что Цели устойчивого развития рассчитаны до 2030 года).

Учитывая продолжающийся научно-технический прогресс и международный курс на развитие наук в ближайшее Десятилетие, цифровые технологии, искусственный интеллект будут только набирать обороты, что требует переосмысления всей структуры прав человека на международном уровне и политических решений государств на национальном уровне, поскольку права человека в связи с цифровой средой или «цифровые права человека» не должны быть исключены из действующих механизмов правовой защиты и оказаться лакуной права прав человека.

Основная часть. В резолюции, принятой Советом по правам человека ООН 14 июля 2023 г. «Новые и появляющиеся цифровые технологии и права человека» отмечается что с учетом подхода, заложенного во Всеобщей Декларации прав человека, 75-летие которой празднуется в 2023 году, необходимо исходить из универсальности, неделимости, взаимозависимости и взаимосвязанности всех прав человека и основных свобод. При этом те же права, которые применяются в режиме офлайн, действуют и в режиме онлайн.

В рамках Организации объединенных наций идет процесс разработки «глобального цифрового договора», который запланирован для согласования государствами на Саммите будущего в сентябре 2024 г. Генеральным секретарем ООН предлагается, чтобы в этом договоре нашли закрепление принципы, задачи

и действия по продвижению «ориентированного на человека цифрового будущего, которое основывается на всеобщих правах человека и позволяет достичь целей в области устойчивого развития».

Разработка глобальных актов (как мягкого права, так и декларативного или в перспективе обязательного характера) в сфере цифровых технологий вызвана, с одной стороны, их интенсивным развитием, с другой стороны, новыми рисками и проблемами для защиты прав человека, включая выход из-под территориального национального воздействия государств технологических и IT компаний.

Позитивные аспекты в сфере цифровизации. Новые и появляющиеся цифровые технологии могут содействовать усилиям по ускорению человеческого прогресса, поощрению и защите прав человека и основных свобод, включая экономические, социальные и культурные права (актуальность которых повышается в самые кризисные времена), обеспечению преодоления всех цифровых разрывов, поддержке осуществления прав лиц с инвалидностью, граждан, находящихся в уязвимом или маргинализированном положении, расширению прав и возможностей всех женщин и девочек и гарантированию того, чтобы «никто не был забыт в процессе достижения целей в области устойчивого развития».

«Ассистивные технологии», как разновидность современных достижений, особенно способствуют полному осуществлению прав человека людьми с инвалидностью.

Системы искусственного интеллекта, при наличии адекватных гарантий, имеют потенциал для поощрения, защиты и осуществления прав человека, особенно экономических, социальных и культурных, путем облегчения доступа к информации и участия граждан в общественной жизни, повышения эффективности и доступности различных услуг – здравоохранения, обеспечения более широкого наличия и доступности образования, расширения прав и возможностей женщин любого возраста, содействия полному осуществлению прав пожилыми людьми, гражданами с инвалидностью и находящимися в уязвимом положении, укрепления мер по смягчению последствий изменения климата и адаптации к нему, охраны окружающей среды.

Риски в области развития информационных технологий и недостатки правового регулирования. Риски, которые новые и появляющиеся цифровые технологии несут для защиты, поощрения и осуществления прав человека (права на жизнь, на равенство и недискриминацию, на свободу мнений; право искать, получать и распространять информацию; права на свободу мирных собраний и свободу ассоциации; право на эффективное средство правовой защиты; экономические, социальные и культурные права, включая право каждого человека на наивысший достижимый уровень физического и психического здоровья; права детей на защиту от насилия, жестокого обращения, отсутствия заботы и сексуальной эксплуатации; право на неприкосновенность частной жизни) в соответствии с обязательствами государств по международному праву прав человека, включают:

– дискриминацию;

– цифровые разрывы, возрастные, связанные с инвалидностью, гендерные, географические, городские и сельские, что может отражать и усиливать существующее социальное, культурное и экономическое неравенство;

– недопредставленность женщин в секторах науки, технологии, инженерного дела и математики, ограничение их участия в проектировании и разработке новых технологий;

– отсутствие адекватного регулирования, эффективных мер по предотвращению, смягчению и устранению неблагоприятного воздействия технологий на права человека в соответствии как с обязательствами государств по международному праву прав человека (обязательные нормы международных договоров), так и обязанностями предприятий согласно Руководящим принципам предпринимательской деятельности в аспекте прав человека (акт мягкого права для бизнеса);

– системы искусственного интеллекта, используемые без надлежащих гарантий, для идентификации, отслеживания, профилирования, распознавания лиц, создания синтетических, фотореалистичных изображений, прогнозирования поведения или выставления оценок лицам, создают серьезные риски для защиты, поощрения и осуществления прав человека (права на неприкосновенность частной жизни, на свободу мнений и их свободное выражение, на свободу мысли, совести и религии, права на равную защиту закона и на справедливое и публичное разбирательство дела, экономические, социальные и культурные права) за счет – a) укоренения и усиления предвзятости, что может приводить к дискриминации и неравенству; b) обострения угроз, связанных с ложной информацией, дезинформацией и языком ненависти, приводящих к насилию, включая политическое; c) неприемлемого риска для прав человека некоторых видов применения искусственного интеллекта;

– отсутствие целостного понимания технологии и единых усилий по регулированию цифровых технологий, искусственного интеллекта и управлению ими на международном и национальном уровнях.

Необходимые меры на международном и национальном государственном уровне для защиты прав человека в связи с цифровыми технологиями:

– обеспечение надлежащих гарантий и человеческого надзора при применении новых и появляющихся цифровых технологий, обеспечения уважения и поощрения прав человека в национальных, региональных и международных нормативных правовых рамках, законодательстве и в процессе концептуальной проработки, дизайна, использования, развития, дальнейшего внедрения и оценки воздействия новых и появляющихся цифровых технологий;

– установление технических стандартов для цифровых технологий при обеспечении значимого участия всех заинтересованных сторон, в том числе частный сектор, научные круги, средства массовой информации и гражданское общество;

– на национальном уровне отводить правам человека центральное место в нормативной правовой базе по вопросам разработки и использования цифровых технологий;

– на международном уровне создать общесистемное руководство «по вопросам должной осмотрительности» в области прав человека и оценки воздействия при использовании новых технологий (акт мягкого права с перспективами формирования обязательных стандартов для расширенного круга субъектов, учитывая экстерриториальность цифровых технологий и Интернета).

Заключение. На международном уровне предлагается обратить внимание на следующие аспекты повышенной защиты в области прав человека:

– защита людей от вреда, причиняемого системами искусственного интеллекта,

– обеспечение безопасности систем искусственного интеллекта;

– защита лиц от дискриминации, например путем обеспечения того, чтобы данные, используемые при обучении алгоритмов, являлись точными, актуальными, репрезентативными и проверенными на предмет «закодированной предвзятости»;

– содействие прозрачности систем искусственного интеллекта, обеспечение адекватной объяснимости решений, поддерживаемых искусственным интеллектом с учетом различных уровней рисков, возникающих в связи с технологиями, для прав человека;

– укрепление надзорного и правоприменительного потенциал государств по отношению к AI и секторам, где он применяется с создание более эффективных мер по защите от рисков для прав человека, связанных с AI;

– содействие проведению исследований, обмену передовым опытом по вопросам прозрачности, человеческого надзора и подотчетности в отношении применения систем искусственного интеллекта с целью предотвратить и избежать распространение дезинформации и языка ненависти,

– повышение эффективности работы международных органов, в частности, Совета по правам человека ООН, договорных органов с целью поощрения и защиты прав человека в контексте новых и появляющихся цифровых технологий целостным, всеобъемлющим и инклюзивным образом.

В ноябре 2021 г. 193 государства в ходе Генеральной конференции ЮНЕСКО приняли «Рекомендацию по этическим аспектам искусственного интеллекта» [16] – первый глобальный нормативный документ в этой области. Рекомендация направлена как на защиту, так и на поощрение прав человека, человеческое достоинство и выступает этическим ориентиром, глобальной нормативной основой, направленной на строгое соблюдение принципа верховенства права в цифровом мире.

На универсальном уровне можно выделить следующие наиболее современные акты мягкого права в области цифровых технологий и их влияния на права человека, принятые международными договорными органами как в общем контексте, так и для защиты наиболее уязвимых категорий:

Замечание общего порядка № 25 (2021) о правах детей в связи с цифровой средой, Комитета по правам ребенка ООН;

Замечание общего порядка № 25 (2020) о науке и экономических, социальных и культурных правах (пункты 1 b), 2, 3 и 4 статьи 15 Международного пакта об экономических, социальных и культурных правах) Комитета по экономическим, социальным и культурным правам ООН.

Указанные акты оказали влияние на разработку на национальном уровне Стратегии комплексной безопасности детей в РФ на период до 2030 г. [7] и обновленной Концепции информационной безопасности детей в РФ с 2023 г. [5].

Цифровая безопасность детей и кибербезопасность – взаимосвязанные понятия, основные аспекты их соотношения можно обозначить следующим образом:

1. Правовые решения для органов власти, IT и технологических компаний, образовательных организаций и законных представителей несовершеннолетних для защиты детей:

– от недостоверной информации в Интернете (защита от дезинформации);

– от кибер-агрессии, эксплуатации и преступных посягательств с использованием цифровых технологий и в Интернете;

– персональных данных, частной жизни детей – принцип минимизации данных (обеспечение неприкосновенности в широком и узком значении);

– от незаконного использования данных о детях («встроенные алгоритмы конфиденциальности») – речь идет о защите данных, собираемых организациями, оказывающими услуги и работающими с детьми;

2. Цифровые навыки детей и контроль:

– предназначена или нет цифровая среда для детей (определение возраста доступа, развитие digital skills);

– информированное и отзывное согласие детей и их законных представителей при применении цифровых технологий, Интернета, совершения действий в online-среде;

– соответствие Конвенции ООН о правах ребенка 1989 г., принимаемых ограничений на функционирование любых основанных на интернет-технологиях, электронных или других систем распространения информации (недопустимость непропорционального ограничения права ребенка на игру и доступ к информации и online-ресурсам);

– контроль родителей и лиц, осуществляющих уход за ребенком, за его цифровой деятельностью: соразмерность и соответствие развивающимся способностям несовершеннолетнего (ст. 5 Конвенции ООН о правах ребенка – «принцип развивающихся способней ребенка»);

3. Цифровая идентификация детей: pro et contra

– использование онлайн-аватаров или псевдонимов для защиты личности ребенка;

– защита традиционных духовно-нравственных ценностей и кибербезопасность: баланс правового регулирования;

4. Защита от новых форм насилия в цифровой среде, к примеру кибер-агрессии, кибератак, «информационной войны», вербовки.

5. Smart – родительство и кибербезопасность (развитие отношений дистанционного общения в семье. Согласно Докладу Генерального секретаря ООН «Реализация целей Международного года семьи и связанных с ним последующих процессов» A/77/61–E/2022/4, представленному в 2022 г., новые технологии являются одной из Мега-тенденций, влияющих на институт семьи. Использование технологий в семьях способствует связанности и сплоченности членов семьи путем содействия внедрению новых видов общения и совместного времяпрепровождения. Цифровые технологии являются особенно полезными для решения проблем речевой коммуникации, в семьях с детьми-инвалидами. Главными технологическими тенденциями за последние годы в Докладе названы: стремительные улучшения в сферах деятельности больших данных, машинного обучения, «Интернета

вещей», AI и облачных вычислений. К последним тенденциям, повлиявшим на семьи во всем Мире, относятся on-line обучение, дистанционная работа, получившие широкое распространение в условиях, когда из-за пандемии люди стали абсолютно по-другому преподавать, учиться, работать и жить);

6. Право на игру и поощрение инноваций в области цифровых игр и связанных с ними видов деятельности, способствующих самостоятельности детей, их личностному росту, развитие кибер-спорта;

7. Дети-киберпреступники (дети могут подозреваться/быть обвинены/ признаны виновными в нарушении законов о киберпреступности) – в этой сфере необходимо определение возраста ответственности, ее видов, создание восстановительного правосудия для несовершеннолетних и специальных цифровых служб, которые компетентны в области развивающихся технологий и защиты от киберугроз.

Список литературы

1. Зачатие по интернету: британка родила благодаря набору для оплодотворения с eBay. URL: https://bigpicture.ru/zachatie-po-internetu-britanka-rodila-blagodarja-naboru-dlja-oplodotvorenija-s-ebay/?ysclid=lmcggiyoao877289933

2. О пятой сессии Спецкомитета ООН по разработке всеобъемлющей конвенции о противодействии использованию информационно-коммуникационных технологий (ИКТ) в преступных целях. URL: https://www.mid.ru/ru/foreign_policy/news/1865216

3. О внесении в Спецкомитет ООН российского проекта универсальной международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях. URL: https://www.mid.ru/ru/foreign_policy/news/1770170

4. О начале работы 78-й сессии Генеральной Ассамблеи ООН. URL: https://www.mid.ru/ru/foreign_policy/news/1902714

5. Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р: Распоряжение Правительства РФ от 28.04.2023 № 1105-р // Собрание законодательства РФ. 2023. № 19. Ст. 3481.

6. Подготовка к тридцатой годовщине Международного года семьи в 2024 г.: Резолюция Генеральной Ассамблеи о подготовке к тридцатой годовщине Международного года семьи и ее праздновании A/RES/77/191. URL: https://social.desa.un.org/issues/family/news/preparations-for-the-thirtieth-anniversary-of-the-international-year-of-the

7. О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года: Указ Президента РФ от 17.05.2023 № 358 // Собрание законодательства РФ. 2023. № 21. Ст. 3696.

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

9. Тарасова А. Е., Лысова Я. В. Цифровые права как новое поколение прав человека в системе международного права в сфере прав человека // Вестник Юридического факультета Южного федерального университета. 2023. Т. 10, № 1. С. 87–95.

10. Burchardt, D. Does Digitalization Change International Law Structurally? // German Law Journal. 2023. Vol. 24(3). P. 438–460.

11. Burchardt, D. Editorial to the Special Issue "The Impact of Digitalization on International Law" // German Law Journal. 2023. Vol. 24(3). P. 435–437.

12. De Gregorio, G. Digital Constitutionalism, Privacy and Data Protection. In Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society // Cambridge Studies in European Law and Policy. Cambridge: Cambridge University Press, 2022. Pp. 216–272.

13. ITU's annual Facts and Figures report. URL: https://www.itu.int/itu-d/reports/statistics/2022/11/24/ff22-foreword

14. Khisamova R. V. Children and Internet: Cyber Threats Sorts and Ways of Protection // Legal Issues in the Digital Age. 2023. Vol. 4. № 2. Pp. 122–141.

15. Ienca M., Andorno R. Towards New Human Rights in the Age of Neuroscience and Neurotechnology // LIFE SCI. SOC. POL'Y. 2017. Vol. 1. Pp. 11–15.

16. Recommendation on the Ethics of Artificial Intelligence. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137

17. Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), art. 21, OJ L 119/1 (2016). URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679

18. Shany, Y. Digital Rights and the Outer Limits of International Human Rights Law // German Law Journal. 2023. Vol. 24(3). Pp. 461–472.

Е. Ю. Тихалева,
кандидат юридических наук, доцент,
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации,
Среднерусский институт управления – филиал

РАЗВИТИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РОССИЙСКОЙ ФЕДЕРАЦИИ НА СОВРЕМЕННОМ ЭТАПЕ

Аннотация. Целью проведенного научного исследования является характеристика ключевых тенденций внедрения института искусственного интеллекта в жизнедеятельность российского общества. Рассматриваются поступательные шаги правового регулирования и практической деятельности в области искусственного интеллекта, сделанные и актуальные в 2023 году. Подчеркивается значимость правового регулирования искусственного интеллекта на законодательном уровне. Дается оценка дальнейшего возможного развития данной сферы.

Ключевые слова: право, искусственный интеллект, национальные проекты, мониторинг, цифровые технологии, беспилотные летательные аппараты, робототехника

DEVELOPMENT OF ARTIFICIAL INTELLIGENCE IN THE RUSSIAN FEDERATION AT THE PRESENT STAGE

Abstract. The purpose of the exploration is to characterize the core trends in the integration of the Institute of artificial Intelligence in the life of Russian society. The author examines the progressive steps of legal regulation and practical activities in the area of artificial intelligence, made and relevant in 2023. The importance of legal regulation of artificial intelligence at the legislative level is emphasized. An assessment of the further possible development of this sphere is given.

Keywords: law, artificial intelligence, national projects, monitoring, digital technologies, unmanned aerial vehicles, robotics

В январе 2023 г. Президентом Российской Федерации был утвержден перечень поручений как итог проведения конференции «Путешествие в мир искусственного интеллекта в ноябре 2022 года [4].

В частности, Правительству Российской Федерации был дан ряд поручений, а именно:

– утвердить федеральный проект по развитию отечественной робототехники;

– внести в национальные проекты, а также государственные программы изменения либо дополнения, которые подразумевают использование технологий искусственного интеллекта. Возникает вопрос, по каким критериям должны вносится указанные изменения, а также не приведет ли их повсеместное внедрение к перегруженности программ и бездумному использованию современных средств;

– утвердить требования по обязательному использованию хозяйствующими субъектами современных технологий, включая выделение им субсидий из государственного бюджета. Так, на 2024 год – это 5,26 млрд рублей [3]. Например, Минэкономразвития России выделит гранты на внедрение подобных технологий компаниям, принимающим участие в реализации национального проекта «Производительность труда»;

– подготовить изменения применительно к образовательным программам высшего образования и программам повышения квалификации в отношении повышение уровня компетенций в сфере искусственного интеллекта. В 2023 году 3 000 человек обучаются по соответствующим программам высшего образования; почти 2 000 человек обучаются в рамках дополнительного профессионального образования;

– осуществить мониторинг применения искусственного интеллекта – так называемый «индекс интеллектуальной зрелости». Этим на сегодняшний день занимается Национальный центр развития искусственного интеллекта при Правительстве Российской Федерации (НЦРИИ). Индекс будет представлен в конце года на конференции AI Journey. Предполагается в качестве

критериев учитывать: качество управления, эффект от внедрения искусственного интеллекта в государственном и муниципальном управлении, а также в градообразующие частные компании; количество стартапов в сфере искусственного интеллекта; вклад науки в развитие искусственного интеллекта;

– увеличить список территорий, в пределах которых развиваются соответствующие эксперименты с внедрением беспилотных летательных аппаратов. Так, 18 субъектов Российской Федерации подали заявки на создание научно-производственных центров по развитию беспилотников в течение двух последующих лет. Запланировано создать 8 центров, в последующем расширить их количество до 35;

– подготовить рейтинг вузов применительно к качеству обучения специалистов в сфере искусственного интеллекта. Данное поручение выполняется совместно с Альянсом в сфере искусственного интеллекта. Ранее подобный рейтинг составляла компания «Руссофт». Аналоги есть и за границей – рейтинг британского издания Times Higher Education [7];

– осуществлять реализацию самых успешных практик применения технологий искусственного интеллекта в административно-территориальных единицах – субъектах Российской Федерации. К примеру, доклады в этой области готовит АНО «Цифровая экономика».

В настоящее время подготовлен проект обновленной национальной стратегии искусственного интеллекта, который должны представить Президенту Российской Федерации в ноябре 2023 года. Осуществляется отбор шести научно-исследовательских центров, которые получат государственную поддержку на следующие три года.

Кроме того, на совещании с членами Правительства Российской Федерации в июле 2023 года Президент В. В. Путин среди поручений в области искусственного интеллекта обозначил меры поддержки отечественных разработок в сфере искусственного интеллекта, а также необходимость: расширения количества компаний с государственным участием, использующих технологии искусственного интеллекта; упрощения возможности доступа к правовым режимам в области различных цифровых инноваций; внедрения института страхования ответственности за предполагаемый или реальный возможный ущерб при применении искусственного интеллекта [6].

Таким образом, в России пока отсутствует полноценный закон об искусственном интеллекте. Регулирование в основном осуществляется на подзаконном уровне, однако в прессе имеются заявления о разработке такого акта, в частности от заместителя министра Минцифры России [5]. Необходимость в принятии такого закона очевидна. Практика зарубежных государств показывает его действенность (Южная Корея [1. С. 39–40], Европейский Союз [2. С. 25]).

В качестве основных перспективных направлений развития российского искусственного интеллекта можно назвать активную поддержку со стороны государства, предоставление инвестиций компаниям-разработчикам, ориентацию вузов на подготовку соответствующих специалистов и обмен опытом на всех уровнях взаимодействия.

Список литературы

1. Волощак В. И., Козлов Л. Е., Валитова Д. В., Сарбаш Д. В. Цифровая экономика и искусственный интеллект в Республике Корея: практика политико-правового воздействия // Азиатско-Тихоокеанский регион: экономика, политика, право. 2022. Т. 24, № 4. С. 35–48.
2. Кильдиярова Р. А., Иксанов Р. А., Хужин Р. А. Правовое регулирование отношений с участием искусственного интеллекта // Международный журнал гуманитарных и естественных наук. 2021. № 5-4 (56). С. 24–29.
3. Об утверждении Правил предоставления субсидии из федерального бюджета на поддержку некоммерческой организацией Фонд развития Центра разработки и коммерциализации новых технологий пилотных проектов апробации технологий искусственного интеллекта в приоритетных отраслях: Постановление Правительства РФ от 21.05.2021 № 767. URL: https://www.garant.ru/products/ipo/prime/doc/400697482/?ysclid=llm3ioza6c948708854#review
4. Перечень поручений по итогам конференции «Путешествие в мир искусственного интеллекта» (утв. Президентом РФ 29.01.2023 № Пр-172). URL: https://www.consultant.ru
5. Правительство разработает закон об искусственном интеллекте // РБК. URL: https://www.rbc.ru/rbcfreenews/649b950c9a794732a27a407b
6. Совещание с членами Правительства // Сайт Президента России. URL: http://www.kremlin.ru/events/president/news/71699
7. World University Rankings 2023 // Times Higher Education. https://www.timeshighereducation.com/world-university-rankings/2023/world-ranking

Ш. Р. Хайитов,
доцент,
Ташкентский государственный юридический университет

ЭКСПЕРИМЕНТАЛЬНЫЙ ПРАВОВОЙ РЕЖИМ И ЦИФРОВИЗАЦИЯ ПРАВА

Аннотация. В статье анализируются подходы ученых-правоведов к предмету регулятивная песочница – “Regulatory Sandbox” и выдвигается идея о том, что всестороннее изучение компетенции, прав и обязанностей в сфере экспериментальных правовых режимов позволяют лучше понять суть проблемы применения экспериментальных правовых режимов, его эффективную реализацию на практике также были затронуты вопросы введения регулятивной песочницы в Узбекистане.

Ключевые слова: эксперимент, правовой эксперимент, регулятивная песочница, законодательные акты, умное регулирование, цифровая технология, экспериментальный правовой режим, субъекты правового эксперимента

EXPERIMENTAL LEGAL REGIME AND DIGITALIZATION LAW

Abstract. This article discusses the approaches of legal scholars to the subject of the regulatory sandbox – «Regulatory Sandbox» and puts forward the idea and the fact that a comprehensive study of competence, rights and obligations in the field of experimental legal regimes allows us to better understand the essence of the problem of applying experimental legal regimes, its effective implementation in practice, the issues of introducing a regulatory sandbox in Uzbekistan were also raised.

Keywords: experiment, legal experiment, regulatory sandbox, legislative acts, smart regulation, digital technology, experimental legal regime, subjects of legal experiment

Сегодня в стремительно развивающимся мире трудно представить каждый аспект жизни без современных технологий. В частности, многие сферы юриспруденции также интенсивно интегрируются с инновационными технологиями.

Также сегодня приобретает практическое значение связь цифровых технологий с юриспруденцией, с решением различных казусов и экспериментов.

Регулятивная песочница – "Regulatory Sandbox", которая является одной из разновидностей правового эксперимента, начала широко использоваться в пилотных проектах.

В ряде зарубежных стран был проведен ряд правовых экспериментов по созданию механизмов регулятивной песочницы в области цифровых технологий. Первоначально они были успешно реализованы в Великобритании в 2016 г., а затем внедрены в США, Австралии, Сингапуре, ОАЭ, Китае, Малайзии, Таиланде, Индонезии, Бахрейне, Швейцарии и Канаде.

Регулятивная песочница (regulatory sandbox) – это особый экспериментальный правовой режим для инновационных проектов. Регулятивная песочница позволяет нам отказаться от некоторых правовых норм, препятствующих развитию новых инноваций [1].

После тестирования «регулятивной песочницы» в Великобритании был проведен ряд научно-исследовательских работ, и в результате исследования ученые пришли к выводу, что регулятивная песочница является частью метода "smart regulation – умное регулирование".

Этот термин был принят исследователями факультета права, экономики и финансов Люксембургского университета и Университета Нового Южного Уэльса (Австралия), которые совместно с Европейским банковским институтом подготовили исследовательский документ, обобщающий различные подходы к регулированию, действующие в настоящее время.

Сегодня постоянно появляются новые технологии и сервисы, направленные на упрощение производства, коммуникации и повседневной жизни людей. В то же время законодатель, скорее всего, будет постоянно отставать от развития технологий, и поэтому технологические инновации иногда годами живут и развиваются «за пределами» сферы правового регулирования.

Благодаря созданию особых условий через «регулятивную песочницу» компании, занимающиеся производством новых продуктов и услуг, а также представители органов власти могут протестировать их на предмет этих нововведений,

не нарушая действующего законодательства, а затем, если тестирование пройдет успешно, выйти с ними на рынок.

Механизм «регулятивная песочница» для эффективного принятия решения широко распространен в сфере информационных технологий. «Песочница» использовалась для работы с компьютерными вирусами, позволяя использовать приложения в защищенной оболочке, которая известна как «регулятивная песочница» – (regulatory sandbox).

Регуляторные песочницы представляют собой более новые и более конкретные типы экспериментальных правовых режимов, которые предусматривают тесное сотрудничество между государственными и частными субъектами. Регуляторные песочницы создают безопасную испытательную площадку для инноваций, либо позволяя временно применять другой режим регулирования к небольшой группе фирм, либо предлагая рекомендации по соблюдению требований [2].

Многие разработчики антивирусного ПО используют в своих продуктах «регулятивной песочницы» для проактивной защиты пользователей от еще неизвестных угроз. Например, «Лаборатория Касперского» использует в своих продуктах технологию «безопасной среды», позволяющую использовать подозрительные приложения в изолированной среде.

В развитых странах приобрел популярность во многих областях, особенно в индустрии финансовых технологий, режим «регулятивная песочница», который очень быстро распространился и изменил финансовые рынки, внедрил новые технологии и разработал нормативно-правовую базу для реализации передовых проектов.

Этот режим возник в среде финансовых технологий Великобритании, но уже успел распространиться на другие сферы. В Сингапуре, например, они широко используются в энергетическом секторе, в России в виде особого правового режима для внедрения цифровых технологий.

В Узбекистане тоже активно используется специальный правовой режим «регуляторная песочница» для тестирования новых финансовых операций, технологий и услуг в ограниченной среде. С 1 января 2023 г. в Узбекистане вводится специальный правовой режим, известный как регуляторная песочница».

Это предусмотрено Указом Президента Республики Узбекистан от 9 ноября 2022 г. № УП-244 «О мерах по упрощению государственного регулирования предпринимательской деятельности». Данный указ устанавливает пределы государственного регулирования предпринимательской деятельности.

Регулирование допускается в соответствии со специальным правовым режимом:

– несоблюдение определенных правовых норм при производстве, испытании и внедрении новых товаров и услуг с помощью специальных нормативных актов, ограниченных ограниченным периодом, регионом или отдельным лицом;

– осуществление несанкционированной деятельности без разрешительных процедур, включая получение лицензий, государственной тайны и информации, за исключением документов, доступ к которым ограничен в соответствии с Законом о доступе.

Особый правовой режим вводится между компетентными органами и инициатором на основе соглашения, заключаемого отдельно для каждого проекта. В настоящее время.

В договоре определяются требования и условия реализации проекта, в том числе условия выполнения, перечень правовых норм, не распространяющихся на регион, целевую группу и инициатора, а также критерии (показатели) оценки результатов проекта.

Срок действия специального правового режима для каждого проекта составляет до трех лет.

По результатам применения специального правового режима компетентные органы должны в течение одного месяца проанализировать целесообразность внедрения одобренных продуктов и услуг, и подготовить проект поправок к закону, если внедрение продукта или услуги оправдано.

По результатам анализа проектов, в которых была внедрена система регулятивной песочницы, законопроект «Об особомправовом режиме» должен быть подготовлен к 2025 году.

Какая бизнес-структура тестируется в нормативной песочнице? В «регулятивной песочнице» хозяйствующие субъекты могут тестировать новые продукты и услуги, основанные на результатах современных технологий или другой интеллектуальной деятельности. Но эксперименты проводятся в контролируемой ограниченной среде. То есть четко определены продолжительность эксперимента и место, где он проводится. Первоначально «регуляторную песочницу» предполагалось использовать только для медицинской и фармацевтической деятельности, транспорта, включая беспилотные автомобили, электронного обучения и дистанционных образовательных технологий, финансовых рынков, дистанционной торговли, промышленности, строительства, государственных и муниципальных услуг. Однако впоследствии было принято решение не ограничивать области применения «регуляторной песочницы». На наш взгляд, ограничение «регулятивной песочницы» бессмысленно и расточительно.

Основной задачей регулирующих органов является определение формы и дизайна правовых экспериментов, наиболее подходящих для технологических инноваций, особенно тех, которые часто возникают в цифровой экономике. Ключевой особенностью правовых экспериментов в области цифровых инноваций является необходимость действовать как можно быстрее, когда нет уверенности в эффективности предлагаемого новшества. В традиционном контексте у органов власти есть время, необходимое для экспериментов и дискуссий на всех уровнях компетенции, пока технология не достигнет более зрелого уровня. А в случае экспериментального правового режима будут существовать различные риски определенных инноваций для общества и экономики [3].

Казалось бы, в случае технологических инноваций было бы правильно рассчитать, что механизм «регулятивная песочница» является наиболее оптимальным инструментом правового эксперимента.

Несмотря на то, что использование “регулятивных песочниц” имеет много положительных сторон, можно отметить и ряд проблем, связанных с их внедрением. Эти проблемы, на наш взгляд, заключаются в следующем:

Во-первых, не существует единого регламента по внедрению «регулятивной песочницы». Это означает, что даже в пределах одного государства в разных штатах применяются разные методы реализации. Вторая проблема – отсутствие

критериев оценки эффективности реализации экспериментальных правовых режимов.

В-третьих правовые аспекты внедрения «регулятивной песочницы» не охвачены национальным законодательством.

Основной предпосылкой для введения специальных норм по «песочницам» является то, что технологии развития часто оказываются быстрее, чем предполагают общие нормы. В связи с этим государства постоянно ищут способы быть более гибкими и способствовать устойчивому и эффективному развитию в различных областях. Как справедливо отмечает Клаус Шваб, основатель и бессменный президент Всемирного экономического форума, «необходима новая нормативная база, без которой инновационные технологии не могут применяться с уверенностью». Старое законодательство недостаточно адаптировано к описанным проблемам [5].

В таких обстоятельствах, а также в связи с тем, что невозможно установить адекватные регулирование большинства инноваций без практического опыта, государства ищут способы апробировать новые подходы без кардинальных изменений в законодательстве [5].

Песочницы по определению являются казуистическими нормативными пространствами. Они направлены на адаптацию существующих правил к конкретным инновационным задачам, допуская временные отступления, дополнительные рекомендации или регуляторные удобства. Тем не менее существующие «песочницы» также определяются множеством общих элементов, потому что «песочница» не означает безграничного «нарушения правил». К этим элементам относятся:

– установление строгих правил участия в конкурсе, включая обязательство кандидатов продемонстрировать готовность к испытаниям. Кандидаты не должны находиться на ранней стадии инновационного процесса;

– обоснование использования «песочниц». В настоящее время «песочницы» не являются стандартным вариантом регулирования продуктов и услуг. Поэтому при создании «песочницы» необходимо четко понимать, что без проведения таких экспериментов конкретный продукт или услуга не сможет выйти на рынок в течение разумного периода времени в безопасных условиях;

– приносить пользу потребителям и ограничивать потребительский риск;

– что «песочницы» могут стимулировать подлинные инновации, поскольку они не допускают применения приложений, которые не являются достаточно новыми или аналогичными существующим продуктам и услугам;

– короткая, но заранее установленная продолжительность существования «песочницы” (от трех до шести месяцев для каждой группы);

– участие в группе (когорте) “Песочница” является небольшим и элитным;

– ориентация на стимулирование инноваций и предпринимательства путем дерегулирования [4].

Приведенные выводы позволяют выделить основные формы правового экспериментирования, используемые при разработке цифровых инноваций. В качестве средства оптимизации нормативно-правовой среды, ориентированной на конкретную технологию, механизм регулятивной песочницы представляется наиболее удобным экспериментально-правовым механизмом для цифровых

инноваций, возникающих в экономике, которая быстро меняется в краткосрочных циклах [5–9].

С точки зрения цифрового развития, передовые страны активно используют этот механизм и подводят первоначальные итоги регулятивных экспериментов. По нашему мнению, «регулятивная песочница» является частью «умного регулирования» и может рассматриваться как средство применения метода правового эксперимента, как отдельный механизм его реализации. Цель рассмотрения концепции «регулятивная песочница» в статье состоит в том, чтобы подчеркнуть ее взаимосвязь с правовым экспериментом и его влияние на правовое регулирование.

Список литературы

1. Регуляторный эксперимент позволит адаптировать законодательство под «цифру». URL: https://www.eg-online.ru/article/392177

2. Lim B., Low, C. Regulatory Sandboxes. In: J. Madir (Ed.), FinTech: Law and Regulation, 2019. Pp. 302–325.

3. Рабочая группа БРИКС по исследованию вопросов конкуренции в условиях цифровой экономики. URL: https://brics-icc-2019.org/en/digital-markets

4. Sofia Ranchordás. Experimental Lawmaking in the EU: Regulatory Sandboxes [first published in EU Law Live, Weekend edition, October 22–23, 2021.

5. Завьялова Е., Крыканов Д., Патрунина К. Механизм регуляторных «песочниц» для внедрения цифровых инноваций: опыт внедрения экспериментальных правовых режимов на национальном и наднациональном уровне // Право и управление. XXI век. 2019. Т. 15, № 4. С. 130–138.

6. Кванина В. В., Громова Е. А., Спиридонова А. В. К вопросу о системе принципов предпринимательского права // Бизнес, менеджмент и право. 2018. № 4. С. 18–21. EDN: XWHGMX.

7. Громова Е. А. К вопросу об экспериментальных правовых режимах создания цифровых инноваций (регуляторных песочницах) / Е. А. Громова // Вестник Южно-Уральского государственного университета. Серия: Право. 2019. Т. 19, № 3. С. 36–40. EDN: NOHPQM.

8. Громова Е. А. О роли специальных и экспериментальных режимов в развитии конкурентоспособных цифровых технологий // Юрист. 2021. № 11. С. 34–38. EDN: KIFFFB.

9. Громова Е. А. Российская модель регуляторных песочниц в сфере цифровых инновациа // Право цифровой среды: монография / под ред. Т. П. Подшивалова, Е. В. Титовой, Е. А. Громовой. – Москва: Общество с ограниченной ответственностью «Проспект», 2022. С. 258–267. EDN: ZOMCIK.

А. И. Химченко,
кандидат юридических наук,
Московский государственный юридический университет
имени О. Е. Кутафина

ВЕКТОРЫ РАЗВИТИЯ ЦИФРОВОГО ЗАКОНОДАТЕЛЬСТВА: ФОРМИРОВАНИЕ ДОВЕРИЯ

Аннотация. В условиях развития цифровой среды происходит трансформация привычных форм и механизмов реализации правоотношений, формирование новых инструментов взаимодействий. Целью исследования стал поиск концептуального подхода и формирование предложений по стимулированию цифровой среды доверия в современных условиях. Предпринята попытка систематизировать подходы к формированию среды доверия в условиях развития цифровой среды, выявить направления и векторы развития. По результатам исследования выделяются системные элементы цифровой среды доверия и формируются предложения по совершенствованию отраслевого законодательства.

Ключевые слова: идентификация, достоверность, цифровая среда, доверие, оборот данных, взаимодействие

DIRECTIONS OF DIGITAL LEGISLATION DEVELOPMENT: BUILDING OF TRUST

Abstract. In the context of the development of the digital environment, there is a transformation of the usual forms and mechanisms for the implementation of legal relations, the formation of new tools for interaction. The purpose of this study was to search for a conceptual approach and form proposals to stimulate the digital environment of trust in modern conditions. An attempt is made to systematize approaches to the formation of an environment of trust in the conditions of the development of the digital environment, to identify directions and vectors of development. According to the results of the study, the system elements of the digital environment of trust are identified and proposals are formed to improve the industry legislation.

Keywords: identification, reliability, digital environment, trust, data turnover, interaction

Введение. По мере развития и проникновения цифровой среды, распространения на все более широкий спектр общественных отношений все актуальнее становятся вопросы ее доверенного функционирования становятся все более актуальными.

Составляя основу функционирования любого взаимодействия, доверие играет фундаментальную роль в функционировании и цифровой среды. Дисбаланс доверия является критичным состоянием, поскольку его недостаток вызывает рост издержек и снижение эффективности, а избыток может быть преобразован в инструмент совершения неправомерных действий и обращен против самого субъекта правоотношений.

Поиск качественных правовых решений при этом осложняется как опережающей динамикой развития технологий, так и общей тенденцией снижения доверия к праву [1. С. 140].

Сама структура цифровой материи и специфика ее функционирования не позволяют найти долгосрочных статических решений, и требуют постоянного совершенствования цифрового законодательства, формирования и развития цифровой среды доверия.

Вектор 1 (вопросы идентификации). Достоверное подтверждение личности является одним из системных элементов цифровой среды доверия.

Широкий спектр современных технологических и экономических процессов подразумевает активное применение дистанционных технологий электронного взаимодействия, функционирование которых невозможно без санкционированного доступа участников.

При этом роль, отводимая вопросам идентификации в современной информационной архитектуре, отмеченная в Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы, относящей доверенные технологии электронной идентификации и аутентификации к ключевым направлениям технологического развития позволяет выделить данный вектор в качестве ключевых направлений совершенствования законодательства.

Процессы цифровой трансформации общественных отношений, развитие дистанционных сервисов и услуг предопределяют необходимость поиска решений по развитию инфраструктуры идентификации.

В настоящее время ключевые подходы к идентификации реализованы посредством механизмов Единой системы идентификации и аутентификации (ЕСИА) и Единой биометрической системы (ЕБС) [2. С. 104].

Вместе с тем Банк России в «Основных направлениях развития финансового рынка Российской Федерации на 2023 год и период 2024 и 2025 годов» отмечает увеличивающийся спрос новые упрощенные решения по идентификации и актуальность формирования среды доверия [3. С. 47].

Примером реализации новых решений выступает платформа «Госключ», реализующая возможность подписания зарегистрированными в ЕСИА заявителями документов в электронной форме (возможность подписания которых предусмотрена действующим законодательством).

К перспективным проектам в сфере идентификации и снижения рисков цифровой среды Банком России также отнесены:

– технологии видеопотока;

– технология на основе цифровых отпечатков (введена и рекомендована к использованию в стандарте Банка России СТО БР БФБО-1.7-2023 [4. С. 7];

– платформа «Знай своего клиента», использующая информацию об уровне комплаенс-риска клиентов и контрагентов;

– система проверки сведений об абоненте, в целях снижения рисков совершения мошеннических действий посредством мобильного телефона.

Реализация и развитие новых решений в сфере идентификации затрагивает многие общественные процессы, инициирует возникновение новых

правоотношений, в связи с чем требует глубокой детальной правовой проработки. Отмечается необходимость гармонизации системы определений, установления единого состава объектов и субъектов в сфере идентификации и определения ее правовых принципов как условие разработки специального законодательства в сфере удаленной идентификации [5. С. 75].

При этом к ключевым направлениям развития законодательства в сфере идентификации стоит отнести решение таких вопросов как применение дифференцированного подхода в зависимости от особенностей правоотношений, альтернативность инструментов и конфиденциальность их применения, выработка инструментов мониторинга выполнения требований информационной безопасности идентификации клиентов [6. С. 163].

Вектор 2 (обеспечение достоверности). В числе системных элементов обеспечения цифровой среды доверия находится комплекс вопросов, связанных с обеспечением достоверности и неизменности электронных документов.

Комплекс вопросов по продвижению проектов по внедрению электронного документооборота в организациях, созданию условий для повышения доверия к электронным документам, осуществлению в электронной форме идентификации и аутентификации участников правоотношений отнесен Стратегией развития информационного общества в Российской Федерации к основным задачам применения информационных технологий, что подчеркивает значимость указанной тематики и в разрезе цифровой среды доверия.

В то же время, несмотря на активное применение технологических решений в сфере электронного документооборота в настоящее время отсутствует комплексная правовая основа для осуществления юридически значимого электронного документооборота, унификация подходов к созданию, обороту, хранению и использованию электронных документов.

Вместе с тем в отраслевых концептуальных документах, отмечается взаимосвязь доверия участников процесса с развитием технологий электронного документооборота.

В частности, в Концепции развития электронного документооборота в хозяйственной деятельности (утв. решением президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 25.12.2020 № 34), отмечается недостаточный уровень доверия участников хозяйственной деятельности к соблюдению режима конфиденциальности электронных документов.

Достоверность документов, осуществляемая при их обмене в электронной форме, достигается посредством механизма электронной подписи (ЭП), реализованного нормами Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и используемого для определения подписывающего информацию лица при совершении юридически значимых действий.

Фактором доверия при применении электронной подписи является признание равнозначности документов на бумажном и электронном носителях, а обеспечение доверия реализуется посредством доверенной третьей стороны (юридического лица, осуществляющего проверку электронной подписи).

Стоит отметить процесс совершенствования законодательства об ЭП, в том числе развитием норм, способствующих повышению доверия. Так, нормами Федерального закона от 04.08.2023 № 457-ФЗ были внесены изменения в закон об электронной подписи, предусматривающие незамедлительное уничтожение ключей ЭП по истечении сроков их действия, а также усиление требований к аккредитованным удостоверяющим центрам.

Отдельным немаловажным вопросом достоверности является распространение технологии генерации контента (дипфейков).

К факторам стимулирования доверия в условиях распространения дипфейков можно отнести реализуемые нормами Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» механизмы ограничения доступа к запрещенной информации, ограничения, устанавливаемые авторским и правом интеллектуальной собственности, нормы, регулирующие защиту чести, достоинства и деловой репутации, запрет на использование персональных данных человека без его согласия.

Кроме того, противодействие дипфейкам осуществляется и посредством технологических инициатив.

Так, специалистами Национального центра когнитивных разработок (НЦКР) ИТМО ведется разработка для Главного радиочастотного центра (ГРЧЦ) сервиса, который позволит проверять видеозаписи выступлений на предмет лжи и манипуляций, а Сбербанк оформил патенты на технологии по выявлению дипфейков, для защиты от кибератак и борьбы с фейковыми новостями.

Вместе с тем в действующем законодательстве отсутствуют как понятие дипфейка, так и нормы, направленные на выявление и противодействие и их нейтрализацию.

Вектор 3 (обеспечение безопасности). Проблематика безопасности цифровой среды, учитывая высокую степень проникновения в общественные и деловые процессы, имеет значительный потенциал влияния на доверие к ней.

Вопросы безопасности цифровой среды находят отражение в ключевых программных и документах стратегического планирования и имеют важное значение в механике ее функционирования.

В частности, в Основах государственной политики Российской Федерации в области международной информационной безопасности (утверждены Указом Президента РФ от 12 апреля 2021 г. № 213) среди направлений государственной политики выделяются меры укрепления доверия в области использования информационно-коммуникационных технологий, а Стратегией развития информационного общества в Российской Федерации фиксируется необходимость выработки системы доверия в сети «Интернет».

В целях обеспечения безопасности цифровой среды нормы Федерального закона от 27.07.2006 № 149-ФЗ образуют комплекс регламентирующих распространение информации мер, направленных на повышение достоверности сведений.

На состояние безопасности цифровой среды влияет широкий ряд факторов, в том числе и необходимость совершенствования организационно-правовых аспектов деятельности в рассматриваемой сфере, среди которых нерешенность многих информационно-правовых вопросов в национальной системе права [7. С. 39].

Стратегическим вектором развития безопасности цифровой среды является разработка отдельного федерального закона, регламентирующего обеспечение информационной безопасности, поскольку в настоящее время специализированные нормы разбросаны по большому количеству отдельных нормативных правовых актов [8. С. 115]. В то же время отсутствие регулирования отрасли кибербезопасности требует развития соответствующих правовых средств их функционирования.

Вектор 4 (взаимодействие и функционирование цифровой среды). В процессе развития цифровой среды неизбежно происходит трансформация субъектов взаимодействия, их роли и функционале в технологическом цикле.

Среди новелл информационного законодательства необходимо отметить расширение состава субъектов информационного взаимодействия введением с 01.03.2023 года (реализованное нормами Федерального закона от 29.12.2022 № 584-ФЗ) и появление такого участника цифровой среды как «владелец сервиса размещения объявлений», правовой режим функционирования которого позволяет выделить факторы стимулирования доверия.

Так, статьей 10.7 Федерального закона от 27.07.2006 № 149-ФЗ определено понятие сервиса размещения объявлений и установлены обязанности, в числе которых:

– не допускать использование сервиса в целях совершения уголовно наказуемых деяний и распространение запрещенной информации;

– соблюдать права и законные интересы граждан и организаций;

– обеспечить интеграцию и взаимодействие сервиса размещения объявлений с ЕСИА и ФГИС ЕПГУ в установленных случаях и др.

Отдельное влияние на доверие в цифровой среде имеет применение рекомендательных алгоритмов. Прежде всего, следует отметить внимание законодателя к указанному вопросу и введение в законодательство нормами Федерального закона от 31.07.2023 № 408-ФЗ требований к владельцам рекомендательных алгоритмов закрепляющих необходимость информирования пользователей о применении рекомендательных технологий на информационных ресурсах и размещении в открытом доступе правил применения рекомендательных технологий и контактных данных их владельцев, а также порядок взаимодействия владельца информационного ресурса с Роскомнадзором в случае выявления нарушений.

При этом из указанных норм прямо не следует, какие возможны нарушения прав и законных интересов граждан и организаций, что позволяет отнести к направлениям совершенствования вопрос о необходимости детализация перечня нарушений, а также соответствующих им специальных мер ответственности.

Вектор 5 (оборот данных). Персональные данные образуют ключевой структурный элемент цифровой среды, имеющий высокоемкий потенциал практического применения.

Любой субъект персональных данных изначально заинтересован в их сохранности, в связи с чем, развитие механизмов безопасного доверенного оборота и обработки данных является ключевым вектором развития профильного законодательства в контексте формирования цифровой среды доверия.

Несмотря на существующие механизмы защиты персональных данных, в действующем законодательстве о персональных данных не реализована возможность по управлению субъектом своими персональными данными, отсутствуют механизмы контроля субъектом взаимодействия над данными в процессе всего технологического цикла, отсутствуют понятные и простые механизмы реализации прав субъектов персональных данных, не связанных с судебным порядком.

Также к настоящему времени не нашел своей реализации механизм легального оборота персональных данных в коммерческих целях.

Разработка правовых решений указанных вопросов представляется одним из перспективных векторов развития профильного законодательства и стимулирования доверия к цифровой среде.

Вектор 6 (отдельные инструменты цифровой среды). Цифровая трансформация подразумевает появление новых инструментов и объектов правоотношений, механики их функционирования. Происходит появление новых финансовых элементов и их активное применение в цифровой среде, с характерной тенденцией дальнейшей интенсификации [9. С. 1].

В качестве примера таких объектов стоит отметить цифровые финансовые активы, отношения, возникающие в части которых регулируются нормами Федерального закона от 31.07.2020 № 259-ФЗ.

Элемент доверия реализован в особенностях правового режима, согласно которому цифровые финансовые активы и цифровая валюта подлежат учету, осуществляемому операторами информационной системы и операторами обмена, для которых установлен перечень обязанностей.

В целом вопросы цифровых активов, осложненные в том числе и тем, что особенности организации выпуска и обращения цифровой валюты в действующем законодательстве не находят своего отражения, их использование на территории Российской Федерации в качестве средства платежа законодательно запрещено. При этом ввиду особой чувствительности финансовой сферы в целом и характерным ей рискам как для пользователя, так и для финансовых институтов, требуют внимания и соответствующих решений вопросы минимизации возможностей совершения противоправных действий.

Вектор 7 (защита интересов в цифровой среде). Важным фактором доверия является наличие и функционирование инструментов защиты прав и интересов субъектов взаимодействия в цифровой среде.

В соответствии с положениями Федерального закона от 27.07.2006 № 149-ФЗ субъектам правоотношений доступны следующие инструменты защиты интересов в цифровой среде:

– прекращение выдачи сведений в сети «Интернет»;

– ограничение доступа к недостоверной информации;

– ограничение доступа к информации, обрабатываемой с нарушением законодательства в области персональных данных;

– ограничение доступа к информации, распространяемой с нарушением авторских и (или) смежных прав.

В рамках стимулирующих доверие мер представляется целесообразным расширить инструментарий, предусматривающий одностороннее блокирование субъектом потенциально уязвимых правоотношений со своим участием.

В числе примеров, направленных на стимулирование доверия к цифровой среде стоит отметить проект федерального закона № 197920-8, разработанный в целях совершенствования механизма противодействия хищению денежных средств со счетов клиентов кредитных организаций и механизма их возврата.

Продуктивным направлением является также совершенствование финансовых инструментов, направленных на минимизацию возможности их использования в неправомерных целях и преобразование в цивилизованный финансовый инструмент.

Так, на снижение противоправной деятельности в цифровой среде направлен проект федерального закона № 322818-8, посредством которого предлагается обязать кредитные и микрофинансовые организации уведомлять заемщиков о заключении договоров займа и микрозайма путем направления уведомления через портал «Госуслуги».

Проект Федерального закона № 341256-8, направленный на предупреждение неправомерного получения потребительских займов (кредитов) третьими лицами предусматривает право гражданина установить в своей кредитной истории запрет на заключение с ним договоров потребительского займа и снять такой запрет.

Заключение. Формирование цифрового доверия в современных условиях находится на пересечении различных подходов и методик, отраслевых сфер и направлений. Вместе с тем подразумевает широкий спектр мер по развитию инструментов идентификации и подтверждению личности, обеспечению сохранности, целостности и достоверности данных, реализации механизмов комплексной безопасности и защиты интересов в процессе взаимодействия.

Проведенный анализ показывает, что в настоящее время в действующем законодательстве реализован набор мер, реализация которых способствует стимулированию доверия к цифровой среде.

Вместе с тем динамика развития цифровой среды, усложнение механики взаимодействия и возникающие новые риски предопределяют необходимость поиска новых решений и совершенствования существующих подходов.

Список литературы

1. Полякова Т. А., Наумов В. Б., Минбалеев А. В. Доверие к закону в условиях цифровой трансформации // Государство и право. 2022. № 11. С. 139–147.

2. Химченко А. И. Формирование цифровой среды доверия: динамика развития инфраструктуры идентификации при реализации цифровых услуг // Вестник МГЮА. 2023. № 2. С. 101–110.

3. Основные направления развития финансового рынка Российской Федерации на 2023 год и период 2024 и 2025 годов // Вестник Банка России. 2022. № 63.

4. Стандарт Банка России СТО БР БФБО-1.7-2023. URL: https://cbr.ru/Crosscut/LawActs/File/6177

5. Наумов В. Б. Задача обеспечения тайны идентификации в информационном праве // Мониторинг правоприменения. 2019. № 3(32). С. 70–75.

6. Химченко А. И. Вопросы формирования цифровой среды доверия как структурного элемента в цифровизации государственного управления // Правовое государство: теория и практика. 2022. № 3. С. 159–164.

7. Четвертые Бачиловские чтения: материалы Международной научно-практической конференции / отв. ред. Т. А. Полякова, А. В. Минбалеев, В. Б. Наумов // Институт государства и права РАН. М.; Саратов: Амирит, 2022. 568 с.

8. Полякова Т. А., Камалова Г. Г. Новые векторы развития системы правового обеспечения информационной безопасности как одного из приоритетов безопасности (к 30-летию принятия Закона Российской Федерации «О безопасности») // Правовое государство: теория и практика. 2022. № 2(68). С. 112–122.

9. Концепция цифрового рубля. URL: http://cbr.ru/Content/Document/File/120075/concept_08042021.pdf

10. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

11. Дорожная карта по развитию финансирования субъектов МСП (утв. приказом Банка России от 13.09.2018 № ОД-2387).

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

13. Федеральный закон от 04.08.2023 № 457-ФЗ // Собрание законодательства РФ. 2023. № 32 (часть I). Ст. 6189.

14. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (часть I). Ст. 3448.

15. https://www.kommersant.ru/doc/5646201

16. https://rospatent.gov.ru/ru/news/sber-dipfeyk-17082022

17. Основы государственной политики Российской Федерации в области международной информационной безопасности // Собраний законодательства РФ. 2021. № 16 (часть I). Ст. 2746.

18. Федеральный закон от 29.12.2022 № 584-ФЗ // Собрание законодательства РФ. 2023. № 1 (часть I). Ст. 31.

19. Федеральный закон от 31.07.2023 № 408-ФЗ // Собрание законодательства РФ. 2023. № 32 (часть I). Ст. 6140.

20. Федеральный закон от 31.07.2020 № 259-ФЗ // Собрание законодательства РФ. 2020. № 31 (часть I). Ст. 5018.

21. Проект федерального закона № 197920-8. URL: https://sozd.duma.gov.ru

22. Проект федерального закона № 322818-8. URL: https://sozd.duma.gov.ru

23. Проект Федерального закона № 341256-8. URL: https://sozd.duma.gov.ru

Е. В. Холодная,
кандидат юридических наук, доцент,
Московский государственный юридический университет
имени О. Е. Кутафина

О ДИВЕРГЕНЦИИ ПРАВОВЫХ КАТЕГОРИЙ «ИНФОРМАЦИЯ» И «ЦИФРОВЫЕ ДАННЫЕ»

Аннотация. Под воздействием цифровизации возникает изменение правового понятийного аппарата, зачастую термины берутся из точных наук без уточнения их содержания, что ведет к их неопределенности. В ходе преобразований в конституционные положения, под особым вниманием оказалась категория «цифровые данные», как квази-синоним термина информации. Оцифровка данных представляет собой их перевод в цифровой универсальный формат с помощью вида информационных технологий, именуемых, соответственно, цифровые. Цифровые технологии имеют дело с машиночитаемыми (цифровыми) данными, которые в момент их интерпретации человеком преобразовываются в информацию. Под цифровыми данными понимается совокупность сведений, зафиксированных на носителе в форме, пригодной для автоматизированного хранения, передачи и обработки с помощью цифровых технологий. Кроме цифровых данных по форме представления выделяются аналоговые данные и квантовые данные. Данная классификация имеет значение при определении вида информационных технологий для поиска, сбора и обработки указанных видов данных.

Ключевые слова: информация, цифровые данные, аналоговые данные, квантовые данные, цифровые технологии, информационные технологии, оборот цифровых данных, цифровизация

ON THE DIVERGENCE OF THE LEGAL CATEGORIES “INFORMATION” AND “DIGITAL DATA”

Abstract. Under the influence of digitalization, there is a change in the legal conceptual apparatus, often terms are taken from the exact sciences without specifying their content, which leads to their uncertainty. During the amendments to the constitutional provisions, the category of “digital data”, as a quasi-synonym of the term information, came under special attention. Digitization of data is their translation into a digital universal format using a type of information technology, respectively referred to as digital. Digital technologies deal with machine-readable (digital) data, which, at the moment of their interpretation by a person, are transformed into information. The author believes that digital data is a collection of information recorded on a medium in a form suitable for automated storage, transmission and processing using digital technologies. In addition to digital data, according to the form of presentation, the author distinguishes analog data and quantum data. This classification is important in determining the type of information technology for the search, collection and processing of these types of data.

Keywords: information, digital data, analog data, quantum data, digital technologies, information technologies, digital data turnover, digitalization

Введение. Цифровизация влечет за собой фундаментальные преобразования всех сфер социальной жизни, бизнеса и публичного управления и имеет основное предназначение – оптимизация оборота цифровых данных. Указанные изменения учтены в виде поправок в конституционные положения, что привело к возникновению ряда вопросов, в том числе, о природе цифровых данных и определения особенностей их включения в оборот и др. Поэтому особое внимание должно быть сконцентрировано на термине данные (англ. «data»), как квази-синониме информации, для разграничения категорий информация, данные, цифровые данные из состояния правового тождества, существующего на сегодняшний момент. Полученные результаты могут быть применены для дальнейшего совершенствования действующего законодательства и правоприменительной деятельности.

Основная часть. Специалисты отмечают не только семантические различия терминов (данные представлены в виде различных символов; информация основана на идеях и выводах; сами по себе данные не имеют значения, но организация и анализ данных уже есть информация [9. С. 63-73], информация социально значима и т. д.), но и онтологические различия («data» инвариантны относительно воспринимающего субъекта, так как они возникают только при достижении объективной конвенции о своей структуре; информация же является основанием субъективного мира и специфичным коррелятом данных, существующих объективно как конструкт из материального фундамента) [4. С. 72].

Вообще понятие «информация» в центре научных изысканий с незапамятных времен, однако новый пик развития теории информации связан с технологическим прогрессом. Первые шаги в современной теории информации были сделаны математиками еще в первой половине XX в.: в 1928 г. Ральф Хартли ввел понятие «информации» (энтропии) и первым попытался определить количество или меру информации [14. С. 535–563]. В 1948 г. в учении «Математическая теория связи» Клод Шеннон предложил статистическое определение информации [15. С. 379]. Если говорить обобщенно, то в математике информацией оказываются только те передаваемые сообщения, которые уменьшают неопределенность (энтропию) у получателя информации. При этом информация неразрывно связана с процессом ее передачи (трансмиссии) на основе символов и знаков и определяется этим процессом [2. С. 2–3].

Иными словами, прослеживается неразрывная связь и взаимная обусловленность информации и информационных технологий, обеспечивающих ее оборот. Основоположник кибернетики Норберт Винер определил, что информация – это и не энергия, и не материя, а обозначение содержания, полученного в результате взаимодействия с внешним миром. Также, как и в большинстве философских учениях, первоочередным для кибернетики является момент активного обмена со средой, в результате чего достигается приращение знания [1. С. 123–127]. При этом взаимодействие с внешним миром обеспечивают информационные технологии.

Широкое законодательное толкование термина «информация» позволяет реформировать нормативные акты без изменения основоположений (ст. 2 Закона об информации). В контексте закона универсальный термин «информация» обозначает любые сведения о ком-либо или о чем либо, получаемые из любого источника и в любой форме (письменной, устной, визуальной и т. д.).

Однако Закон об информации фактически ставит знак равенства между категориями «данные» и «информация». Смешение терминов исторически основано на статистической теории информации Клода Шеннона [15. С. 379]. Согласно данной теории, информация представлена набором символов, подлежащих распознанию или декодированию. Сутью декодирования является снятие неопределенности (энтропия) посредством выбора, осуществляемого получателем информации [2. С. 2–3]. Однако вышеуказанная позиция (к признакам – обработка и интерпретация) более приемлема для IT, а не для человека, и ближе к значению «данные» [11. С. 22–27].

Работы в теории права показывают, что в настоящий момент инвариантность терминов информация, сообщения, данные подвергается объективной дивергенции в силу воздействия цифровизации и признания новых качеств и признаков, ранее не проявлявшихся [6; 7. С. 98–110]. Так, в Конституции РФ значительное количество норм посвящено информации как объекту правового регулирования и заложены основы публично-правовых режимов информации (закреплены право на информацию; свобода массовой информации; требование об обязательном распространении ее отдельных видов, например, об экологической обстановке и нормативной информации; введен базис под личную, семейную, государственную тайну и др..). Однако в связи с переходом к цифровой экономике высокая экономическая ценность определена и в отношении цифровых данных и их оборота [8. С. 4–10]. В 2000 году в Конституцию Российской Федерации были внесены поправки, в том числе, в п. «м» ст. 71 добавлено положение, что в ведении Российской Федерации находятся «обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных».

В связи с этим понятие «цифровые данные» и условия их включения в оборот нуждаются в уточнении на уровне федерального закона. Также следует отметить публично-правовую направленность конституционных нововведений как в отношении применения ИТ, так и в отношении оборота цифровых данных, так как положения заявлены с позиции обеспечения и поддержания безопасности. Конституционными положениями задан новый вектор развития публично-правового законодательства, в которое должны быть гармонично встроены новые объекты правового регулирования.

Подсчитано, что 90 % всех данных в мире было создано за последние несколько лет с помощью современных информационных технологий [5]. Большая часть сегодняшней экономики опирается на информацию (данные), и эта зависимость в будущем будет только возрастать [10. С. 483–489]. Соответственно будет возрастать и потребность в создании и совершенствовании новых ИТ, обеспечивающих оборот таких данных.

Данные – это поддающееся многократной интерпретации представление информации в формализованном виде, пригодном для передачи, связи, или обработки [16]. Оцифровка данных представляет собой их унификацию в числовое значение, выражение данных в цифрах (перевод в цифровой универсальный формат; создание цифровых данных и т. п.) с помощью вида информационных технологий, именуемых, соответственно, цифровые [12. С. 8–10]. Цифровые технологии имеют дело с машиночитаемыми (цифровыми) данными, которые в момент их интерпретации человеком преобразовываются в информацию. Иными словами, цифровые данные – это совокупность сведений, зафиксированных на носителе в форме, пригодной для автоматизированного хранения, передачи и обработки с помощью цифровых технологий.

Специфика цифровых данных состоит в том, что они существуют независимо в цифровой среде, но при этом их социальная значимость появляется при условии целенаправленного сбора. Преобразование и обработка цифровых данных по запросу позволяют получить информацию, т. е. информация – это вывод или итог результата преобразования и анализа данных на основе информационных технологий [3. С. 3–7].

Кроме цифровых данных по форме представления можно выделить аналоговые данные и квантовую информацию. Данная классификация имеет значение при определении вида информационных технологий для поиска, сбора и обработки указанных видов данных.

Аналоговые данные представлены в виде непрерывного потока электрических ритмов разной амплитуды с неограниченным числом значений. С помощью аналоговых технологий информация хранится и передается под каждый тип носителя в разных форматах (например, «виниловые» диски, фотопленка и др..).

Квантовая информация или, точнее, квантовые данные – это данные о состоянии квантовой системы, представленные в кубитах. В настоящее время самые активные исследования направлены на развитие сферы квантовых технологий и квантовых данных из-за вероятных угроз нарушения современных вычислений, связи и криптографии, предотвращение которых имеет стратегическое значение для обеспечения безопасности государства [13. С. 38–45].

Итак, только в момент интерпретации данных человеком происходит их преобразование в информацию. На наш взгляд, это уточнение имеет прагматическое значение при создании правовых терминологических конструкций. Сам оборот данных в целом носит публично-правовое обеспечение, а вот уже результат анализа и выборки данных – информация может являться объектом как публично-правовых, так и частно-правовых отношений.

Заключение. Цифровые данные рассматриваются как ключевой актив цифровой экономики и их значимость в данный момент подкреплена конституционными положениями, внедрившими на самом высоком правовом уровне новую для права категорию. Включение цифровых данных в Конституцию Российской Федерации означает требование об их скорейшем встраивании в законодательство с учетом уже существующих категорий и определения места в системе законодательства.

Из сказанного следует, что наступил период, требующий правовых уточнений в отношении терминов «информация» и «цифровые данные», уже введенных в правовое поле как различных категорий, но имеющих значение синонимов с позиции Закона об информации. Для разрешения указанного противоречия требуется на законодательном уровне ввести определение цифровых данных.

Список литературы

1. Винер Н. Кибернетика и общество. М.: Изд-во иностр. лит., 1958. С. 123–-127.
2. Войниканис Е., Якушев М. Информация. Собственность. Интернет: традиции и новеллы в современном праве. М.: Волтерс Клувер, 2004. С. 2–3.
3. Тисов В. В. Онтологические различия информации и данных // Философские проблемы информационных технологий и киберпространства. 2016. № 2. С. 63–73.
4. Калягина Л. В., Разумов П. Е. Категория «данные»: понятие, сущность, подходы к анализу // Вестник КрасГАУ. 2014. № 4. С. 3–7.
5. Ожегов С. И. Словарь русского языка: Ок. 53 000 слов / С. И. Ожегов; под общ. ред. проф. Л. И. Скворцова. 24-е изд., исправ.. М., ООО «Издательство Оникс»: ООО «Издательство «Мир и Образование», 2007. С. 72.
6. Постолатий В. BigData шагает по планете. URL: https://rg.ru/2013/05/14/infa-site.html
7. Терещенко Л. К. Правовой режим информации: специальность 12.00.14 «Административное право; административный процесс»: автореферат диссертации на соискание ученой степени доктора юридических наук / Терещенко Людмила Константиновна. Москва, 2011. 54 с;
8. Терещенко Л. К. Трансформация понятийного аппарата информационного права в условиях цифровизации // Журнал российского права. 2022. Т. 26, № 12. С. 98–110.
9. Терещенко Л. К., Якушев М. В. Влияние цифровой экономики на правовые режимы информации // Информационное право. 2021. № 2. С. 4–10.
10. Холодная Е. В. Проблемы и перспективы оборота BIG DATA // В книге: Право цифровой среды. Монография. Под редакцией Т. П. Подшивалова, Е. В. Титовой, Е. А. Громовой. Москва, 2022. С. 483-489.
11. Холодная Е. В. О некоторых элементах технологий цифрового профилирования // Право и цифровая экономика. 2022. № 3(17). С. 22–27.
12. Холодная Е. В. О проблематике термина «цифровые технологии» как правовой дефиниции // Информационное право. 2022. № 2. С. 8–10.
13. Холодная Е. В. Квантовые технологии как объект права // Вестник Университета имени О. Е. Кутафина (МГЮА). 2022. № 4(92). С. 38–45.
14. Hartley R. V. L. Transmission of Information, Bell System Technical Journal, July 1928. Pp. 535–563.
15. Shannon C. E. A Mathematical Theory of Communication // The Bell System Technical Journal. 1948. Vol. 27. P. 379.
16. SO/IEC 2382-1:1993 «Информационные технологии. Словарь. Часть 1. Основные термины» (2382-1:93 «Information technology – Vocabulary – Part 1: Fundamental terms». NEQ)

О. А. Хотько,
кандидат юридических наук, доцент,
Белорусский государственный университет

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЭКСПЛУАТАЦИИ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМ (НА ПРИМЕРЕ ЗАКОНОДАТЕЛЬСТВА РЕСПУБЛИКИ БЕЛАРУСЬ, СОЮЗНОГО ГОСУДАРСТВА И ПРАВА ЕВРАЗИЙСКОГО ЭКОНОМИЧЕСКОГО СОЮЗА)

Аннотация. Целью исследования является анализ нормативных правовых актов Республики Беларусь и интеграционных объединений с ее участием, затрагивающих область общественных отношений, возникающих в связи с созданием и эксплуатацией интеллектуальных транспортных систем. Особенность статьи заключается в определении основных направлений совершенствования правовых норм и законодательных актов в свете необходимости обеспечения национальной и региональной безопасности на территории евразийского пространства и Союзного государства.

Ключевые слова: транспортное законодательство, интеллектуальные транспортные системы, правовое регулирование, гармонизация законодательства, Евразийский экономический союз

PROBLEMS OF LEGAL REGULATION OF OPERATION OF INTELLIGENT TRANSPORT SYSTEMS (BASED ON THE EXAMPLE OF THE LEGISLATION OF THE REPUBLIC OF BELARUS, THE UNION STATE AND THE LAW OF THE EURASIAN ECONOMIC UNION)

Absract. The purpose of the study is to analyze the regulatory legal acts of the Republic of Belarus and integration associations with its participation, affecting the area of public relations arising in connection with the creation and operation of intelligent transport systems. The peculiarity of the article lies in determining the main directions for improving legal norms and legislative acts in the light of the need to ensure national and regional security on the territory of the Eurasian space and the Union State.

Keywords: transport legislation, intelligent transport systems, legal regulation, harmonization of legislation, Eurasian Economic Union

Введение. В условиях развития цифровизации, укрепления технологического суверенитета непрерывно осуществляется расширение новейших технологий в транспортной сфере. Велением времени и признаком правового государства является эффективное правовое регулирование новых правоотношений с целью недопущения правовой неопределенности, явных пробелов в праве. Актуальность регулирования в сфере создания и обеспечения национальной сети интеллектуальных транспортных систем на современном этапе определяется потребностью систематизации правовых норм, комплексного подхода к их закреплению

в законодательстве. Более того, не только национальные акты требуют пристального внимания, но и учет развития правовых норм и их гармонизация в свете укрепления интеграции государств-членов межгосударственных объединений, поскольку согласованные меры требуются в рамках проведения транспортной политики при внедрении интеллектуальных транспортных систем как инструмента реализации целей по повышению безопасности транспортной деятельности, эффективности в процессе управления транспортной системой при расширении дорожно-транспортной сети и появлении новых транспортных коридоров, отслеживании движения грузов в пути и информировании участников дорожного движения и в процессе эксплуатации иных видов транспорта.

В российской транспортно-правовой науке освещены основные подходы, применяемые при разработке и законодательном закреплении интеллектуальных транспортных систем и обозначены существующие в данной области проблемы [1]. Вместе с тем в белорусской юридической науке данные вопросы не являлись предметом специального анализа, в то же время сочетание передовых информационных и коммуникационных технологий именуемых как интеллектуальные транспортные системы получает применение при отсутствии правовых исследований эффективности норм законодательных актов, а именно понимания особенностей правового регулирования и изучения институциональной среды. Впервые в Республике Беларусь авторы учебного пособия показали сложившиеся правовые подходы на начальном этапе развития, в том числе в рамках права межгосударственных образований, в которых наше государство участвует [5. С. 12–13]. В данной работе предпринята попытка провести осмысление транспортного законодательства с целью выработки оптимальных предложений по его совершенствованию и уточнению роли регулирования интеллектуальной транспортной системы на современном этапе социального-экономического развития Республики Беларусь и Союзного государства России и Беларуси.

Основная часть. В Концепции обеспечения безопасности дорожного движения, утвержденной постановлением Совета Министров Республики Беларусь от 23 мая 2023 г. № 329, отмечается, что государственная политика в области безопасности дорожного движения основывается на осуществлении мер, принимаемых в том числе в отношении интеллектуальных транспортных систем, включая формирование требований к новым транспортным средствам разных категорий, а также разработку состава и иерархии интеллектуальных транспортных систем с учетом цифровизации систем управления дорожным движением, внедрения современных информационно-коммуникационных технологий обеспечения безопасности дорожного движения и автоматизации его управления (п. 14.6).

Относительно разработки новейшего законодательства стоит обратить внимание на постановление Совета Министров Республики Беларусь от 25 октября 2023 г. № 724 «О порядке функционирования интеллектуальных транспортных систем», которым утверждено положение, касающееся применения таких систем на автомобильных дорогах общего пользования, содержащее цели и задачи, порядок создания интеллектуальных транспортных систем, что направлено на повышение эффективности дорожного движения, качество транспортной деятельности.

Создание правовых основ развития интеллектуальных транспортных систем имеет особое значение, так как правовые положения способствуют комплексному решению ряда важнейших задач и позволят на системной основе осуществлять управление транспортным средством и дорожным движением, его оптимизацию, информировать специальные службы по соблюдению законодательства и повысить безопасность дорожного движения. Так, с октября 2022 г. в Республике Беларусь установленные камеры видеофиксации считывают номера автомобилей, на основании чего определяются автовладельцы, участвующие в дорожном движении без прохождения технического осмотра, тем самым с помощью искусственного интеллекта ведется контроль за соблюдением норм административного законодательства. Развитие данных интеллектуальных систем может быть связано с появлением экологических датчиков, позволяющим оперативно собирать информацию об уровне загрязнения атмосферного воздуха.

Исходя из сказанного отметим, что отсутствие в белорусском законодательстве понятийного аппарата и иерархии интеллектуальных транспортных систем говорит о неполном правовом подходе в данной области общественных отношений и составляет пробелы в законодательстве. С этой целью предлагается в Законе Республики Беларусь от 5 мая 1998 г. № 140-З «Об основах транспортной деятельности» закрепить в ст. 1 правовую категорию «интеллектуальная транспортная система» и в главе 4 «Обеспечение транспортной деятельности» отразить меры, которые следует принять в отношении эксплуатации интеллектуальных транспортных систем, поскольку консолидирующий транспортную деятельность нормативный правовой акт должен учитывать новейшие технологические разработки. В национальном законодательстве требуется правовое регулирование интеллектуальных транспортных систем в рамках закрепления отдельных положений относительно безопасности транспортной деятельности.

Обратимся к положениям права Евразийского экономического союза (далее – ЕАЭС), непосредственно регулирующим рассматриваемую сферу отношений. Понятие интеллектуальной транспортной системы закреплено в Основных направлениях и этапах реализации скоординированной (согласованной) транспортной политики государств-членов Евразийского экономического союза на 2021–2023 годы», утвержденном решением Евразийского экономического совета от 26 декабря 2016 г. № 19, под которой понимается «интеграция современных информационных и коммуникационных технологий и средств автоматизации с транспортной инфраструктурой, транспортными средствами и пользователями, ориентированная на повышение безопасности и эффективности транспортного процесса». В рамках права ЕАЭС также следует назвать такой акт, как распоряжение Межправительственного совета от 20 августа 2021 г. № 15 «О плане мероприятий («дорожной карте») по реализации Основных направлений и этапов реализации скоординированной (согласованной) транспортной политики государств-членов Евразийского экономического союза на 2021–2023 годы», в котором обозначена подготовка предложений по формированию правовых основ для функционирования национальной сети интеллектуальных транспортных систем государств-членов и в том числе разработка проекта концепции по

совершенствованию взаимодействия данных систем в Союзе с учетом национальных подходов. Стоит заметить, что направленные на реализацию скоординированной (согласованной) транспортной политики участвующих в ЕАЭС государств мероприятия касаются сферы автомобильного транспорта. Однако как раз о новых используемых видах следует говорить в свете того, что их эксплуатация осуществляется быстрее, чем определяется правовое регулирование в данной сфере. Кроме того, государствами-членами ЕАЭС разработаны Рекомендации Коллегии Евразийской экономической комиссии от 22 декабря 2020 г. № 27 «О согласованных подходах к взаимодействию национальных интеллектуальных транспортных систем, в том числе в целях совершенствования транспортного (автомобильного) контроля». Выработка таких подходов предусматривает: повышение безопасности транспортной системы, доступности услуг транспортного комплекса, эффективности управления транспортными процессами, снижение вредного воздействия на окружающую среду. Особое значение принадлежит, с позиции автора, таким задачам, как формирование правовых основ создания, развития и обеспечения национальной сети интеллектуальных транспортных систем, а также целесообразность установления обязательных требований к интеллектуальным транспортным системам и ее компонентам, необходимость принятия мер по развитию и совершенствованию информационного взаимодействия в сфере транспортного (автомобильного) контроля с целью его повышения. Вышеназванные Рекомендации предусматривают разработку проекта Концепции взаимодействия национальных интеллектуальных транспортных систем.

Основной вывод, который можно сделать из анализа правовых актов, касается следующих аспектов. Правовое регулирование отношений в данной сфере в Республике Беларусь и ЕАЭС находится на этапе становления, соответственно, нельзя назвать его эффективным и системным с точки зрения полноты и качества. В некоторой степени можно согласится с исследователями в том, что относительно формирования единой политики и обеспечения технологического суверенитета «ЕАЭС движется по пути Союзного государства» [2]. Действительно, интеграционное объединение ЕАЭС имеет достаточно неоспоримых преимуществ, включая беспошлинное перемещение грузов и иные, на что обращает внимание рост товарооборота, реализация масштабных проектов в транспортной и инфраструктурной областях, соответственно, развивается динамично в глобальном миропорядке, при этом государства-участники все должны занимать единую позицию по ключевым вопросам и направлениям взаимодействия интеграционного объединения.

Таким образом, можно утверждать, что в законодательных актах, включая документы стратегического характера фрагментарно осуществлено правовое регулирование, поскольку выработаны цели и задачи интеллектуальных транспортных систем в определенной сфере, а именно в направлении обеспечения безопасности дорожного движения в Республике Беларусь, включая координацию создания и развития в отношении таких систем на автомобильных дорогах и улицах. Кроме того, путем принятия акта рекомендательного характера в отношении транспортного (автомобильного) контроля определены правовые положения на пространстве ЕАЭС, которые являются основой для разработки решений и распоряжений

органов Союза. Однако не имеется комплексного правового акта, охватывающего все виды транспорта, включая беспилотные транспортные средства, поскольку они, как и иные средства автоматизации, являют собой интеграцию информационных и коммуникационных технологий. Соответственно, важна как разработка указанной выше Концепции, так и внесение дополнений в Протокол о скоординированной (согласованной) транспортной политике (Приложение № 24 к Договору о Евразийском экономическом союзе от 29 мая 2014 г.) относительно данных инноваций в транспортной сфере, поскольку они неизбежно касаются реализации вышеуказанной политики. В национальном законодательстве требуется правовое регулирование интеллектуальных транспортных систем в рамках закрепления отдельных положений в рамках главы относительно безопасности транспортной деятельности.

На современном этапе развивается система законодательства Союзного государства, которая в перспективе может стать «основанием для создания системы права Союзного государства» [7. С. 144]. Союзное государство России и Беларуси выступает объединением, обладающим достаточно твердыми позициями в укреплении интеграционных отношений и являющееся гарантом безопасности граждан объединения в свете ряда возникающих угроз безопасности и противостояния санкций. Анализ актов, принятых в рамках функционирования Союзного государства и регулирующих вопросы формирования объединенной транспортной системы свидетельствует о том, что меры по сближению законодательства государств-участников данного Союза разработаны, но не все аспекты в развитии данных отношений учитываются в силу отсутствия должной научной проработки. Однако отсутствие единых подходов к закреплению вопросов его ведения тормозит интеграционное взаимодействие. Новый вектор в транспортной сфере двух стран, обозначающий актуальность сотрудничества в рамках разработки единого порядка управления системами транспорта, диктует и потребность в новом подходе к тем отношениям, которые уже получили свое распространение. Предлагается выработать правовой механизм применения интеллектуальных транспортных систем на региональном уровне в целях обеспечения безопасности на основе устойчивого осуществления транспортной деятельности, включающий оказание взаимной правовой и информационной, а также технической помощи при создании цифровых платформ и иных вопросов, а также создать в Союзном государстве систему подготовки кадров в данной сфере. Совершенствование правового регулирования в рассматриваемой области отношений представляется достаточно перспективным при разработке Основ транспортного законодательства государств-участников Союзного государства с учетом того, что формирование объединенной транспортной политики относится к исключительному ведению Союзного государства. При этом в Российской Федерации разработаны документы программного характера, в частности, принято распоряжение Правительства Российской Федерации от 21 июня 2023 г. № 1630-р «Об утверждении Стратегии развития беспилотной авиации Российской Федерации на период до 2030 г. и на перспективу до 2035 г. и плана мероприятий по ее реализации», а также распоряжение Правительства Российской Федерации от 25 марта 2020 г. № 724-р «Об утверждении Концепции

обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования» и иные концепции и стратегии, включая стандарты, касающиеся безопасности и деятельности интеллектуальных транспортных систем. Вместе с тем следует сопоставлять определения понятий, обогащая науку и не допускать разрозненность в актах Союзного государства, права ЕАЭС и развивать национальное законодательство в тех государствах-членах объединения, где это еще не осуществлено. Поэтому многообразие форм сотрудничества государств обусловливает углубление гармонизации и унификации национального законодательства, включая правовые основы, направленные на развитие транспортной инфраструктуры и обеспечение национальной безопасности.

Развитие отношений в исследуемой сфере нацелено в том числе на реализацию конституционных прав личности, способствует в том числе внедрению мер по охране окружающей среды с учетом объективной значимости «общественных отношений, возникающих в процессе функционирования транспортной системы» [3. С. 7], что доказывает необходимость учета всех аспектов в этой связи, а именно институциональных особенностей, поддержание уровня экологической безопасности. Соответственно, автор данной статьи обращает внимание на роль интеллектуальной транспортной системы как фактора, влияющего на обеспечение права человека на благоприятную окружающую среду [8-10], поскольку правовое обеспечение в данной области «должно способствовать развитию новых технологий в этой сфере» [6], и положительно влиять на все сферы общественных отношений, сферы безопасности и защищенности. Так, интеллектуальные транспортные системы выступают значимым средством «осуществления мониторинга окружающей среды, что позволяет осуществлять оценку изменений и прогноз состояния окружающей среды» [6. С. 130], а требования экологической безопасности следует установить в законодательстве Республики Беларусь, а в Российской Федерации дополнить требованием применения интеллектуальных транспортных систем.

Заключение. Таким образом, преимущества эксплуатации интеллектуальной транспортной системы, такие как информационно-коммуникационный фактор, безопасность, эффективность, экономичность, экологичность, устойчивость транспортной деятельности, будут результативны при системном правовом регулировании отношений в данной области. Проблемы правового регулирования в сфере эксплуатации интеллектуальных транспортных систем охватывают следующие обусловлены недостаточностью разработки правовых норм, что требует комплексного подхода в данной сфере и будет отвечать усилению реализации нормативных правовых актов, затрагивающих многообразный спектр отношений. Однако для создания системного законодательства и значительных институциональных условий функционирования интеллектуальных транспортных систем объективно необходимо выработать направления, систематизирующие и развивающие теоретические основы правового обеспечения данных отношений, которые связаны с решением задач безопасного функционирования транспортных средств «за счет придания активным элементам транспортно-логистической

свойств интеллектуального поведения» [4. С. 57] в вид системы научных подходов на юридическую природу правового регулирования отношений, что следует объединить в концепцию транспортной безопасности, включающую: а) методологии, применимой к данной области регулирования, позволяющей определять пути его совершенствования и при этом решить имеющиеся правовые проблемы; б) сферу правового регулирования и формирование структуры институционального характера; основные принципы обеспечения устойчивости и безопасности в сфере перемещения транспортных средств и последствий такой эксплуатации.

В связи с изложенным представляется утверждать, что в современных условиях особое значение имеет обоснование существования системы отношений в сфере интеллектуальной транспортной системы как единой комплексной сферы правового регулирования с определением ее места и роли в рамках транспортного права, охватывающей неоднородные элементы, подлежащей дальнейшему развитию в юридической науке с определением объектов и субъектов отношений в данной сфере, содержания и оснований их возникновения и прекращения. Данный вывод опирается на позицию о недостаточности регулирования и применения имеющихся правовых положений, а таже системного видения новых развивающихся отношений. Правовое понятие «интеллектуальная транспортная система» следует признать системообразующим при совершенствовании правового регулирования данных отношений на национальном и региональном уровнях.

Более того, выработка доктринальной основы в исследуемой области нуждается в дальнейшем развитии, что включает необходимость обстоятельных исследований междисциплинарного характера, в том числе при взаимодействии на межгосударственном уровне ученых России и Беларуси, осуществляемых на системной основе. Развитие науки транспортного права относительно разграничению видов правоотношений в сфере транспортной безопасности, уточнению предмета правового воздействия позволит совершенствовать национальное законодательство, гармонизировать правовые нормы Союзного государства и государств-членов ЕАЭС для единообразного толкования и применения.

Список литературы

1. Бажина М. А. Интеллектуальные транспортные системы – основа de lega ferenda транспортной системы Российской Федерации // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 630–649.

2. Гриц: Союзное государство Беларуси и России – это интеграционное ядро ЕАЭС. URL: https://sputnik.by/20230823/grits-soyuznoe-gosudarstvo-belarusi-i-rossii--eto-integratsionnoe-yadro-eaes-1078784609.html

3. Землин А. И. К вопросу о включении транспортного права в номенклатуру специальностей научных работников в сфере юриспруденции // Публично-правовые и частноправовые аспекты реализации транспортной стратегии Российской Федерации: сб. науч. ст. / под ред. А. И. Землина. М.: РУСАЙНС, 2023.

4. Иванов Ф. Ф. Интеллектуальные транспортные системы. Минск: Беларус. навука, 2014. 214 с.

5. Капский Д. В., Хотько О. А., Правовые основы транспортной деятельности: учебн. пособие. Минск: Вышэйшая школа, 2019. 317 с.

6. Молчанов А. А. Некоторые правовые аспекты и проблемы использования интеллектуальных транспортных систем // Аграрное и земельное право. 2018. № 2. С. 21–27.

7. Право Союзного государства Беларуси и России: учебник: в 2 т. Т 1. / отв. ред. Р. А. Курбанов. М.: Проспект, 2018. 400 с.

8. Хотько О. А. Правовое обеспечение экологической безопасности при осуществлении транспортной деятельности. Минск: БГУ, 2022. 415 с.

9. Хотько О. А. Теоретические основания законодательного регулирования интеллектуальных транспортных систем в контексте правового обеспечения экологической безопасности и устойчивого развития государства и общества // Искусственный интеллект и тренды цифровизации: материалы Третьего Междунар. трансп.-правового форума, приуроч. к 125-летию Рос. ун-та трансп., Москва, 10–11 февр. 2021 г. / Рос. ун-та трансп. ; под ред. А. А. Чеботаревой, В. Е. Чеботарева. – М.: Юрид. ин-т РУТ (МИИТ), 2021. С. 127–132.

10. Хотько О. А. Цифровизация и экологизация транспортной деятельности на евразийском пространстве: правовые аспекты обеспечения эффективности // Информационная безопасность личности в современном международном праве: материалы кругл. стола, каф. гос. упр. юрид. фак. Белорус. гос. ун-та, Минск, 12 апр. 2022 г. / Белорус. гос. ун-т; редкол.: В. С. Михайловский (гл. ред.), Е. Ф. Довгань, Н. О. Мороз. Минск: БГУ, 2022. С. 294–298.

С. Р. Чеджемов,
доктор педагогических наук, профессор,
Северо-Кавказский горно-металлургический институт
(государственный технологический университет)

ЦИФРОВАЯ БЕЗОПАСНОСТЬ И ПРАВО: К НЕКОТОРЫМ ПРОБЛЕМАМ ПРЕПОДАВАНИЯ КУРСА «ПРАВОВЫЕ ОСНОВЫ ПРИКЛАДНОЙ ИНФОРМАТИКИ»

Аннотация. Вопросы цифрой безопасности сегодня имеют не переоценимое важное значение в условиях, когда между странами и народами так необходимо взаимодействие, которое обеспечит синтез гуманитарной и технической мысли во благо человечества. Но преобладающими становятся действия так называемых недружественных стран, своими санкциями ограничивающих действия нашего государства и его систем в физических цифровых и биологических доменах. В этих условиях должны измениться образовательные стандарты и правовые стереотипы взаимоотношений в системе преподавания в высшей школе, где особенно необходимы практические действия по формированию и развитию правовых знаний. Целью работы является анализ некоторых проблем, связанных с обеспечением технической безопасности посредством преподавания курса «Правовые основы прикладной информатики».

Keywords: прикладная информатика, цифровая безопасность, всеобщее образование в Интернете, киберпреступность, интернет-мошенничество.

DIGITAL SECURITY AND LAW: ON SOME PROBLEMS OF TEACHING THE COURSE "LEGAL BASES OF APPLIED INFORMATION SCIENCE"»

Abstracts. Digital security issues are of great importance today at a time when interaction between countries and peoples is so necessary, which will ensure the synthesis of humanitarian and technical thought for the benefit of humanity. But the actions of the so-called unfriendly countries are becoming predominant, restricting the actions of our state and its systems in physical, digital and biological domains with their sanctions. Under these conditions, they must change educational standards and legal stereotypes of relationships in the system of teaching in higher education, where practical actions are especially needed for the formation and development of legal knowledge. The aim of the work is to analyze some of the problems associated with ensuring digital security and some problems of teaching the course "Legal Foundations of Applied Informatics».

Keywords: applied informatics, digital security, Internet universal education, cybercrime, Internet fraud

Вот уже больше полстолетия прошло с тех пор, как в умы и сердца человечества сначала осторожно, а потом все более нахраписто вошел Интернет – глобальная информационная паутина, окутавшая своими сетями весь мир. Сегодня кто-то сравнивает ее с твердой рукой помощи всеобщего разума, в разы упростившей поиск нужной информации, а кто-то – с липкими сетями старушки Шолоб из столь ныне популярной трилогии Р. Толкиена «Властелина Колец», полагая, что ни одна грязная подворотня прошлого не предоставляла столько вредной информации, сколько может почерпнуть человек с неокрепшим сознанием на просторах Интернета.

Задача педагогов и родителей сделать технический прогресс и Интернет, в частности, союзником в деле достойного воспитания подрастающего поколения. В рамках введения хочется в очередной раз отметить мудрость устроителей настоящей конференции и злободневность проблематики обсуждаемых вопросов. Профессорско-преподавательским составом нашего вуза накоплен определенный опыт в этом плане [1; 2].

Отрадно, что научное сообщество России и в центре, и в регионах не стоит в стороне от решения проблема модернизации информационного пространства, тем более что информационная безопасность сегодня затрагивает все слои нашего общества, в том числе и люди, которые потенциально, как бы стоят дальше всех от проблем информатизации, в частности, пенсионеры. Эта проблема в общем спектре обеспечения информационной безопасности и является ведущей нашего сегодняшнего выступления.

Сегодня нашей системе высшего образования предстоят нелегкие, но крайне необходимые реформам по переходу от «Болонской образовательной системы»

к отечественной, патриотически настроенной системы высшего образования, но при этом наукоемкой. Именно об этих задачах однозначно высказался министр науки и высшего образования В. Н. Фальков, подчеркнувший, что «к Болонской системе надо относиться как к прожитому этапу. Будущее за нашей собственной уникальной системой образования, в основе которой должны лежать интересы национальной экономики и максимальное пространство возможностей для каждого студента».

О необходимости отказа от Болонской системы в той ее части, где знания выступают вне воспитывающего потенциала, думаю, говорить не приходится. В этом вопросе мы полностью согласны с уже прозвучавшими мнениями в отношении соросовских экспериментов в нашей системе образования по сути дела выхолащивающие морально-нравственные ценности и интеллектуально-поисковую деятельность в обучении. Об этом не раз говорили такие известные общественные деятели и ученые нашего государства, как секретарь Совета безопасности РФ Николай Патрушев, вице-спикер Госдумы Петр Толстой, президент Российской академии образования (РАО) Ольга Васильева, ректор МГУ Виктор Садовничий, председатель Ассоциации юристов России Сергей Степашин и многие, многие другие, в том числе и участники настоящей конференции в 2022 году.

Для российской педагогической мысли понятия «обучение и воспитание» взаимосвязаны еще со времен школьной практической деятельности великого русского писателя Льва Толстого, основавшего в своем имении школу и считавшего, что нельзя обучать, не воспитывая и воспитывать не обучая.

Это же идея стала юридической максимой и в федеральном законе «Об образовании» в котором применяется следующее понятие: «образование – единый целенаправленный процесс воспитания и обучения, являющийся общественно значимым благом и осуществляемый в интересах человека, семьи, общества и государства, а также совокупность приобретаемых знаний, умений, навыков, ценностных установок, опыта деятельности и компетенции определенных объема и сложности в целях интеллектуального, духовно-нравственного, творческого, физического и (или) профессионального развития человека, удовлетворения его образовательных потребностей и интересов».

Интернету все возрасты покорны. Главное, чтобы он не стал ареной противоправных действий в различных областях нашей жизнедеятельности. Между тем интернет-мошенничество в сфере мобильных банковских приложений сегодня становится лидирующим в данной сфере противоправных отношений.

В Северо-Кавказском горно-металлургическом институте (государственном технологическом университете», расположенном в г. Владикавказе ряд лет осуществляется обучение по направлению подготовки/специальности: 09.03.03 Прикладная информатика. Направленность (профиль) программы бакалавриата «Прикладная информатика в экономике».

Автором настоящего сообщения разработана и внедрена в учебный процесс по уровню образования – бакалавриат рабочая программа дисциплины «Правовые основы информационной деятельности». Она разработана на основе: Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом

Министерства науки и образования Российской Федерации № 922 от 19.09.2017 (с изменениями и дополнениями № 1456 от 26.11.2020г. и № 83 от 8.02.2021), учебным планом очной формы обучения подготовки бакалавров по направлению 09.03.03 Прикладная информатика.

Цель изучения курса «Правовые основы информационной деятельности» состоит в формировании у студентов правовых знаний, в частности основ российского и международного права, что способствует формированию у обучающихся современного правого мировоззрения и правосознания, необходимых для успешного осуществления профессиональной деятельности.

Задачами изучения дисциплины являются:

– овладение понятиями институтов государства и права, государственно-правовых явлений в современной жизни;

– выработка ценностных жизненных ориентаций, основанных на приоритете прав и свобод человека и гражданина;

– формирование уважения к принципам законности, понимание их особого значения в жизни человеческого общества и в процессе осуществления будущей профессиональной деятельности.

Изучение дисциплины «Правовые основы информационной деятельности» основывается на совокупности знаний, накопленных студентами по гуманитарным и естественным дисциплинам и сам курс, состоит из 9 лекционных тем:

Тема 1. Основы законодательства Российской Федерации о информационной деятельности.

Тема 2. Правовые основы регулирования отношений в сфере информации, информационных технологий и защиты информации.

Тема 3. Правовая охрана авторских и смежных прав в сфере информатики.

Тема 4. Правовая охрана прав на результаты интеллектуальной деятельности и средства индивидуализации в области информатики.

Тема 5. Правовое регулирование отношений, связанных с использованием информационно коммуникационных сетей.

Тема 6. Правовой статус электронного документа. Электронная цифровая подпись. Понятие электронного документооборота.

Тема 7. Правовое регулирование обеспечения информационной безопасности в сфере информатики. Место информационной безопасности в системе национальной безопасности. Концепция информационной безопасности Российской Федерации. Защита информации.

Тема 8. Правовая защита неприкосновенности частной жизни при автоматизированной обработке персональных данных. Информационная безопасность детей.

Тема 9. Юридическая ответственность за правонарушения и преступления в информационной сфере.

Обучающийся, освоивший дисциплину, должен не только владеть информацией, основанной на знании основных положений российского и международного права, регулирующих информационную деятельность, но и разбираться в сущности проблем современного сообщества, их природе, обладать технологиями формирования основ личностного правового мировоззрения.

Сделать это самому студенту будет вряд ли под силу. Во всяком случае большинство наших обучающихся нуждается в квалифицированной помощи преподавателя. Именно под его руководством студенчество будет оттачивать навыки и умения анализировать и синтезировать правовую информацию, связанную с проблемами современного правопорядка, а также природой и технологиями формирования основ личностного правового мировоззрения.

Для этого необходим синтез социально-гуманитарных знаний, навыков и умений, в частности технологии анализа и синтеза положений российского и международного законодательства, связанных с проблемами современного информационного общества и правового личностного мировоззрения и осуществляемых на его основе практических действий.

Современные политико-правовые реалии в мире таковы, что возрастает всплеск так называемой интернет-преступности, зачастую ставящей под угрозу информационную безопасность всего нашего населения и в особенности ее самую незащищенную часть – лиц пожилого возраста – пенсионеров.

Именно они становятся объектами мошенничества с использованием информационных технологий. Так, что впору говорить о технологическом всеобуче для пенсионеров. По аналогии с подобным общественно-политическом явлением, имевшим место в истории отечественного государства и права в 20-е годы XX в., но теперь это должен быть интернет-ликбез.

Тогда речь шла об обучении письму и счету лиц до 60-летнего возраста, сегодня наше общество не может себе позволить такую возрастную градацию. Тем более, что это вполне справедливо может расцениваться как дискриминационная мера по возрасту. И все же рискнем предложить, чтобы наши студенты проводили интернет-ликбез как для всех категорий граждан по ин желанию, так и для лиц старше 50 лет в обязательном порядке.

Сделать это можно и в рамках так называемых юридических клиник, действующих в наших вузах и оказывающих юридическую помощь населению. Необходимо не только научить все наше население азам информационных технологий, но и в целях их безопасности наглядно объяснить уловки так называемым интернет-мошенников. И здесь, думается, реальную помощь могут оказать службы безопасности банков РФ.

Ныне правовые реалии таковы, что информация о всех дееспособных, да и не только, граждан нашего общества хранятся в «компьютерах» различного рода министерствах и ведомствах. Это так называемая интернет-база – списки клиентов государственных учреждений и организаций, да и различного рода интернет записи эпистолярного жанра: родственников, друзей, знакомых, различная информация о них, видеозаписи и фотографии, отражающие наши предпочтения, перемещения, во времени и в пространстве. Особое место среди них занимают сведения о финансовой состоятельности и именно они за последнее время становятся объектом «охоты».

В правоохранительной сфере, занимающейся вопросами экономических правонарушений, появились так называемые антиробингуды зарящиеся на так называемые, «гробовые» сбережения. Средством совершения мошеннических

действия становится сотовая связь, тем более что большинство отечественных, да и мировых банковских систем широко практикуют мобильные версии в смартфонах и айфонах, планшетах и так далее, которые стали и, думается, к сожалению, тенденция эта продолжится, местом и средством киберпреступлений.

Надо отдать должное нашим правоохранительным органам, пытающимся превентивно реагировать на эти случаи, выстраивать не только эффективную оперативно-розыскную, но и аналитическую работу по их профилактике. Так, например, на территории Республики Северная Осетия-Алания в системе МВД был создан и успешно действует отдел по борьбе с противоправным использованием информационно-телекоммуникационных технологий, деятельность которого стала предметом обсуждения на специальном заседании Общественного совета МВД России по РСО-Алания. С отчетом о деятельности выступил начальник отдела, полковник полиции А. Гасиев.

Руководимый им отдел на практике разоблачает распространенные схемы телефонного мошенничества: в сфере банковской деятельности, всевозможные уловки злоумышленников, которые пытаются завладеть имуществом и денежными средствами граждан-пенсионеров.

Для преодоления этих противоправных действий сотрудниками этого отдела, как и иных подразделений МВД России по РСО-Алания проводят профилактическую работу по информированию населения республики о преступных методах мошенников и способах защиты от них. Однако пока еще малоактивны студенты наших высших учебных заведений, в том числе обучающиеся по так называемым «айтишным направлениям».

Вместе с тем именно эта категория обучающейся молодежи может сыграть решающую роль в обеспечении информационной безопасности и взаимодействия различных фигурантов его обеспечения. Думается, что продуктивное исследование данной проблемы невозможно в рамках лишь юридических наук и требует взаимодействия с другими социально-гуманитарными науками в зависимости от того, какой вопрос выдвигается ученым в качестве объекта и предмета исследования.

Банковские интернет-приложения позволяют облегчить жизнь людям, избавить их от личного посещения офисов банков, выстаивания в очередях, но оно же делает клиентов банка легкой «добычей» злоумышленников.

Об актуальности проблематики обеспечения информационной безопасности внутри государства убедительно писал еще в 2015 г. профессор М. М. Кучерявый, считая «одним из системообразующих факторов модернизации структуры и содержания национальной безопасности» [9. С. 25]. Думается, что настало время обратится и к так называемой «банковской» безопасности посредством мобильных технологий.

В качестве заключения хочется подчеркнуть, что вышеизложенные авторские рассуждения, конечно же, не исчерпывают проблему исследования. Надеемся на заинтересованный диалог по поднимаемым вопросам и способам их решения. Считаем так же целесообразным, чтобы в Уголовный Кодекс РФ были внесены изменения, ужесточающие наказание за совершенные преступления посредством информационных технологий.

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. Журавлев М. М. Либерально-юридические аспекты правового государства. Вестник Томского государственного университета. Право. 2016. №1 (19). С. 5-12.

3. Полякова Т. А., Филатова Л. В. Влияние глобализации на построение информационного общества в России // Вестник РУДН. Серия: Информатизация образования. 2008. № 1. С. 20–26.

4. Полякова Т. А, Минбалеев А. В. Новые вызовы и угрозы в информационном пространстве: правовые проблемы обеспечения информационной безопасности // Информационное право. 2018. № 4. С. 44–46.

5. Химченко А. И. Информационное общество: правовые проблемы в условиях глобализации: дис. ... канд. юрид. наук. М., 2014.

6. Чеджемов С. Р., Золоева З. Т. Ресурс информационного права в профилактике коррупционных проявлений в учебном процессе вузов на основе применения блокчейн-технологий. Юридическое образование и наука. 2019. № 3. С. 22–25.

7. Чеджемов С. Р., Золоева З. Т. Глобальное информационное общество – зло или благо человечества? // Государственная власть и местное самоуправление. 2022. № 7. С. 10–14.

8. Кучерявый М. М. К осознанию информационного суверенитета в тенденциях глобального информационного пространства // Наука, новые технологии и инновации Кыргызстана. 2015. № 12. С. 22–27.

А. М. Черненко,
кандидат физико-математических наук,
Институт космических исследований
Российской академии наук

АКТУАЛЬНЫЕ ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПАТЕНТНЫХ ИССЛЕДОВАНИЯХ

Аннотация. Искусственный интеллект в патентных исследованиях используется для автоматизации процессов анализа патентных данных, выявления тенденций развития технологий, прогнозирования патентоспособности и определения классов МПК. В статье рассмотрены различные аспекты применения искусственного интеллекта (ИИ) в области патентного исследования: использование алгоритмов обработки естественного языка (NLP) для анализа текстовых описаний патентов и выделения ключевых слов, фраз и терминов, методы машинного обучения для анализа признаков патентов, связанных с патентоспособностью, и прогнозирования вероятности патентоспособности. Обсуждаются подходы к идентификации семантически схожих патентов, создание структурированных

отчетов на основе результатов и анализ с помощью ИИ больших объемов патентных данных для построения патентных ландшафтов. Проведен обзор и сравнение наиболее известных сервисов для патентных исследований с функциями ИИ.

Ключевые слова: искусственный интеллект, машинное обучение, патенты, патентные исследования, патентный поиск, патентоспособность, уровень техники, патентоведение, патентная чистота, патентоспособность, тенденции развития, результаты интеллектуальной деятельности, РИД, ИИ, интеллектуальная собственность

CURRENT OPPORTUNITIES AND PROSPECTS OF ARTIFICIAL INTELLIGENCE APPLICATION IN PATENT RESEARCH

Abstract. Artificial Intelligence (AI) is utilized in patent research to automate processes of patent data analysis, identify technology trends, forecast patentability, and determine IPC classes. This article explores various aspects of AI application in patent research. It covers the use of Natural Language Processing (NLP) algorithms to analyze patent text descriptions, extract keywords, phrases, and terms. It also delves into machine learning methods for analyzing patent features related to patentability and predicting patent eligibility. Other aspects include identifying semantically similar patents, generating structured reports based on the results, and using AI to analyze large volumes of patent data to construct patent landscapes. An overview and comparison of the main patent research systems with artificial intelligence functionalities have been conducted.

Keywords: artificial intelligence, AI, machine learning, ML, deep learning, prior art, search queries, search strategies, patentability, technology trends, patent law, patent research, patent intelligence, intellectual property

Введение. Патентные исследования играют ключевую роль в современном мире, особенно в области инноваций и технологического развития. Патенты представляют собой юридические документы, которые защищают интеллектуальную собственность и права инноваторов на их изобретения, технические решения и технологии.

Важность патентных исследований обусловлена несколькими факторами:

– Стимулирование инноваций: Патенты предоставляют инноваторам экономические стимулы для создания новых технологий и изобретений. Они обеспечивают монопольные права на использование, продажу и распространение изобретений, что способствует привлечению инвестиций в исследования и разработки.

– Защита интеллектуальной собственности: Патенты предоставляют юридическую защиту авторским правам и интеллектуальной собственности.

– Повышение конкурентоспособности компаний: благодаря патентам компании могут предлагать уникальные и инновационные продукты или услуги, что помогает улучшить их позицию на рынке, привлечь новых клиентов.

– Исследование и анализ технической информации: Патенты содержат детальные технические описания изобретений. Исследователи и инженеры могут

использовать патентные базы для доступа к информации о существующих технологиях и тенденциях развития в различных отраслях.

– Предотвращение нарушений: Патентные исследования позволяют предотвратить нарушение чужих патентных прав.

Использование искусственного интеллекта для анализа текстовых описаний патентов. Современные патентные исследования сталкиваются с огромными объемами текстовых данных, содержащихся в патентных документах. Искусственный интеллект предоставляет мощные инструменты для обработки и анализа этих текстовых описаний, что существенно улучшает процесс извлечения значимой информации из патентных документов.

Обработка естественного языка (NLP) [11] позволяет ИИ понимать и анализировать человеческий язык. В контексте патентных исследований, NLP используется для извлечения ключевых слов и фраз из текстовых описаний патентов [3]. Алгоритмы NLP автоматически определяют существенные термины, которые описывают технические особенности и инновационные аспекты изобретения. Это позволяет исследователям быстро и точно определить суть патентных документов и выявить ключевые понятия, связанные с темой исследования.

При анализе текстовых описаний патентов, часто возникает необходимость обработки словоформ для улучшения качества и точности анализа. ИИ использует методы лемматизации и стемминга для приведения слов к их базовой форме или корню [2]. Так, лемматизация – это процесс приведения слова к его базовой, словарной форме, которая называется «леммой». Лемма представляет собой основной корень слова, без приставок, окончаний и других словоизменительных форм. Применение лемматизации позволяет свести различные формы одного слова к единой форме, что облегчает анализ текста и уменьшает размер словаря.

Пример:

Лемма слова «бежит» – «бежать»

Лемма слова «мыли» – «мыть»

Стемминг – это процесс обрезания аффиксов (приставок и суффиксов) у слова для получения его корневой формы, которая называется «стем». В отличие от лемматизации, стемминг может приводить к получению не всегда правильной формы слова, но при этом он работает гораздо быстрее.

Пример:

Стем слова «бежит» – «беж»

Стем слова «мыли» – «мыл»

Оба метода лемматизации и стемминга используются для предварительной обработки текста перед его анализом, классификацией, поиском или другими задачами NLP. Выбор между лемматизацией и стеммингом зависит от конкретной задачи и требований к точности обработки текста.

Далее при помощи процесса Part-of-Speech Tagging (POS-тегирование) производится определение частей речи каждого слова в тексте (например, существительное, глагол, прилагательное и т. д.) [14]. POS-тегирование позволяет сравнивать и искать патенты на основе их лингвистических характеристик. Например, можно искать патенты, в которых определенные типы слов или части речи

встречаются в близком контексте. Также POS- тегирование может помочь выделить и классифицировать технические характеристики и элементы в патентных текстах, такие как материалы, процессы и устройства.

Последний этап анализа – извлечение именованных сущностей (Named Entity Recognition, NER), таких как названия компаний, местоположения, персоны, даты и т. д. [9].

Задача NER состоит в том, чтобы идентифицировать и выделить в тексте упоминания именованных сущностей, а также классифицировать их по предопределенным категориям, таким как «Person» (Личность), «Organization» (Организация), «Location» (Локация), «Date» (Дата) и т. д. Это позволяет автоматически распознавать именованные сущности в больших объемах текста, что может быть полезно для анализа информации, поиска, категоризации данных и других задач.

Пример: В предложении «Apple Inc. была основана Стивом Джобсом и Стивом Возняком в 1976 году в городе Купертино», задачей NER будет идентифицировать следующие именованные сущности:

«Apple Inc.» – Организация

«Стивом Джобсом» – Личность

«Стивом Возняком» – Личность

«1976 году» – Дата

«Купертино» – Локация

NER широко применяется в обработке текстов для множества приложений, таких как информационный поиск, анализ социальных медиа, автоматическая обработка текстовых данных, извлечение информации, обработка документов, анализ настроений и другие задачи анализа и классификации текста. Благодаря тому, что основной вид патентной документации – описания изобретений – имеют унифицированную структуру, извлечение из нее именованных сущностей легко поддается автоматизации и осуществляется с гораздо более высокой степенью надежности чем из непатентной документации.

Итак, из описания изобретения можно извлечь различные типы именованных сущностей, включая:

– Имена авторов, изобретателей, патентообладателей, патентных поверенных, названия компаний или других организаций, связанных изобретением.

– Специализированные и технические термины, описывающие изобретения.

– Местоположения, связанные с исследованиями, тестированием или внедрением изобретения. Страны приоритета.

– Даты подачи заявки, даты публикаций и другие важные сроки.

– Числовые значения, параметры, характеристики изобретения.

– Товарные знаки и бренды.

– Названия продуктов, технологий или процессов, которые являются частью изобретения.

– Классы Международной патентной классификации (МПК) и/или Совместной патентной классификации (СПК).

– Регистрационные номера заявок и свидетельств.

– Прочие элементы библиографической и технической патентной информации, являющиеся обязательными компонентами патентного документа.

Извлечение именованных сущностей из описания изобретения может быть полезным для автоматической индексации, поиска по патентным базам данных, анализа технических тенденций и обнаружения новых технологических решений.

Идентификация семантически схожих патентов с помощью ИИ. Искусственный интеллект применяет методы семантического анализа и машинного обучения для автоматического выявления семантических связей между патентными документами. В процессе идентификации семантически схожих патентов, системы ИИ строят векторные представления для каждого текстового описания патента [13]. Эти векторы содержат числовую информацию о смысловой структуре текста и его содержании. Одним из наиболее распространенных методов является преобразование текстовых описаний патентов в числовые векторы с помощью методов word2vec, GloVe или FastText (см., например, [12]). Эти методы позволяют представить слова в виде векторов в многомерном пространстве, где близкие по смыслу слова имеют близкие векторы.

Затем, используя алгоритмы кластеризации, такие как k-means, hierarchical clustering, DBSCAN и другие ИИ группирует патентные документы на основе схожести их векторных представлений [7]. Патенты, которые имеют близкие векторные представления, считаются семантически схожими и объединяются в один кластер. Таким образом, системы ИИ выявляют группы патентов, которые относятся к общей тематике или имеют схожие инновационные решения.

Дополнительно, ИИ может использовать методы сравнения текста, такие как TF-IDF (Term Frequency-Inverse Document Frequency), для выявления наиболее схожих фрагментов между патентными документами [8]. Это позволяет выделить общие технические концепции и ключевые слова, которые характеризуют семантически схожие патенты.

Искусственный интеллект как вспомогательный инструмент в предварительном поиске непатентных источников информации. Искусственный интеллект активно используется для улучшения процесса поиска информации в различных системах, включая поиск патентов и научных статей. Одним из методов, где применяется ИИ, является «Query Expansion» (расширение запроса).

Query Expansion – это техника, которая позволяет автоматически расширить или дополнить исходный поисковый запрос, чтобы улучшить качество и точность результатов поиска. При использовании Query Expansion система автоматически анализирует и понимает содержание исходного запроса и затем расширяет его, добавляя синонимы, близкие по смыслу термины, и другие связанные ключевые слова.

Как работает Query Expansion:

– Анализ запроса: Система анализирует исходный запрос, идентифицирует ключевые слова и термины, которые важны для пользователя.

– Синонимы и близкие термины: Используя методы обработки естественного языка (NLP) и машинного обучения, система определяет синонимы и близкие по смыслу термины для каждого ключевого слова.

– Расширение запроса: Система добавляет найденные синонимы и близкие термины к исходному запросу, чтобы расширить его.

– Поиск расширенного запроса: Расширенный запрос используется для поиска информации, и система возвращает результаты, которые могут быть более полезны и точны для пользователя.

Использование ИИ в Query Expansion позволяет системам автоматически обрабатывать большие объемы данных и анализировать сложные связи между терминами, что повышает эффективность и качество поиска информации.

Применение искусственного интеллекта для прогнозирования патентоспособности. В современных патентных исследованиях ИИ активно применяется для предсказания вероятности отказа в регистрации изобретения. Этот процесс включает анализ различных признаков патентов, применение методов машинного обучения и предоставляет значительные преимущества в оценке патентоспособности.

Анализ признаков патентов, связанных с патентоспособностью. Первый шаг в прогнозировании патентоспособности – это анализ признаков, которые могут влиять на решение о выдаче патента. Такие признаки могут включать технические аспекты изобретения, степень новизны, изобретательский уровень, патентоспособность по сравнению с уже существующими патентами и многое другое. ИИ способен автоматически извлечь и классифицировать эти признаки из текстовых описаний патентов, что значительно облегчает и ускоряет процесс анализа.

Анализ признаков патентов, связанных с патентоспособностью, является ключевым шагом в использовании ИИ для прогнозирования вероятности успешного получения патента для конкретного изобретения. Для этого необходимо выделить релевантные признаки из текстовых описаний патентов и структурированных данных, которые могут оказывать влияние на решение патентного офиса.

Искусственный интеллект применяет описанные выше методы обработки естественного языка (NLP) для анализа текстовых описаний патентов.

Построение и валидация модели прогнозирования. Собранные признаки и данные используются для построения модели прогнозирования. Модель обучается на исторических данных, которые содержат информацию о патентах, выданных или отклоненных офисом по интеллектуальной собственности. Модель ищет закономерности и зависимости между признаками и исходом получения патента для создания прогноза для нового изобретения [6].

После построения модели необходимо провести ее валидацию на новых данных, чтобы убедиться в ее точности и надежности. Модель проверяется на тестовой выборке, которая не использовалась при обучении, для оценки ее производительности и способности обобщать знания на новые данные.

Методы машинного обучения для прогнозирования вероятности патентоспособности. Для прогнозирования вероятности патентоспособности конкретного изобретения ИИ использует различные методы машинного обучения [4]. Эти методы позволяют анализировать обширные объемы патентных данных и выявлять закономерности, которые сложно обнаружить вручную. Ниже представлены основные методы машинного обучения, применяемые для этой цели:

– Логистическая регрессия является одним из наиболее распространенных методов машинного обучения для задач классификации. Она используется

для предсказания вероятности принадлежности объекта к одному из двух классов – в данном случае, к патентоспособному или непатентоспособному классу. Логистическая регрессия строит линейную модель, которая оценивает влияние различных признаков на вероятность патентоспособности.

– Случайный лес (Random Forest) является ансамблевым методом машинного обучения, который объединяет несколько деревьев решений для принятия окончательного решения. Каждое дерево строится на случайной подвыборке данных и случайных признаках, что позволяет избежать переобучения модели. Случайный лес обладает высокой точностью и устойчив к шумам в данных, что делает его эффективным методом для прогнозирования патентоспособности.

– Нейронные сети – это глубокие модели машинного обучения, которые имитируют работу человеческого мозга. Они состоят из множества связанных между собой нейронов, которые обрабатывают данные и выдают результат. Нейронные сети обладают высокой гибкостью и способностью обучаться на больших объемах данных, что позволяет достичь высокой точности прогнозирования патентоспособности.

– Градиентный бустинг – это еще один ансамблевый метод машинного обучения, который объединяет несколько слабых моделей в одну сильную. Он работает поэтапно, последовательно обучая модели и исправляя ошибки предыдущих моделей. Градиентный бустинг способен эффективно моделировать сложные зависимости в данных и обеспечивает высокую точность прогнозирования.

– Метод опорных векторов (Support Vector Machines, SVM) используется для задач классификации и регрессии. Он находит оптимальное разделение классов в пространстве признаков с помощью опорных векторов, что позволяет достичь высокой разделяющей способности. SVM подходит для прогнозирования вероятности патентоспособности на основе множества признаков из патентных данных.

Использование указанных методов машинного обучения позволяет с высокой точностью прогнозировать вероятность патентоспособности конкретного изобретения.

Автоматизация процесса создания структурированных отчетов о патентном исследовании на основе полученных результатов помощью искусственного интеллекта. Создание структурированных отчетов является важным этапом в патентных исследованиях, поскольку предоставление информации в удобной и понятной форме является ключевым для принятия обоснованных решений.

Полученные результаты анализа патентных данных структурируются и организуются в соответствии с предопределенным шаблоном отчета. Используя методы семантического анализа и машинного обучения, система ИИ определяет связи и зависимости между различными элементами информации, что позволяет создать целостный и логически связанный отчет. Здесь следует отметить, что на данный момент нет конкретных систем или программных решений, которые обеспечивающий автоматизацию процесса создания отчетов по патентным исследованиям в соответствии с ГОСТом.

Одним из важных аспектов создания структурированных отчетов является визуализация данных. Система ИИ использует различные методы визуализации,

такие как графики, диаграммы и таблицы, чтобы наглядно представить полученные результаты. Визуализация помогает сделать отчет более понятным и удобным для восприятия, а также выявить тенденции и закономерности в патентных данных.

После завершения процесса анализа и структурирования данных, система ИИ генерирует пользовательский отчет. В отчете содержатся все полученные результаты, представленные в понятной и удобной для пользователя форме. Отчет может включать краткое описание найденных патентов, ключевые слова, классификацию по МПК, связанные патентные документы и другую важную информацию.

Анализ больших объемов патентных данных с помощью искусственного интеллекта – инструмент построения патентных ландшафтов. Анализ больших объемов патентных данных является критическим аспектом патентных исследований, поскольку позволяет выявить тенденции развития технологий, обнаружить новые технические решения и оценить конкурентное положение в определенной области.

Обнаружение тенденций развития технологий и выявление новых технических решений с помощью ИИ является одним из ключевых преимуществ его применения в анализе патентных данных. ИИ обладает уникальными возможностями обработки и анализа больших объемов информации, что позволяет исследователям и бизнес-аналитикам выявлять важные тенденции и инновационные направления в различных отраслях.

Используя методы машинного обучения, ИИ способен выявлять инновационные направления в патентных данных [5]. Алгоритмы кластеризации и классификации помогают группировать похожие патенты и выделить наиболее перспективные технологические решения. Это позволяет исследователям определить, какие области технологий находятся в стадии активного развития и являются приоритетными для дальнейшего изучения.

С помощью ИИ можно осуществлять прогнозирование будущих технологических трендов на основе анализа патентных данных (см., например, [10]). ИИ способен определить, какие технологии и инновации находятся в стадии активного развития, и предсказать их будущее развитие. Это позволяет компаниям и организациям принимать информированные решения о направлении своих исследовательских и разработочных проектов.

Искусственный интеллект помогает выявить потенциальных партнеров для сотрудничества и инвестиционных возможностей на основе анализа патентных данных [1]. Алгоритмы анализа позволяют выделить компании и организации, которые активно разрабатывают новые технологии и имеют перспективные патенты. Это позволяет исследователям и бизнес-аналитикам находить потенциальных партнеров для сотрудничества, а инвесторам – инноваторов.

Обзор и сравнение основных систем патентных исследований с функциями искусственного интеллекта. На рынке существует несколько платных сервисов для патентных исследований, которые используют ИИ и машинное обучение для обработки и анализа патентных данных. Вот наиболее известные из них, условно ранжированные по популярности: PatSnap, Clarivate Analytics (ранее

Derwent Innovation), Questel Orbit, PatentSight, Cipher, PatSeer, IP.com. Любая из этих систем предоставляет набор востребованных патентоведом инструментов высокого уровня, опирающихся на ИИ, однако каждая имеет свои отличительные особенности, описанные ниже:

Искусственный интеллект играет ключевую роль в сервисе PatSnap, предоставляя разнообразные функции для патентных исследований и анализа интеллектуальной собственности:

Патентный поиск и классификация: PatSnap использует ИИ для выполнения быстрого и точного поиска патентов по ключевым словам, классам, компаниям, авторам и другим параметрам. Также платформа предоставляет автоматическую классификацию патентов, что позволяет пользователю систематизировать патентные данные для дальнейшего анализа.

Анализ технических трендов и патентных портфелей: ИИ в PatSnap позволяет проводить анализ технических трендов, выявлять новые разработки и определять важные сегменты рынка. Также сервис помогает анализировать патентные портфели компаний и конкурентов для оценки их стратегий интеллектуальной собственности.

Определение патентоспособности: PatSnap использует ИИ для определения вероятности успешного получения патента на новое изобретение, анализируя его уникальность и сходство с существующими патентами.

Поиск технологических аналогов и патентной литературы: Платформа использует ИИ для поиска технологических аналогов и схожих патентов, что помогает понять уровень конкуренции и особенности технических решений.

Прогнозирование технологических трендов: ИИ в PatSnap может использоваться для прогнозирования технологических трендов и оценки развития определенных технологий в будущем.

Систематизация и анализ данных: ИИ позволяет PatSnap обрабатывать и систематизировать большие объемы патентных данных, что делает анализ и сравнение информации более эффективным и удобным для пользователей.

Патентные алерты и уведомления: Сервис предоставляет возможность устанавливать алерты и уведомления на основе заданных пользователем критериев, чтобы быть в курсе новых патентных заявок и изменений в технологической области.

В августе 2023 г. PatSnap представила пользователям чат-бот PatSnapGPT с сервисами “Patent Search Expert,” “Patent Technical Disclosure Assistant,” and “R&D Assistant”, которые позволяют патентоведу вести диалог с ИИ на естественном языке Clarivate Analytics предоставляет широкий спектр сервисов для анализа интеллектуальной собственности, и многие из них включают функции ИИ:

Патентный поиск и классификация: ИИ используется для выполнения точного поиска патентов и иных документов по различным параметрам, таким как ключевые слова, классы МКПО, авторы, даты и другие характеристики. Автоматическая классификация патентов также помогает быстро организовать данные для дальнейшего анализа.

Анализ технических трендов и конкурентной активности: С использованием ИИ, Clarivate Analytics может проанализировать большие объемы патентных

данных и выявить технические тренды, определить активность конкурентов, а также предоставить обзоры по определенным технологическим областям.

Определение патентоспособности: С помощью ИИ сервис может предсказывать вероятность успешного получения патента на основе анализа сходства существующих патентов и других факторов, что помогает принять обоснованное решение о патентовании.

Рекомендации по патентам и техническим аналогам: Clarivate Analytics может использовать ИИ для предоставления рекомендаций по патентам, связанным с интересующей вас областью, а также для нахождения технических аналогов и сходных решений.

Прогнозирование технологических трендов: ИИ может быть задействован для прогнозирования технологических трендов и предсказания развития определенных технических областей.

Анализ портфеля патентов и оценка конкурентоспособности: Clarivate Analytics позволяет проводить анализ патентного портфеля компании или конкурента с использованием ИИ, что помогает оценить их интеллектуальную собственность и конкурентоспособность на рынке.

Патентные алерты и мониторинг: ИИ позволяет настраивать автоматические патентные алерты и мониторинг новых патентных заявок, чтобы быть в курсе последних разработок в выбранных областях.

Помощь в подборе наименований и названий бренда: алгоритм ИИ генерирует предложения для названий на основе заданных, одновременно анализируя их существующие доменные имена и имена в социальных сетях. Затем составляется список вариантов, включая семантические и фонетические альтернативы с лингвистическими комментариями, которые помогают выбрать оптимальный вариант.

PatentSight. Преимущество этого сервиса – высокое качество исходных патентных данных и их верификация. Например, система отображает исторические изменения названий компаний, учитывает слияния и поглощения, а также исправляет орфографические ошибки и ошибки при переводе.это Эта платформа для анализа интеллектуальной собственности включает различные функции ИИ для более точного и эффективного патентного анализа:

Автоматическая классификация и кластеризация патентов: ИИ в PatentSight позволяет автоматически классифицировать и группировать патенты по сходству и тематике. Это упрощает организацию и анализ больших объемов патентных данных.

Анализ технических трендов и прогнозирование: PatentSight использует ИИ для выявления технических трендов и прогнозирования развития определенных технологических областей на основе анализа патентных данных.

Оценка патентного портфеля и конкурентоспособности: С помощью ИИ PatentSight позволяет оценить стоимость и конкурентоспособность патентного портфеля компании или конкурента, проводя анализ и сравнение патентных данных.

Поиск технологических аналогов и партнеров: PatentSight использует ИИ для поиска технологических аналогов и партнеров, что помогает выявить новые возможности для сотрудничества и развития бизнеса.

Анализ рисков и возможностей в патентных данных: ИИ позволяет выявлять риски и возможности в патентных данных, что помогает принимать обоснованные решения по интеллектуальной собственности.

Патентные алерты и мониторинг: PatentSight предоставляет возможность устанавливать автоматические патентные алерты и мониторинг новых патентных заявок, чтобы быть в курсе последних разработок и изменений в выбранных областях.

Интеграция данных: PatentSight может интегрироваться с другими внутренними источниками данных компании, что позволяет получать более полное представление о патентном портфеле и его влиянии на бизнес.

Cipher – это платформа для анализа интеллектуальной собственности, сильной стороной которой является использование технологий машинного обучения для построения патентных ландшафтов. Данные платформа предлагает и другие функции ИИ для обработки и анализа патентных данных:

Патентный поиск и классификация: ИИ в Cipher обеспечивает эффективный патентный поиск, используя различные параметры, такие как ключевые слова, классы МКПО, авторы, компании и даты. Также платформа предлагает автоматическую классификацию патентов, что упрощает организацию данных.

Анализ технических трендов и конкурентной активности: Cipher использует ИИ для проведения анализа технических трендов и выявления конкурентной активности на основе данных патентов. Это позволяет получить представление о технических разработках в отрасли и оценить деятельность конкурентов.

Оценка патентной ценности и рисков: С помощью ИИ Cipher проводит оценку патентной ценности, выявляет риски нарушения патентных прав и помогает принимать обоснованные решения о стратегии интеллектуальной собственности. Поиск технологических аналогов и партнеров: Cipher использует ИИ для поиска технологических аналогов и потенциальных партнеров, что помогает выявить новые возможности для сотрудничества и развития бизнеса.

Прогнозирование технологических трендов: ИИ в Cipher может быть задействован для прогнозирования технологических трендов и оценки развития определенных технических областей в будущем.

Автоматическая обработка данных и аналитика: Cipher использует ИИ для автоматической обработки больших объемов патентных данных и предоставляет аналитические отчеты и графики для наглядного представления результатов анализа.

Патентные алерты и мониторинг: Сервис предоставляет возможность устанавливать автоматические патентные алерты и мониторинг новых патентных заявок, чтобы быть в курсе последних разработок в выбранных областях.

Questel Orbit – это патентный информационный сервис, состоящий из ядра и ряда дополнительных специализированных модулей. Основанный на алгоритмах машинного обучения модуль автоматической патентной классификации AI-Classifier использует ИИ, чтобы быстро искать и классифицировать патентные документы в соответствии с конкретными задачами. Поддерживается возможность создания неограниченного количества ИИ-классификаторов, и их интеграции с сервисом патентных алертов. Сервис предоставляет также и полный набор стандартных инструментов ИИ для анализа и обработки патентных данных:

Патентный поиск и классификация: Questel Orbit использует ИИ для выполнения точного и быстрого патентного поиска по ключевым словам, классам МКПО, авторам, компаниям и другим параметрам. Платформа также предоставляет автоматическую классификацию патентов, что облегчает организацию и анализ данных.

Анализ технических трендов и конкурентоспособности: Questel Orbit использует ИИ для выявления технических трендов и анализа конкурентной активности на основе патентных данных. Это помогает пользователям быть в курсе последних разработок и действий конкурентов.

Оценка патентной ценности и прогнозирование: С помощью ИИ Questel Orbit позволяет оценивать стоимость патентов и предсказывать их будущую ценность на основе анализа технических тенденций.

Поиск технологических аналогов и партнеров: Questel Orbit использует ИИ для поиска технологических аналогов и потенциальных партнеров, что помогает пользователям выявить новые возможности для сотрудничества и развития бизнеса.

Патентные алерты и мониторинг: Сервис предоставляет возможность настройки автоматических патентных алертов и мониторинга новых патентных заявок, чтобы быть в курсе последних разработок в выбранных областях.

Автоматическая обработка данных и аналитика: Questel Orbit использует ИИ для автоматической обработки больших объемов патентных данных и предоставляет аналитические отчеты и графики для более удобного визуализации результатов анализа.

Интеллектуальный поиск и аналитика текста: ИИ в Questel Orbit обеспечивает интеллектуальный поиск и аналитику текста, что позволяет пользователям находить более точные и соответствующие результаты поиска.

PatSeer – это патентный информационный сервис, который предоставляет различные функции ИИ, которые можно использовать как в рамках автоматизированного поиска, так и индивидуально – на каждом этапе анализа и обработки патентных данных. Вот некоторые из основных функций ИИ, предоставляемых сервисом PatSeer:

Патентный поиск и классификация: PatSeer использует ИИ для выполнения точного и быстрого патентного поиска, по ключевым словам, классам МКПО, авторам, компаниям и другим параметрам. Платформа также предоставляет автоматическую классификацию патентов, что облегчает организацию и анализ данных.

Анализ технических трендов и конкурентоспособности: PatSeer использует ИИ для выявления технических трендов и анализа конкурентной активности на основе патентных данных. Это помогает пользователям быть в курсе последних разработок и действий конкурентов.

Оценка патентной ценности и прогнозирование: С помощью ИИ PatSeer позволяет оценивать стоимость патентов и предсказывать их будущую ценность на основе анализа технических тенденций.

Поиск технологических аналогов и партнеров: PatSeer использует ИИ для поиска технологических аналогов и потенциальных партнеров, что помогает пользователям выявить новые возможности для сотрудничества и развития бизнеса.

Патентные алерты и мониторинг: Сервис предоставляет возможность настройки автоматических патентных алертов и мониторинга новых патентных заявок, чтобы быть в курсе последних разработок в выбранных областях.

Автоматическая обработка данных и аналитика: PatSeer использует ИИ для автоматической обработки больших объемов патентных данных и предоставляет аналитические отчеты и графики для более удобной визуализации результатов анализа.

Интеллектуальный поиск и аналитика текста: ИИ в PatSeer обеспечивает интеллектуальный поиск и аналитику текста, что позволяет пользователям находить более точные и соответствующие результаты поиска.

IP.com – это патентный информационный сервис, который предоставляет различные функции ИИ для анализа и обработки патентных данных. Среди других сервисов IP.com выделяется качеством и глубиной проработки обучаемых моделей, как в части алгоритмов, так и качества и разноплановости используемых для обучения патентных данных. Вот некоторые из основных функций ИИ, предоставляемых сервисом IP.com:

Автоматический патентный поиск: IP.com использует ИИ для выполнения автоматического патентного поиска, основанного на ключевых словах, классах МКПО и других параметрах. Это позволяет быстро найти патенты, относящиеся к интересующимся областям.

Анализ технических трендов: ИИ в IP.com позволяет выявлять технические тренды на основе анализа патентных данных. Это помогает пользователям быть в курсе последних разработок и инноваций в выбранных областях.Определение патентоспособности: IP.com использует ИИ для оценки патентоспособности изобретений, анализируя их уникальность и сходство с существующими патентами.

Прогнозирование технологических трендов: С помощью ИИ IP.com может предсказывать будущие технологические тренды на основе анализа данных патентов.

Оценка конкурентной активности: IP.com использует ИИ для анализа патентных данных конкурентов, что позволяет пользователям оценить их активность и стратегию в области интеллектуальной собственности.

Поиск технологических аналогов и партнеров: IP.com использует ИИ для поиска технологических аналогов и потенциальных партнеров, что помогает пользователям выявить новые возможности для сотрудничества и развития бизнеса.

Интеллектуальный анализ текста: ИИ в IP.com обеспечивает интеллектуальный анализ текста патентных документов, что позволяет пользователям находить более точные и соответствующие результаты поиска.

Также некоторые функции ИИ постепенно интегрируются в патентные сервисы стран и организаций. Например, в системе поиска SearchPlatform Роспатента реализован «Поиск похожих документов с использованием искусственного интеллекта» (searchplatform.rospatent.gov.ru/equal_docs), который принимает на вход не поисковый запрос, а текстовое описание изобретения. В сервисе Google Patents поиск патентов осуществляется по обычным запросам, однако далее система позволяет использовать ИИ для анализа уровня техники для найденных патентов и

поиска их аналогов. Текст статьи должен содержать введение, основную часть статьи и заключение.

Заключение. Искусственный интеллект предоставляет ряд ключевых технологий, революционизирующих патентные исследования. Методы обработки естественного языка (NLP) позволяют анализировать текстовые описания патентов, выделяя ключевые слова и термины. Алгоритмы машинного обучения способствуют более точному анализу признаков патентов, связанных с патентоспособностью, и предсказывают вероятность патентоспособности. Кластерный анализ с применением алгоритмов, таких как k-means и DBSCAN, позволяет группировать патентные документы на основе схожести их векторных представлений.

В итоге, применение ИИ в патентных исследованиях обеспечивает высокую точность и эффективность анализа патентных данных. Это включает в себя автоматическую классификацию патентов, прогнозирование патентоспособности, создание структурированных отчетов и анализ крупных объемов данных. Сервисы, основанные на ИИ, такие как PatSnap и Clarivate Analytics, предоставляют современные инструменты для эффективной работы с патентами. Использование Google Patents и Lens.org дополняет этот арсенал с бесплатными исследовательскими ресурсами. Разработки в этой области обещают новые перспективы для улучшения патентных исследований и инновационных разработок в целом.

Список литературы

1. Aristodemou L., Tietze F.. The state-of-the-art on Intellectual Property Analytics (IPA): A literature review on artificial intelligence, machine learning and deep learning methods for analysing intellectual property (IP) data. // World Patent Information. 2020. № 55. Pp. 37–51.

2. Arts S., Jianan H., and Gomez J. K. Natural language processing to identify the creation and impact of new technologies in patent text: Code, data, and new measures // Research Policy. 2021. Vol. 50, №. 2. Art. 104144.

3. Cascini G. and Neri F., Natural Language Processing for patents analysis and classification // ETRIA World Conf., TRIZ Future, 2004. Pp. 199–212.

4. Jiang H., Fan S., Zhang N., Zhu B., Deep learning for predicting patent application outcome: The fusion of text and network embeddings // Journal of Informetrics. 2023. Vol. 17. Iss. 2. Art. 101402.

5. Kwon, U., Geum, Y. Identification of promising inventions considering the quality of knowledge accumulation: a machine learning approach // Scientometrics. 2020. Vol. 125. Pp. 1877–1897.

6. Lee C-W, Tao F, Ma Y-Y, Lin H-L. Development of Patent Technology Prediction Model Based on Machine Learning // Axioms. 2022. Vol. 11. № 6 Art. 253.

7. Lei L., Qi J. and Zheng K., Patent Analytics Based on Feature Vector Space Model: A Case of IoT // IEEE Access. 2019. Vol. 7, Pp. 45705-45715.

8. Niemann H., Moehrle M. G., Frischkorn J, Use of a new patent text-mining and visualization method for identifying patenting patterns over time: Concept, method and test application // Technological Forecasting and Social Change. 2017. Vol. 115, Pp. 210–220.

9. Puccetti G,, Giordano V., Spada I., Chiarello F., Fantoni G., Technology identification from patent texts: A novel named entity recognition method // Technological Forecasting and Social Change. 2023. Vol. 186. Art. 122160

10. Shibata M., Ohtsuka Y., Takahashi M. and Okamoto K., "Advanced FPGA technology trend based on patent analysis with link mining," // 2018 International Conference on Electronics Packaging and iMAPS All Asia Conference (ICEP-IAAC), Mie, Japan, 2018, Pp. 147–151.

11. Souili A., Cavallucci D., Rousselot F., Natural Language Processing (NLP) – A Solution for Knowledge Extraction from Patent Unstructured Data // Procedia Engineering. 2015. Vol. 131. Pp. 635–643.

12. Trappey AJC, Liang C-P, Lin H-J. Using Machine Learning Language Models to Generate Innovation Knowledge Graphs for Patent Mining // Applied Sciences. 2022. Vol. 12. № 19. Art. 9818.

13. Villa A. M., Wirz M., A sequential patent search approach combining semantics and artificial intelligence to identify initial State-of-the-Art documents // World Patent Information. 2022. Vol. 68. Art. 102096.

14. Wang, B., Liu, S., Ding, K. et al. Identifying technological topics and institution-topic distribution probability for patent competitive intelligence analysis: a case study in LTE technology // Scientometrics. 2014. Vol. 101. Pp. 685–704.

М. Н. Чирагов,
руководитель направления цифрового права,
Общество с ограниченной ответственностью «ЛигалПикс»

АВТОМАТИЗАЦИЯ ЮРИДИЧЕСКОЙ ФУНКЦИИ (LEGALTECH) КАК СТИМУЛ РАЗВИТИЯ ПРАВА

Аннотация. В статье предпринята попытка дать определение LegalTech, обозначить ключевые направления и исследовать оказываемого эффекта на право. Проанализированы возможные способы использовании LegalTech в частном секторе. Выделены основной набор мотивации использовать LegalTech в бизнесе. Кроме того, рассмотрен запрос рынка на специалистов в сфере LegalTech и необходимые навыки, и знания для таких работников.

Ключевые слова: LegalTech, LawTech, LegalOps, технологии в праве, цифровизация, автоматизация юридической функции, оптимизация юридический процессов

AUTOMATION OF LEGAL FUNCTION (LEGALTECH) AS AN INCENTIVE FOR THE DEVELOPMENT OF LAW

Abstract. The article attempts to define LegalTech, identify key areas and explore the effect it has on the law. Possible ways to use LegalTech in the private sector are analyzed. The main set of motivations to use LegalTech in business are highlighted.

In addition, the market demand for specialists in the field of LegalTech and the necessary skills and knowledge for such workers were considered.

Keywords: LegalTech, LawTech, LegalOps, technology in law, digitalization, automation of legal functions, optimization of legal processes

Введение. С ноября 2022 года идет активное обсуждение GPT (Generative Pre-trained Transformer). Все больше упоминались специальностей, которые могут быть заменены благодаря GPT. Не стало исключением и юриспруденция. Более сдержанные позиционируют GPT в качестве еще одного инструмента для работы, другие всерьез дискутируют об угрозе для профессии юриста в его классическом виде.

Стоит заметить, что история подобных рассуждений не нова. Каждое появление новой технологии сопровождается поиском потенциально заменяемых функций. Что касается юриспруденции, таким примером может быть практически любой LegalTech продукт. Апогеем обсуждения в России стал юридический спор робота от Мегафон с Романом Бевзенко на полях ПМЮФ-2018 [1]. Победу в «сражении» одержал человек.

В 2019 году робот «Smartsettle ONE» за час решил арбитражный спор о недоплаченной сумме за консалтинговые услуги, которые стороны не могли уладить три месяца [2].

Развитие отечественной правовой информатизации в той или иной степени шло с 1975 года, ознаменовавшееся созданием Научного центра правовой информации (НЦПИ). Начало 90-х годов тесно связано не только с появлением справочно-правовых систем, но и формированием нормативно-правовой базы. К примеру, Указом Президента Российской Федерации от 28.06.93 № 966 [3] была утверждена Концепция правовой информатизации. Позже будет утверждена программа «Правовая информатизация органов государственной власти Российской Федерации» и разработка программ «Правовая информатизация органов исполнительной власти Российской Федерации» и «Правовая информатизация органов государственной власти субъектов Российской Федерации» [4]. Основной целью создаваемых программ была «цифровая кодификация».

Смещение акцента со справочных систем на продукты, способные анализировать большой массив данных и предлагать решение, активизировали обсуждение о возможности подмены юридической функции. Стали появляться сервисы, которые могли дать простой ответ на поставленный вопрос, формировали договоры, исковые заявления, анализировали правовую позицию и т. п. Однако существенным недостатком подобных сервисов все еще оставалась необходимость наличие юриста (в качестве субъекта, который точно формулирует, интерпретирует вопрос). Соответственно, речь идет об инструментах, которые должны облегчить работу. По некоторым данным, юрист в среднем тратит 23 % своего времени на рутинные задачи, а помощник юриста 69 % [5]. Представляется, что LegalTech-решения должны быть направлены на оптимизацию работы специалиста, освободить его от технической работы и позволить больше работать над вопросами права. То есть автоматизировать часть юридической функции.

Казалось, что к решению указанной задачи близко подобрался именно GPT, так как инструмент вселял надежду и одновременно пугал тем, что формировал ответ естественным языком. На очевидные ляпы в ответах апологеты сервиса просят закрыть глаза, так как машину необходимо обучить. На рис. приведен пример ответа GPT на поставленный автором вопрос.

Рис. Пример ответа GPT на поставленный автором вопрос о привлечении к субсидиарной ответственности

Чат-GPT не ответил на вопрос, но стоит отдать должное за профессионализм не отвечать на запросы, суть которых неизвестна.

В статье автором проанализированы основные инструменты автоматизации юридической функции и их влияние на развитие права.

Термин LegalTech. Термину LegalTech дано столько же уникальных определений, сколько статей на эту тему. Начиная от «технологий в праве», заканчивая позицией, когда LegalTech рассматривается как процесс. Отсутствие единого понимания приводит к неоднозначным выводам о перспективах развития LegalTech. Много внимания уделяется к LegalTech в понимании нового направления, а некоторые авторы и вовсе предлагают законодательно закрепить гарантиии соблюдения прав и свобод человека и гражданина в процессе использования решений LegalTech [6]. Не очень понятно, зачем дублировать фундаментальный конституционно-правовой принцип гарантий соблюдения прав и свобод человека и гражданина, а главное, на что это может повлиять с правовой точки зрения на LegalTech. Встречается мнение, что LegalTech подотрасль информационного права [7], с чем сложно согласиться. Причисление LegalTech к отрасли или подотрасли не имеет под собой методологического обоснования. В статье нет цели разобрать все LegalTech-решения. Основная цель – проанализировать влияние LegalTech на развитие права.

Автор не руководствуется позицией обязательного внедрения в частном секторе цифровых технологий, в каждом случае причины должны иметь экономическое обоснование и добровольный порядок. В качестве примера можно привести справочно-правовые системы (СПС). Если при выполнении юридической работы не использовать справочно-правовую систему, то качество и скорость работы

юриста будет хуже, чем у коллег, которые используют СПС. LegalTech направлен на повышение эффективности юридической функции, это его основная функция. Эффективность и автоматизация должны осуществляться путем внедрения технологий в юридическую функцию. Если речь о процессах (в том числе бизнес-процессы), об использовании новых подходов или кадровых решениях, то это не LegalTech. Задачи внутри юридической функции автоматизируются по мере возможностей технологий и развития законодательства.

Таким образом, по мнению автора LegalTech – это экономически обоснованные технологические решения/инструменты, направленные на повышение эффективности юридической функции. Подобное определение актуально в полной мере для B2C и B2B секторов. LegalTech в публично-правовой плоскости может иметь несколько иные цели и задачи.

Юридическая функция содержит в себе огромное количество задач. По мере автоматизации этих задач эффективность увеличивается. Страхи о полной автоматизации кажутся преждевременными, так как технологии пока лишь помогают юристу, но никак не угрожают ему. Этим мы обязаны специфике профессии и правоприменителю. Тенденция на автоматизацию ряда рутинных задач сохранится еще много лет.

LegalTech в России. В России LegalTech в классическом его смысле стартовал с появлением справочно-правовых систем. Правда вряд ли в этот момент кто-то называл LegalTech таким образом. Удовлетворялся запрос юристов на систематизацию и быстрый поиск среди массива нормативных и судебных актов.

В 2019 г. компания «Deloitte» опубликовала аналитику российского рынка юридических услуг и выделила четыре этапа развития LegalTech в России [8]:

– механизация, которая позволила конвертировать все документы в электронную форму;

– получение компаниями доступа к этой информации, организация ее эффективного хранения и передачи данных между сотрудниками;

– автоматизация компаниями рутинных процессов;

– работа компаний над внедрением расширенной аналитики, которая в том числе может влиять на решение судей. Речь об инструментах, позволяющих выявить закономерности в судебных актах и т. п.

Следует выделить еще один этап (пятый), а именно, взаимодействие с клиентами (пользователями). Подобные сервисы направлены на адаптацию коммуникации между профессиональным субъектом (юридическая компания или юрист) и пользователем, который не является специалистом в этой области. Базовым примером могут быть чат-боты (в том числе с подключением GPT), которые на первой линии могут консультировать клиента.

Позднее автоматизация коснулась административных процедур в части получения различных справок, выписок, совершения некоторых юридически значимых действий. Когда-то для регистрации гражданина в качестве индивидуального предпринимателя обращались к так называемым «юристам-регистраторам». Сейчас подобное встречается гораздо реже, так как процедура максимально упрощена и автоматизирована. В широком понимании юристы от этого процесса

работу не потеряли, разве только те, кто занимался исключительно регистрацией ИП. Однако рассматривать специалистов, которые занимаются лишь сопровождением базовых административных процедур (получение статуса ИП, заграничного паспорта и др.) юристами в полном смысле профессии нельзя.

С развитием блокчейна юристы все чаще стали встречать попытку использования этой технологии (начиная от смарт-контрактов, заканчивая NFT). Этим темам были посвящены множество конференций, где предлагалось проработать регулирование, выделить отрасль/подотрасль и т. п. Автор придерживается позиции, что нагромождение гражданско-правового регулирования под влиянием технического развития общества не приводит к развитию права. В подавляющем большинстве случаев действующее регулирование при должном толковании и применении подходит для «новых инструментов». О ненадобности плодить новые формы в праве, а адаптировать действующие нормы еще в начале прошлого века писал Г. Ф. Шершеневич [9].

Смарт-контракт – это оформление договора в форме программного кода в блокчейне для обеспечения последующего автоматического самоисполнения. Разного рода предложения выделить смарт-контракты в отдельный вид сделок необоснованны, так как речь о механизме, а не виде договора. В противном случае нам пришлось бы каждую сделку выделять в отдельный вид.

Схожая ситуация с NFT. В ГК РФ появилась ст. 141.1. о цифровых правах. Кажется, что существенных изменений в этой сфере не произошло.

Автоматизация юридических процессов позволяет более точно и последовательно применять законы. Аналитика данных и ИИ могут помочь выявить законодательные пробелы и несоответствия в судебных решениях, что способствует улучшению качества правоприменения. Это также может снизить вероятность произвольных решений судей.

Актуальность LegalTech-решений. По данным Гартнер, к 2024 году юридические отделы автоматизируют 50 % юридической работы [10]. Подобные прогнозы кажутся, мягко говоря, смелыми. При этом, по мнению компании McKinsey, 23 % из общего объема работы среднестатистического юриста можно автоматизировать существующими технологиям [11]. Даже на уровне стажера или помощника юриста большинство задач на сегодняшний день не автоматизировано. Для подтверждения этого утверждения возможно посетить почтовую службу своего города в поздний час.

Схожая ситуация и с конструкторами договоров. Юристы в РФ редко пользуются подобными сервисами, так как у каждой компании/отдела есть свои наработки по договорам. Своеобразная база знаний.

Возникновение огромного количества LegalTech продуктов, которые не востребованы, может быть связано со слабым изучением рынка и целевой аудитории. Стороннему наблюдателю без опыта в юридической сфере какой-то инструмент может показаться весьма востребованным, однако для юристов ненужным. Юридическим компаням актуальны системные решения, которые позволяют фиксировать задачи и часы, контролировать их выполнение, предоставлять функции по совместной и удаленной работе и т. п.

Современные решения в LegalTech связаны с вспомогательными продуктами в работе юриста. Перспектива направлена на внедрение искусственного интеллекта (ИИ). Однако и в этом случае о подмене юридической функции рано говорить. ИИ внедрен в системы автопилота, но мы только стали подступать к беспилотным автомобилям на улицах. Сферы, где есть риски, доверять технологиям сложно, а юридическая функция требует еще мышления и креатива, что характерно только для человека (пока). LegalTech пока не способен производить разнообразную юридическую работу, если она сопряжена с проявлением творческого характера. Автоматизированное создание какого-либо документа результат лишь компоновки информации. Наглядно веру в сверхспособности технологий (на примере чат-ботов) разобрал в своей статье Балдур Бьярнарсон [12]. Он отмечает, люди, скептически настроенные к чат-ботам, менее склонны их использовать. Те, кто убежден в ограниченности их возможностей, не поддаются ажиотажу. Кроме того, ответы чат-бота выглядят крайне релевантными в том контексте, в котором пользователь их задает, но на самом деле они статистически универсальны. Математическая модель, стоящая за чат-ботом, просто предоставляет статистически вероятный, на основе анализа обучающей выборки текстов, ответ на вопрос. Чрезмерный оптимизм поддается проверке своей ситуацией. Окажет ли предпочтение гражданин в решении важного для себя вопроса сервису или предпочтет профессионального юриста? Все зависит от степени риска. При регистрации ИП через приложение гражданин ничего не теряет, а если речь о многомиллионном споре, то вероятно предпочтение будет отдаваться юристу.

Важно, что с появлением технологических решений накапливается большой массив конфиденциальных данных, которые необходимо охранять. В России в последние годы планомерно дополняется нормативная база в части охраны персональных данных. Несмотря на это, ежемесячно появляется информация об очередной утечке, что актуально практически для всех стран. Однако и это не позволяет сделать вывод о том, что автоматизация порождает дополнительные правовые проблемы. Речь скорее о смещении юридических акцентов.

Специалисты в области LegalTech. Возникновение большого количества LegalTech продуктов на рынке привело к появлению универсального специалиста в области LegalTech (LegalTech-аналитика, LegalTech-консультант, CLOO – Chief Legal Operations Officer). Предполагается, что такие специалисты должны обладать знаниями в области [13]:

– программирования на каком-либо из высокоуровневых языков (к примеру, Python);

– клиент-серверного взаимодействия, включая принцип работы API (application programming interface);

– существующих семейств программных продуктов для бизнеса (1С, SAP);

– осведомленность о публичных API, предоставляющих данные о судебных делах, о деятельности органов государственной власти;

– распространенных офисных программ (форматы сохранения данных в них, макросы);

– процесса создания ПО (стадии постановки задачи, разработки кода-ревью, тестирования, развертывания на целевой инфраструктуре).

– теории права (фундаментальные различия между отраслями права, структура правовых норм, иерархия нормативных правовых актов);

– общее понимание отрасли права, в рамках которой осуществляется автоматизация;

– основных договоров (договор возмездного оказания услуг, лицензионный договор), на основе которых осуществляется передача прав на LegalTech-продукты.

Отечественная образовательная система пока не готовит специалистов, которые обладали бы всеми указанными навыками и знаниями. Обучение проводится в рамках курсов или самостоятельно за счет междисциплинарного подхода. При этом LegalTech-специалист не обязательно должен уметь в полной мере программировать или обладать другими техническими навыками на уровне самостоятельной работы. Важно понимание принципов и функционала, чтобы иметь возможность видеть возможные технические решения юридических задач и уметь управлять командой, состоящей из разных специалистов.

Влияние LegalTech на право. LegalTech призван способствовать упрощению и оптимизации коммуникации субъектов гражданско-правовых отношений, создавая необходимые условия для развития новых отношений в товарообороте и определяя перспективные направления развития законодательства.

Глобально у нас выбор есть выбор между опережающим регулированием и догоняющем. У каждого подхода существуют свои положительные и негативные последствия. Однако «право должно быть относительно стабильно, поэтому задача юридической науки заключается не только в выявлении уже происшедших существенных изменений в опосредуемых правом отношениях, но и в прогнозировании грядущих изменений с тем, чтобы сводить до минимума промежутки неизбежного «расхождения» между стабильной системой правовых норм и развивающимися общественными отношениями – лишь на такой основе правовое регулирование в наибольшей степени можно приблизить к оптимальному» [14]. Соответственно, чем лучше организована правовая основа, тем меньше дополнительного регулирования потребуется в будущем.

Право не должно подменяться техническими требованиями и руководствоваться только технологическими вызовами [15]. Необходимо соблюдать принцип максимальной адаптации и интерпретации действующего законодательства. Дополнительное регулирование должно быть нацелено на устранение пробелов.

Появление нового цифрового юридического языка будет способствовать дебюрократизации правотворческого процесса. На сегодняшний день LegalTech больше развит в публичном секторе. Пока только крупный бизнес имеет возможность выделять большой бюджет на развитие LegalTech в организации. Подобную ситуацию нельзя охарактеризовать с негативной оценкой, так как бизнес всегда исходит из целесообразности применения тех или иных инструментов. К примеру, практически все юридические компании, департаменты и юристы используют СПС. Они понимают выгоду и необходимость этого решения. Другой подход, например, к конструкторам договоров. В каждом конкретном

случае необходимо необходимо обосновывать рентабельность использования инструмента/решения.

Развитие LegalTech имеет два основных эффекта на право. Во-первых, способствует снижению правового нигилизма в обществе. Происходит это не только за счет повышения доступности правовой помощи для населения, но и благодаря формированию определенного поведения. Если граждане будут использовать правовые методы решения для небольших споров, то и в более сложных делах сохранится паттерн использовать юридические механизмы. Для юристов это благоприятная тенденция, так как количество обращающихся к профессионалам существенно вырастет. Решение же рутинных и административных задач нельзя в полной мере отнести к юридической функции. Подобные действия далеко не всегда требуют специального знания, что порождает возникновение на рынке «специалистов», у которых есть опыт конкретного действия, но к юридическому сообществу отношения не имеют. Таким образом, автоматизация рутинных задач слабо влияет на рынок профессиональных юристов. Тезис о том, что «распространение искусственного интеллекта способствует замене юристов-профессионалов роботами в некоторых рутинных процессах» [15] верен лишь в части рутинных процессов.

Теоретически, использование LegalTech может несколько снизить цены на юридические услуги и сократить часы, так как юрист будет меньше времени затрачивает на решение определенных задач.

Во-вторых, юридическая функция сместит акцент на работу над правовыми задачами. Деятельность юриста в меньшей степени будет связана с административными и тривиальными вопросами (в большей степени они будут автоматизированы), что хорошо для профессии и права. По результатам опросов [16], юристы тратят более 34 % рабочего времени на технические задачи, что сказывается на эффективности и цене услуг.

Заключение. В последние годы LegalTech активно обсуждается в академической среде, публикуются материалы и монографии. Этот процесс закономерен и позитивно отражается на развитии направления в России. Однако отсутствует консенсус в части определения, как следствие, понимания LegalTech. Анализ литературы на данную тему позволяет сделать вывод о том, что большинство авторов склонны причислять к LegalTech все что связано с цифровизацией (цифрой) и технологиями. Кроме того, акцент на создании специального регулирования, который решит все существующие барьеры кажется ошибочным. В первую очередь LegalTech это инструмент и помощник юриста. Инструмент, который высвобождает для специалиста драгоценное время для решения правовых задач. Бизнес же получает снижение издержек и повышение эффективности. Доступность юридической помощи позитивно скажется на правосознании граждан, что выгодно для всего юридического сообщества.

Список литературы

1. Указ Президента РФ от 28.06.1993 № 966 «О Концепции правовой информатизации России» // СПС КонсультантПлюс.

2. Указ Президента РФ от 04.08.1995 № 808 «О президентских программах по правовой информатизации» // СПС КонсультантПлюс.

3. Информационно-технологическое обеспечение юридической деятельности (LegalTech): учебник. М.: Проспект, 2022.

4. Мамиофа И. Э. Охрана изобретений и технический прогресс. М., 1974.

5. Синицын С. А. Российское и зарубежное гражданское право в условиях роботизации и цифровизации. Опыт междисциплинарного и отраслевого исследования: монография. М.: Инфотропик Медиа, 2021.

6. Шершеневич Г. Ф. Курс торгового права. М., 2003. Т. II.

7. Савенко Н. Е. Legaltech в цифровой экономике и правовом регулировании экономической деятельности граждан // Право. Журнал Высшей школы экономики. 2023. № 1.

8. Еремеев С. Г., Майоров А. В., Минченков Е. Н. О юридическом концепте направления legaltech: перспективы становления и развития // Теория и история государства и права. 2019. № 4. С. 9-17.

9. Юридический баттл: робот от МегаФон vs Роман Бевзенко. URL: https://pravo.ru/lf/story/202675

10. Settlement of legal dispute using B.C.-produced robot mediator called first ever. URL: https://www.law360.ca/articles/11621/settlement-of-legal-dispute-using-b-c-produced-robot-mediator-called-first-ever

11. День юриста: нет роботам, да работе. URL: https://zakon.ru/blog/2017/12/03/den_yurista_net_robotam_da_rabote

12. Опрос юристов в СНГ. URL: https://clck.ru/35dUfd

13. The LLMentalist Effect: how chat-based Large Language Models replicate the mechanisms of a psychic's con. URL: https://softwarecrisis.dev/letters/llmentalist

14. 5 Legal Technology Trends Changing In-House Legal Departments. URL: https://www.gartner.com/smarterwithgartner/5-legal-technology-trends-changing-in-house-legaldepartments%3D

15. Harnessing automation for a future that works. URL: https://www.mckinsey.com/featured-insights/digital-disruption/harnessing-automation-for-a-future-that-works

16. Russian legal services market. Coaxing progress from uncertainty. URL: https://www2.deloitte.com/content/dam/insights/us/articles/22565_russian-legal-services-market-/DI_Russian-legal-services-market.pdf

А. Ю. Чурикова,
кандидат юридических наук, доцент,
Саратовская государственная юридическая академия

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В УГОЛОВНОМ ПРОЦЕССЕ: ВЗГЛЯД УЧЕНЫХ И ПРАКТИКОВ НА ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Аннотация. Цифровые технологии и программы искусственного интеллекта давно стали частью повседневной жизни, но уровень владения данными технологиями пользователей остается крайне низким. В сфере уголовного судопроизводства,

где решаются вопросы об уголовной ответственности, особенно важно взвешенное принятие решения о возможности использования искусственного интеллекта. Этим обуславливается необходимость исследования мнений представителей науки и практики. В целях выявления и сравнения представлений ученых и правоприменителей о проблемах и перспективах использования искусственного интеллекта в уголовном судопроизводстве было проведено социологическое исследование методом поперечных срезов с использованием анкетирования. В результате исследования у прокуроров, следователей и дознавателей было выявлено негативно-настороженное отношение к внедрению технологий искусственного интеллекта в уголовный процесс. На основе проведенного анализа выявлен ряд проблем, препятствующих использованию технологий искусственного интеллекта в уголовном судопроизводстве. Также выделено семь основных направлений перспективного применения искусственного интеллекта при производстве по уголовному делу: принятие и поддержка в принятии процессуальных решений, прогнозирование, контроль сроков, помощь в доказывании, моделирование ситуаций, интеллектуальное распознавание речи.

Ключевые слова: уголовное судопроизводство, цифровая трансформация, системы поддержки принятия решений, искусственный интеллект, проблемы внедрения цифровых технологий, уголовное дело

ARTIFICIAL INTELLIGENCE IN CRIMINAL PROCEDURE: SCIENTISTS' AND PRACTITIONERS' VIEWS ON PROBLEMS AND PROSPECTS

Abstract. Digital technologies and artificial intelligence programmes have long been part of everyday life, but the level of user proficiency in these technologies remains very low. In criminal proceedings, where issues of criminal liability are decided, it is particularly important to make a balanced decision on the possibility of using artificial intelligence. This necessitates a study of the views of academics and practitioners. In order to identify and compare the perceptions of scientists and law enforcers about the problems and prospects of using artificial intelligence in criminal proceedings, a sociological study was conducted by cross-sectional method using questionnaires. As a result of the study, a negative and cautious attitude towards the introduction of artificial intelligence technologies in criminal proceedings was revealed among prosecutors, investigators and inquirers. Based on the analysis, a number of problems hindering the use of artificial intelligence technologies in criminal proceedings were identified. Seven main directions of prospective application of artificial intelligence in criminal proceedings were also identified: adoption and support in making procedural decisions, forecasting, control of deadlines, assistance in proving, modelling of situations, intellectual speech recognition.

Keywords: criminal procedure, digital transformation, decision support systems, artificial intelligence, problems of digital technology implementation, criminal case

Введение. Стремительная и повсеместная компьютеризация и доступность компьютерных технологий дали новый толчок для развития и применения математического моделирования в юриспруденции. В качестве одного из наиболее

перспективных направлений цифровой трансформации правоохранительной деятельности и правосудия в науке активно обсуждается возможность использования искусственного интеллекта (далее – ИИ) в сфере уголовного судопроизводства [1. С. 43–44; 2. С. 89–91; 3. С. 217–220; 4]. Для большинства технологически развитых государств решение вопросов, связанных с внедрением систем на базе ИИ в уголовный процесс, представляется приоритетным [5. С. 482–484; 6. С. 205–206; 7].

В связи с этим разработка обоснованного правового регулирования использования программ искусственного интеллекта является одним из наиболее перспективных направлений правовых исследований. При этом лица, занимающиеся подобными исследованиями, как правило, являются специалистами в области юриспруденции и не всегда объективно представляют уровень развития современного ИИ, ограничения и особенности, связанные с обучением программ ИИ, а также потребности правоприменителей, которые могли бы быть удовлетворены при использовании технологий ИИ в уголовно процессе.

При решении вопроса о возможности использования ИИ в уголовном судопроизводстве возникает необходимость определения рамок оптимизации и автоматизации процессов, истинных ожиданий и потребностей правоприменителей. Ученые порой выражают желание, чтобы программы ИИ принимали решения по уголовному делу, очеловечивая при этом ИИ [8. С. 217–218; 9. С. 210–211], либо, напротив, настороженно относятся к возможности использования ИИ в уголовном процессе, предлагая ввести ограничения на применение данных программ [10. С. 105–106; 11. С. 758–759]. Ученые задают основные тенденции по внедрению ИИ в уголовное судопроизводство, предлагая различные варианты применения данных программ. Между тем, именно суды, прокуроры, органы расследования являются основными субъектами реализации любых направлений цифровой трансформации в области уголовного судопроизводства и от их отношения, ожиданий и принятия происходящих преобразований зависит в первую очередь эффективность применения любых технологических новшеств. С. Ю. Чуча обоснованно указывает, что условием внедрения в правосудие искусственного интеллекта является доверие сторон и суда [12. С. 116, 120]. Поэтому крайне важно анализировать и учитывать мнение участников уголовного судопроизводства при внедрении и использовании цифровых технологий.

Таким образом, особую актуальность приобретает исследование и сопоставление мнения ученых и практиков в сфере уголовного процесса относительно их отношения к возможностям и перспективам использования программ ИИ.

Методы исследования. В целях выявления и сравнения представлений ученых и правоприменителей о проблемах и возможностях использования ИИ в уголовно-процессуальной деятельности было проведено социологическое исследование методом поперечных срезов путем анкетирования следующих групп респондентов: прокуроры, сотрудники органов расследования (следователи и дознаватели), адвокаты, работающие по уголовным делам и ученые, научные интересы которых лежат в сфере уголовного процесса. В рамках проведенного социологического исследования задавался вопрос: «Какие, на Ваш взгляд, существуют

перспективы использования программ искусственного интеллекта в уголовном процессе?» разным группам респондентов (практиками и ученым в сфере уголовного судопроизводства). Данный вопрос был открытым (предполагал написание краткого или развернутого ответа), что было сделано намеренно, чтобы оценить реальное отношение респондентов к применению ИИ в уголовном процессе. Развернутые ответы были получены от 69 сотрудников органов прокуратуры, 34 следователей и дознавателей, 38 адвокатов-защитников и 86 ученых-процессуалистов. Кроме того, перед респондентами также ставился вопрос: «Как вы относитесь к цифровизации уголовного процесса?», на который можно было ответить «положительно», «отрицательно», «нейтрально», либо написать свой развернутый ответ. На данный вопрос дали ответ 61 прокурор, 43 следователя и дознавателя, 33 адвоката и 81 ученый.

Анкетирование проводилось на территории Российской Федерации в период с сентября 2022 года по апрель 2023 года, преимущественно с использованием гугл-форм. Распространение анкет происходило путем рассылки приглашения для заполнения анкет в гугл-формах на официальные e-mail-адреса, а также путем личного вручения анкет на бумажных носителях.

Обработка и анализ полученных данных проходили в несколько этапов. Во-первых, по первому вопросу о перспективах использования ИИ в каждой группе респондентов все полученные ответы систематизировались и обобщались в группы по схожей смысловой нагрузке:

– положительные (например, к ним были отнесены такие ответы респондентов, как: «облегчение работы», «помощь», «большие», «положительные», «улучшение качества уголовного процесса», «может быть они смогут разгрузить нас в заполнении бумаг» и т. д.). К этой группе были отнесены ответы, не имеющие конкретных предложений, но выражающие надежду и положительные ожидания;

– неопределенные (например: «маловероятно», «неизвестно», «сомнительно», «слабые», «неясные», «это неизбежное будущее», «второстепенные», «разные, в зависимости от уровня их внедрения», «не разбираюсь», «затрудняюсь ответить» и т. д.). К этой группе были отнесены ответы, в которых респонденты затруднялись определить свое точное отношение к использованию программ ИИ в уголовном процессе;

– негативные (например: «никаких», «сведено к нулю», «надеюсь, нет», «невозможно», «бесперспективно», «отсутствуют», «перспективы связаны с ошибками и хаосом» и т. д.). К данной группе были отнесены ответы, в которых выражалось неприятие или негативные ожидания от применения программ ИИ в уголовном судопроизводстве;

– конкретные решения (например: «помощь при отслеживании сроков», «анализ доказательств», «помощь при изучении дел», «при прогнозировании содержания будущего судебного решения», «принятие не ключевых процессуальных решений», «отслеживание сроков» и т. д.). К этой группе были отнесены ответы, содержащие конкретные предположения и предложения об использовании программ ИИ при расследовании и рассмотрении уголовных дел.

Ответы были разделены по видам для каждой группы респондентов отдельно, чтобы провести соотношение мнений респондентов относительно перспектив использования программ искусственного интеллекта в уголовном судопроизводстве. После чего сопоставлялись и анализировались обобщенные данные между группами респондентов с целью выявления отношения к применению ИИ в уголовном процессе и сопоставления выявленных тенденций по группам. Ответы на второй вопрос сопоставлялись с полученными данными по первому вопросу с целью выявления корреляций.

На втором этапе детально анализировались ответы респондентов с конкретными направлениями/предложениями/ожиданиями по использованию ИИ в уголовном процессе. Таким образом, выявлялись основные представления о перспективах использования ИИ по отдельным группам респондентов, после чего полученные результаты сопоставлялись между собой с целью опровержения, либо подтверждения гипотезы о существовании значительного расхождения между представлениями ученых и практиков о перспективах применения ИИ в уголовном процессе.

Результаты исследования. 1. Распределение и формирование мнений заинтересованных субъектов о перспективах применения программ ИИ в уголовном процессе. Человеческий мозг обладает рядом уникальных качеств, которые играют далеко не последнюю роль в объективном рассмотрении уголовного дела. На значимость эмоций в процессе принятия решения судьями указывает П. М. Морхат, выделяя важность не только формального знания права, но еще и определенного уровня когнитивной и эмоциональной компетенции [13. С. 45–46].

Когнитивно-эмоциональные навыки профессиональных участников уголовного процесса, безусловно, имеют большое значение для принятия законных, обоснованных и справедливых решений по делу. Однако не стоит забывать, что искусственный интеллект – это самообучающаяся программа, направленная на поиск решения без заранее заданного алгоритма. Наибольшую сложность представляет именно процесс обучения искусственного интеллекта.

Например, в сфере судопроизводства для обучения соответствующей программы искусственного интеллекта необходимо, чтобы данной программой был проанализирован значительный объем принимаемых по различным делам решений. Однако никто не застрахован от ошибок правоприменителей, допускаемых ими при принятии решений. Эти ошибки при их систематическом характере будут накапливаться и имитироваться программами искусственного интеллекта. Обучение же программы искусственного интеллекта в «идеальных условиях» также может привести к возникновению в дальнейшем ошибок, связанных с невозможностью принятия и прогнозирования такими программами решений в реальной жизненной ситуации.

Эта особенность обучения программ искусственного интеллекта обуславливает потребность в высококвалифицированных кадрах, понимающих основы работы подобного рода программ, а также в продуманной и научно обоснованной программе обучения искусственного интеллекта.

Таким образом, кадровый вопрос становится одним из решающих при внедрении программ искусственного интеллекта в практическую деятельность правоохранительных органов. Мнение правоприменителей о программах искусственного интеллекта, их ожидания от применения данных программ могут существенно повлиять на фактическую реализацию любой реформы.

Для определения соотношения мнений по группам респондентов (прокуроры, следователи, адвокаты-защитники и ученые-процессуалисты) подсчет мнений определенного вида осуществлялся в процентном соотношении относительно числа ответивших в конкретной группе. Полученные результаты представлены на графике, отражающем распределения мнений респондентов (рис. 1).

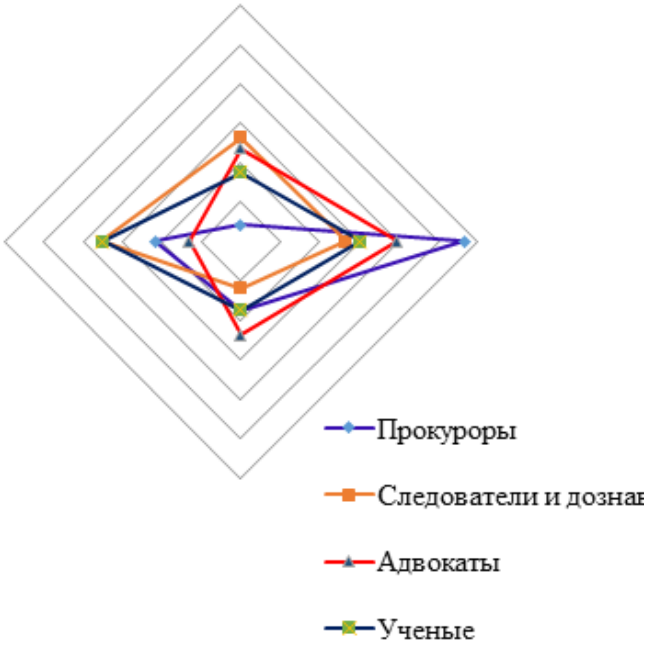

Рис. 1. Схема соотношения мнений респондентов о перспективах применения программ искусственного интеллекта в уголовном судопроизводстве

На графике наглядно продемонстрировано имеющееся у практиков и ученых представление о перспективах применения программ ИИ в уголовном процессе. Так, среди прокуроров было получено наименьшее число ответов, свидетельствующих о положительном восприятии перспектив применения ИИ в уголовном процессе (всего 4,3 % от числа опрошенных прокуроров), в то время как негативных оценок использования ИИ от прокуроров поступило почти в 4 раза больше – 17,4 %. Большинство ответивших сотрудников прокуратуры (56,5 %) выразило неопределенное отношение к применению ИИ в уголовном процессе, либо предложило конкретные решения (21,7 %), что свидетельствует в целом о хоть и настороженном, но не резко-негативном отношении со стороны прокуроров к внедрению технологий ИИ в правоприменение. При сравнении распределения ответов сотрудников органов прокуратуры с распределением ответов у других групп респондентов видно, что только у прокуроров негативных ответов больше, чем положительных и самый большой процент неопределенных

ответов. Прокуроры первые из опрошенных субъектов уголовного процесса реализуют программу цифровой трансформации [14], такое распределение ответов может свидетельствовать о наличии сложностей и проблем при реализации данной программы.

В целом, у остальных групп респондентов мы видим баланс между числом негативных и положительных мнений, а также довольно большое количество ответов у всех участников опроса, свидетельствующее о их неопределенном отношении к использованию программ ИИ в уголовном судопроизводстве.

Полученные ответы по перспективам применения ИИ коррелируют с данными, полученными в результате ответа респондентов на вопрос о их отношении к цифровизации уголовного процесса (рис. 2).

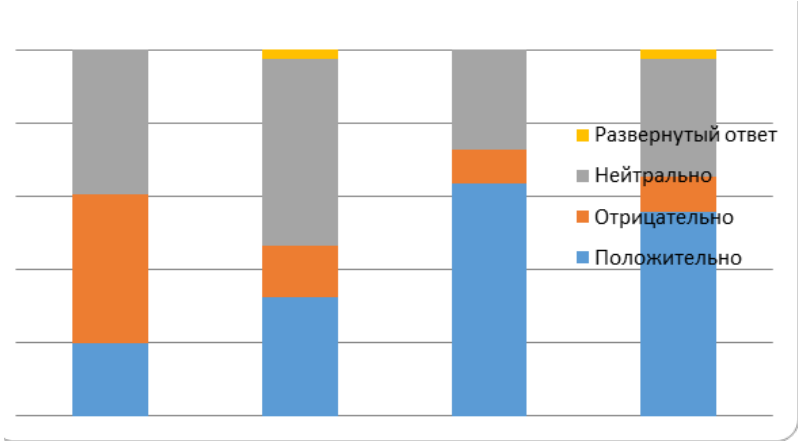

Рис. 2. Распределение ответов респондентов на вопрос «Как вы относитесь к цифровизации уголовного процесса?»

Из представленной на рис. 2 диаграммы видно, что прокуроры относятся к цифровизации в большей степени отрицательно, следователи и дознаватели в основном нейтрально, а адвокаты и ученые в большинстве положительно. Однако именно органы прокуратуры и расследования будут непосредственно применять цифровые технологии, а выявленное у данных групп респондентов негативно-настороженное отношение к внедрению новых технологий в уголовный процесс может существенно повлиять на реализацию процесса цифровой трансформации уголовного судопроизводства. Не желая применять новые технологии, правоприменители всегда смогут найти схемы «обхода». Поэтому важно обнаружить причины для формирования такого отношения и устранить их.

Распространенная среди респондентов негативная оценка перспектив применения ИИ в уголовном процессе, на наш взгляд, связана с целым рядом проблем внедрения технологий ИИ, а также некомпетентностью в вопросах основ работы программ искусственного интеллекта, что вызывает либо опасения в его применении, либо абстрактно-завышенные ожидания.

На наш взгляд, можно выделить следующие основные существующие и возможные проблемы внедрения технологий ИИ:

– неравномерный уровень технического оснащения;

– современный уровень технического развития (ИИ находится на начальном этапе развития и пока эти технологии весьма несовершенны);

– проблемы обучения программ ИИ;

– систематические изменения законодательства (ИИ обучается на примерах и изменение законодательства делает затруднительным применение знаний, так как используемые для обучения примеры будут иметь в основе своего принятия устаревшую законодательную базу);

– уровень квалификации сотрудников, занимающихся уголовно-процессуальной деятельностью, в сфере IT-технологий.

В связи с этим считаем целесообразным проводить систематическое обучение среди сотрудников, осуществляющих уголовно-процессуальную деятельность, повышая тем самым уровень их технических знаний. Кроме того, негативное отношение правоприменителей к цифровой трансформации и программам ИИ часто складывается из-за увеличения и без того высокой нагрузки на сотрудников правоохранительных органов, прокуратуры и суда. Прежде чем полноценно перейти к цифровому формату в уголовном судопроизводстве, им приходится дублировать информацию и действия, внося информацию в различные базы данных, а также создавая документы и на электронных, и на бумажных носителях. Поэтому требуется продуманный подход по внедрению новых технологий, который позволит исключить увеличение нагрузки.

2. Соотношение мнений ученых и правоприменителей по способам использования ИИ в уголовном процессе. Проходя анкетирование, 30 ученых-процессуалистов и 32 практических работника (прокуроры – 15, следователи – 10, дознаватели – 2, адвокаты – 5) написали свои конкретные предложения и представления по использованию программ ИИ в уголовном судопроизводстве. Все мнения по конкретным направлениям перспективного применения ИИ можно разделить на шесть основных групп:

Принятие процессуальных решений (такое мнение выразили 10 % ученых, при этом 66,7 % из них указали, что перспективным является принятие ИИ не ключевых решений по делу);

Поддержка принятия решений (такие ответы были даны 20 % ученых, при этом большинство из них (83,3 %) указали на то, что основным направлением внедрения ИИ в уголовном процессе должно стать создание системы поддержки принятия решений, также указывалось на помощь в принятии решений путем составления их проектов);

Прогнозирование принятия решений (так считают еще 20 % ученых);

Контроль сроков (данное направление считают наиболее перспективным 16,7 % ученых и 25 % (от общего количества) практиков);

Помощь в доказывании (анализ, обработка, собирание и сопоставление информации по делу, работа с большими данными, Быстрая обработка информации из различных информационных систем (видеокамеры, реестры, базы данных), оценка имущества для ареста или залога и т. д.). Мнения о том, что данное направление является наиболее перспективным придерживается 26,7 % ученых и 68,7 % практических работников;

Моделирование различных следственных ситуаций, поведения преступника и т. д. (23,3 % ученых и 6,3 % правоприменителей).

При этом ни в одном из предложений, высказанных практиками, не рассматривается в качестве перспективного направления возможность принятия или прогнозирования программами ИИ решений в уголовном судопроизводстве. Более того, двое из респондентов-правоприменителей (следователь и прокурор) в своих ответах прямо указали на то, что не видят перспектив в принятии решений программами ИИ, либо при помощи данных программ, но считают перспективным использование программ ИИ для собирания и сопоставления информации (доказательств). В свою очередь, из 30 ученых, написавших конкретные решения по использованию программ ИИ в уголовном процессе, 15 (половина) высказались за принятие, прогнозирование или помощь в принятии программами ИИ решений в уголовном судопроизводстве.

Полученные данные свидетельствуют о существенном расхождении представлений ученых и правоприменителей о перспективных направлениях использования ИИ в уголовном судопроизводстве. Практики ориентированы в первую очередь на решение прагматических задач, а также улучшение качества правоприменения за счет снижения рутинной нагрузки, в то время как ученые рассматривают программы ИИ как возможных «беспристрастных арбитров». Полагаем, что данный факт имеет значение для проведения дальнейших исследований возможностей использования ИИ в уголовном процессе, так как негативное отношение правоприменителей к принятию решений программами ИИ может сказаться и на возможности внедрения систем поддержки принятия решений.

Стоит обратить внимание на то, что никто из респондентов не назвал в качестве перспективного направления применение интеллектуального распознавания речи. ИИ уже сейчас в бытовых нуждах повсеместно применяется для преобразования речи в текст (модули распознавания речи Google, Яндекс, ИИ «Алиса», «Маруся» и т. п.). Имеется позитивный опыт Применения ИИ для составления протоколов как в досудебном, так и в судебном производстве по уголовным делам в Китае [15; 16]. Эта функция ИИ может существенно облегчить труд правоприменителей. Не надо будет больше тратить значительный объем времени для составления процессуальных документов (достаточно будет проговаривать вслух необходимые сведения), а также не надо будет вручную заносить сведения в базы данных. Полагаем, что данное направление развития и применения ИИ также можно отнести к одному из наиболее перспективных в уголовном судопроизводстве.

Выводы. Таким образом, в результате проведенного исследования было выявлено настороженно-негативное отношение прокуроров, следователей и дознавателей к цифровизации уголовного судопроизводства, а также неопределенность, несформированность мнений правоприменителей в отношении использования программ ИИ в уголовном процессе.

Несмотря на массовое распространение цифровых технологий, уровень владения данными технологиями пользователей остается крайне низким. Уровнем квалификации сотрудников, особенно руководящего состава, могут быть обусловлены системные провалы при переходе с бумажных носителей к электронному уголовному делу, а также проблемы с использованием технологий ИИ в уголовном

процессе. Лица, не понимающие принципов работы цифровых технологий, а также не желающие разбираться в программном обеспечении, могут требовать дублирования информации на бумажных носителях. Устранить данную проблему возможно путем обязательного, систематического прохождения повышения квалификации в сфере информационно-телекоммуникационных технологий сотрудниками органов расследования, прокуратуры и суда.

Создание правового регулирования, направленного на внедрение цифровых технологий, в том числе и ИИ, должно осуществляться с учетом проблем правоприменения, существующих в настоящее время. От решения этих проблем зависит уровень прозрачности и открытости уголовного судопроизводства, его законность и обоснованность, соблюдение сроков расследования и рассмотрения дела.

В ходе исследования была подтверждена гипотеза о существовании значительного расхождения между представлениями ученых и практиков о перспективах применения ИИ в уголовном процессе. Практические работники видят применение технологий ИИ в направлениях, которые способны облегчить их техническую, рутинную работу, никто из опрошенных практиков не видит перспектив в принятии или прогнозировании программами ИИ решений в уголовном процессе, в то время как среди ученых такое представление об использовании ИИ в уголовном судопроизводстве является распространенным.

Данные, полученные в ходе исследования, в том числе и об основных направлениях применения программ ИИ в уголовном судопроизводстве, позволяют по-новому взглянуть на проблемы цифровой трансформации уголовного судопроизводства, а также определить приоритетные для правоприменения направления развития программ ИИ в сфере уголовного судопроизводства.

Список литературы

1. Baltrūnienė B. Place of artificial intelligence in the detection and investigation of crime: the present state and future perspectives // Problemy Współczesnej Kryminalistyki. 2022. Vol. 26. Pp. 43–58.

2. Хатов Э. Б. Цифровой помощник или цифровой прокурор? // Российский журнал правовых исследований. 2023. Т. 10, № 1. С. 87–92.

3. Custers B. AI in Criminal Law: an overview of AI applications in substantive and procedural Criminal Law // Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice. 2022. Pp. 205–223.

4. Roksandić S., Protrka N., Engelhart M. Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand? // 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO). IEEE, 2022. Pp. 1225–1232.

5. Governatori G., Bench-Capon T., Verheij B. et al. Thirty years of Artificial Intelligence and Law: the first decade //Artificial Intelligence and Law. 2022. Vol. 30. №. 4. Pp. 481–519.

6. Федорович В. Ю., Химичева О. В., Андреев А. В. Внедрение технологий информатизации и искусственного интеллекта как перспективные направления развития современного уголовного судопроизводства // Вестник Московского университета МВД России. 2021. №. 2. С. 205–210.

7. Об искусственном интеллекте в уголовном праве и его использовании полицией и судебными органами в уголовных делах: Резолюция Европейского парламента от 6 октября 2021 г. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

8. Поляков С. Б. Наше мнение: только искусственный интеллект принудит судью к справедливости // Вестник Московского университета МВД России. 2021. №. 3. С. 213-218.

9. Колоколов Н. А. Искусственный интеллект в правосудии – будущее неотвратимо // Вестник Московского университета МВД России. 2021. № 3. С. 201–212.

10. Цветков Ю. А. Искусственный интеллект в правосудии // Закон. 2021. № 4. С. 91–107.

11. Миронова Е. Ю. Достижение назначения уголовного судопроизводства в условиях цифровизации общества: анализ российского и зарубежного опыта // Всероссийский криминологический журнал. 2022. Т. 16, № 6. С. 754–767.

12. Чуча С. Ю. Искусственный интеллект в правосудии: юридико-психологические аспекты правоприменения // Правоприменение. 2023. Т. 7, № 2. С. 116–124.

13. Мохат П. М. Применение искусственного интеллекта в судопроизводстве // Право и цифровая экономика. 2019. № 1. С. 44–47.

14. Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года: Приказ Генеральной прокуратуры Российской Федерации № 627 от 14.09.2017 г. URL: https://epp.genproc.gov.ru/web/gprf/expert_advice/events?item=5094989

15. Wang R. Legal technology in contemporary USA and China // Computer Law & Security Review. 2020. Vol. 39. Art. 105459.

16. Guo M. Internet court's challenges and future in China // Computer Law & Security Review. 2021. Vol. 40. Art. 105522.

А. Ю. Чурилов,
кандидат юридических наук,
Томский государственный университет

К ВОПРОСУ О ВОЗМОЖНОСТИ ОБОРОТА ИНТЕЛЛЕКТУАЛЬНЫХ ПРАВ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН

Аннотация. Применение новых технологий, включая блокчейн и NFT, может стать инструментом для обеспечения защиты прав и законных интересов правообладателей и стимулирования инноваций в различных сферах. В работе рассматриваются две правовые проблемы, связанные с депонированием и оборотом результатов интеллектуальной деятельности, в том числе объектов авторского права. Первая проблема заключается в возможности использования технологии блокчейн для депонирования таких объектов. Вторая проблема заключается в обороте прав на депонированные объекты.

Ключевые слова: исключительное право, NFT, блокчейн, депонирование, договор об отчуждении исключительного права, лицензионный договор, реальный договор, консенсуальный договор, объект авторского права

REGARDING THE POSSIBILITY OF TRADING INTELLECTUAL PROPERTY RIGHTS USING BLOCKCHAIN TECHNOLOGY

Abstract. The application of new technologies, including blockchain and NFTs, can become a tool for ensuring the protection of rights and lawful interests of rights holders and stimulating innovation in various fields. This paper examines two legal issues related to the deposit and circulation of intellectual property results, including copyright objects. The first issue is the possibility of using blockchain technology to deposit such objects. The second issue concerns the transfer of rights to deposited objects.

Keywords: exclusive right, NFT, blockchain, deposit, assignment agreement, license agreement, real agreement, consensual agreement, object of copyright

Активно развивающимся направлением использования технологии блокчейн в настоящее время является создание невзаимозаменяемых токенов (далее – NFT, NFT-токен), посредством которых можно осуществлять передачу различных, в частности цифровых, благ. Считается, что использование NFT позволяет привязать конкретный объект права к цифровому «образу» и тем самым вести учет прав на них, в том числе осуществлять посредством передачи такого токена передачу прав на определенное благо, например, недвижимость [3].

Фиксация существования результата интеллектуальной деятельности с использованием системы блокчейн может осуществляться двумя способами – с депонированием объекта и без такового. Каждый из этих способов заслуживает отдельного внимания, поскольку имеет как преимущества, так и недостатки, а также связанные с ними правовые риски.

Процесс фиксации существования РИД без депонирования представляет собой выдачу определенного «сертификата», который может представлять собой, например, уже упомянутый NFT-токен, создаваемый в системе блокчейн. Преимущество этого способа проявляется в том, фиксация существования РИД в блокчейн гарантирует неизменность этого свидетельства (информации, содержащейся в нем) и подтверждение того, что информация о лице, которое предоставило информацию для фиксирования прав на РИД, не будет изменена неправомерными действиями третьих лиц. У такого способа фиксации есть и недостатки. В частности, поскольку депонирования результата интеллектуальной деятельности не происходит, убедиться в том, что депонент является правообладателем конкретного произведения, в отношении которого выдан сертификат, практически невозможно.

Фиксация с депонированием, в свою очередь, позволит избежать недостатков, присущих процессу фиксации без депонирования. Вместе с тем следует отметить те правовые проблемы, которые могут возникнуть при таком способе фиксации факта создания РИД и прав на него. В фиксации с депонированием можно

выделить два основных пути: депонирование будет осуществляться традиционным способом на устройства хранения стороны (речь идет о традиционных системах хранения информации – SQL базах данных), либо с использованием технологии блокчейн – т. е. хранение депонированного РИД будет осуществляться в связке с соответствующим сертификатом (NFT) в самой системе блокчейн.

Одной из ключевых правовых проблем, связанных с депонированием объектов авторского права, является проблема потенциального нарушения исключительного права на депонируемый объект. В соответствии со ст. 1270 ГК РФ использованием произведения независимо от того, совершаются ли соответствующие действия в целях извлечения прибыли или без такой цели, считается, в частности, воспроизведение произведения – т. е. создание одного или нескольких экземпляров произведения. Возникает резонный вопрос – не будет ли депонирование являться формой воспроизведения объекта авторского права? Судебная практика и доктринальные воззрения по этому вопросу на протяжении нескольких лет разительно изменились. Как еще в 2016 году указал ВС РФ, хранение охраняемого произведения в цифровой форме в электронном средстве является воспроизведением в смысле статьи 9 Бернской конвенции [1]. В итоге Верховный суд РФ изменил свое мнение на диаметрально противоположное, указав, что само по себе хранение материального носителя, в котором выражен объект авторского права, без цели введения его в гражданский оборот не является самостоятельным способом использования произведения, в связи с чем такое хранение не требует специального согласия правообладателя [2].

Следовательно, простое хранение в памяти компьютера без каких-либо дополнительных действий с депонированным объектом не будет представлять собой использование по смыслу ст. 1270 ГК РФ, и не будет требовать согласия правообладателя.

Второй путь фиксации прав на результаты интеллектуальной деятельности – фиксация с депонированием соответствующего объекта в блокчейн-системе. В частности, одной из особенности блокчейн систем является открытость и публичность всей информации, которая в нем находится и, следовательно, депонирование объекта может являться актом доведения до всеобщего сведения, что, в отсутствие согласия, будет являться нарушением исключительного права правообладателя.

Преимуществом использования блокчейн-реестров для депонирования РИД является появление возможности для организации оборота прав на соответствующий объект. Оборота прав будет осуществляться следующим образом: при депонировании РИД правообладатель вправе создать смарт-контракта с присоединенным к нему элементом NFT. Такая связка позволит в любой момент времени идентифицировать соответствующий объект, который связан со смарт-контрактом.

Особенностью оборота исключительных прав с использованием смарт-контрактов является то, что права по нему должны переходить при передаче NFT от продавца к покупателю – в этой связи, поскольку момент перехода права и передачи NFT совпадают, можно также утверждать о возможности заключения договора об отчуждении исключительного права как по модели реального договора,

который будет заключен с момента передачи NFT, так и по консенсуальной модели, при этом такой договор может быть заключен в традиционной «аналоговой» форме и передача токена NFT, который воплощает в себе исключительное право, будет приравниваться к передаче исключительных прав.

Вопросом, требующим отдельного обсуждения, является вопрос о форме договора, заключаемого по конструкции смарт-контракта. В соответствии со ст. 1234 ГК РФ, договор об отчуждении исключительного права заключается в письменной форме, при этом несоблюдение письменной формы влечет недействительность договора. С точки зрения действующего законодательства, в частности, ст. 434 ГК РФ, в соответствии с которой, оговор 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 в соответствии с правилами абзаца второго пункта 1 статьи 160 ГК РФ, т. е. при соблюдении требований идентификации сторон при использовании технических средств и возможности воспроизведения сделки на материальном носителей. Как отмечают исследователи, элементом смарт-контракта как программного кода является цифровая подпись, которая подтверждает волю участников сделки, запускает действие алгоритма смарт-контракта при заключении договора [3]. Такую подпись можно рассматривать как элемент идентификации сторон в том случае, если для ее применения будет использована площадка организации, требующая регистрации и предоставления совокупности данных участников, благодаря которым они могут быть идентифицированы.

Поводя итог, следует заключить, что, несмотря на определенные правовое и технические сложности, реализация фиксации и оборота исключительных прав на объекты авторского права с применением технологии блокчейн возможна. При этом, помимо указанных проблем, при реализации такого проекта необходимо учитывать те затраты, которые необходимо будет понести организации. К ним можно отнести, в частности, затраты на разработку или приобретение программного и аппаратного обеспечения для депонирования с использованием технологии блокчейн; необходимость оплаты транзакционных сборов за размещение данных в сети блокчейн (этот вопрос представляет отдельный интерес в том случае, если реализовывать такое депонирование будет юридическое лицо, не являющееся собственником своего имущества), а также необходимость разработки юридической документации для депонирования объектов авторского права.

Список литературы

1. Определение Судебной коллегии по экономическим спорам Верховного Суда РФ от 08.06.2016 № 308-ЭС14-1400 по делу № А20-2391/2013 // СПС «КонсультантПлюс».

2. Постановление Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» // Бюллетень Верховного Суда РФ. 2019. № 7.

3. Санникова Л. В., Харитонова Ю. С. Цифровые активы: правовой анализ: монография. Москва: 4 Принт, 2020. 304 с.

Н. В. Шакель,
кандидат юридических наук, доцент,
Общество с ограниченной ответственностью «Степановский,
Папакуль и партнеры»

ОТКРЫТЫЕ ЛИЦЕНЗИИ В ПРАВЕ РЕСПУБЛИКИ БЕЛАРУСЬ

Аннотация. В работе проведен анализ положений законодательства Республики Беларусь об открытых лицензиях в отношении объектов авторского права и смежных прав. Соответствующие положения появились в законодательстве в 2020 году и в настоящее время активно применяются на практике. Вместе с тем отдельные положения регулирования требуют совершения, в частности, установлен разный срок действия лицензии в ситуации, когда лицензируется компьютерная программа (программа для ЭВМ) и база данных или иные объекты авторского права и смежных прав. Предложены пути совершенствования законодательства.

Ключевые слова: авторское право, цифровые технологии, открытые лицензии, правообладатель, пользователь, срок лицензии, законодательство

OPEN LICENSE IN THE LEGISLATION OF THE REPUBLIC OF BELARUS

Abstract. In the work, the author analyzed the provisions of the legislation of the Republic of Belarus on open licenses in relation to objects of copyright and related rights. The relevant provisions appeared in the legislation in 2020 and are currently being actively applied in practice. At the same time, certain provisions of the regulation require commission, in particular, a different period of validity of a license is established in a situation where a computer program (computer program) and a database or other objects of copyright and related rights are licensed. Ways of improvement of the legislation are offered.

Keywords: copyright, digital technologies, open licenses, copyright holder, user, license term, legislation

Развитие цифровых технологий повлекло появление новых произведений, которые стали использоваться значительным количеством пользователей, зачастую находящихся в разных регионах мира. В результате стали появляться так называемые «открытые лицензии». Такие лицензии представляет собой удобный механизм, позволяющий правообладателю определить условия использования его объекта авторского права без излишней формализации данного процесса.

Положения, определяющие условия использования произведений на основании открытых лицензий, закреплены и в законодательстве Республики Беларусь (соответствующие изменения вступили в силу в мае 2020 года). Сегодня на основании ст. 45 Закона Республики Беларусь от 17.05.2011 № 262-З «Об авторском праве и смежных правах» (далее – ЗоАП) допускается заключение лицензионных договоров, которые должны быть договорами присоединения, условия которых определяются единолично правообладателем, в упрощенном порядке («открытая лицензия») [1]. Вместе с тем в рассматриваемой области имеются определенные

проблемные аспекты, как с теоретической точки зрения, так и при практической реализации норм, в связи с чем полагаем актуальным еще раз обратиться к данной проблеме.

В целом тематика открытых лицензий получила определенное внимание в юридической литературе. Так, Е. Янтикова, последовательно рассматривая условия открытых лицензий, отмечала, что «единственным существенным условием открытой лицензии является ее предмет, который состоит в предоставлении на неисключительной основе права использования конкретного произведения определенными способами» [2. С. 289]. А. А. Петрушкевич указывал, что законодатель не указал однозначно, допускает ли открытая лицензия сублицензирование, и предлагал внести соответствующие изменения в ЗоАП, запретив заключение сублицензионного договора по открытой лицензии [3. С. 68]. В нашей более ранней публикации мы рассматривали вопрос соотношения открытой лицензии и требований, которые предъявляются к внешнеторговым договорам, отмечая определенные проблемные аспекты и предлагая пути их решения [4. С. 117]. Вместе с тем положения законодательства, касающиеся открытых лицензий, требуют дальнейшего изучения и научного осмысления.

Остановимся еще раз на основных положениях законодательства Республики Беларусь об открытой лицензии. В соответствии в ЗоАП, все условия открытой лицензии должны быть доступны неопределенному кругу лиц и размещены таким образом, чтобы лицензиат имел возможность ознакомиться с ними перед началом использования соответствующего объекта авторского права или смежных прав (ч. 2 и 3 п. 1 ст. 45 ЗоАП). Вместе с тем ЗоАП не предусматривает и не детализирует то, каким образом следует размещать условия открытых лицензий. Отметим, что законодательство Республики Беларусь не имеет трансграничного действия, как следствие, его положения не регулируют вопросы создания объекта интеллектуальной собственности за рубежом и его последующую «судьбу». Рассматривая норма по сути признает наличие соответствующих лицензий и «легализует» их использование субъектами хозяйствования, частными лицами и иными субъектами.

Следует отметить, что ЗоАП указывает на то, что открытая лицензия как механизм лицензирования может применяться к любым объектам авторского права и смежных прав (п. 1 ст. 41 ЗоАП). При этом в зависимости от того, какой объект лицензируется, меняются условия лицензирования. Как указывает законодатель, «если срок действия открытой лицензии не определен, то лицензионный договор считается заключенным в отношении компьютерных программ и баз данных на весь срок действия исключительного права, а в отношении других видов произведений и объектов смежных прав – на пять лет» (п. 3 ст. 45 ЗоАП). В теоретическом плане возможно поставить вопрос о правомерности и обоснованности такого разграничения объектов авторского права и смежных прав. Следует отметить, что в данном положении видится определенная проблемность. Она связана с тем, что компьютерные программы и базы данных известны своей «недолговечностью», а именно, тем устаревания соответствующих ресурсов, систем достаточно короткий. За 5-10 лет в деятельности организаций зачастую полностью меняется

используемое программное обеспечение, существенно дополняются и изменяются (с учетом поступающей информации) базы данных. При этом «обычные» произведения, не относящиеся к компьютерным программам и базам данных, используются длительный срок, в том числе в течение срока жизни автора и много лет после его смерти (например, произведения литературы могут не терять актуальности и через много лет после их написания). Законодатель закрепил обратный данной логике подход: компьютерные программы и базы данных лицензируются в течение всего срока действия авторского права, а иные объекты – только в течение 5 лет.

Представляется, что данный подход не является удачным в силу ряда обстоятельств, основным из которых является комплексный характер объектов в цифровой форме, которые могут лицензироваться в онлайн-отношениях. Так, например, веб-сайт состоит из не только из программной части (соответствующей программы для ЭВМ), но из текста, рисунка и прочих объектов. В результате предоставления прав на использование сложных объектов на условиях открытой лицензии может оказаться, что права перейдут на разный срок, даже несмотря на то, что объект представляет единое целое.

Вместе с тем рассматриваемый подход может быть признан оправданным с той точки зрения, что длительный (по сути – бессрочный) период использования удобен для пользователей, так как позволяет предсказуемо использовать объект (зная, что лицензия не прекратится в обозримый срок).

Тем не менее нельзя не учитывать тот факт, что в современных условиях цифровизации лицензирование на условиях открытой лицензии идет в основном через сеть Интернет (и размещенные в ней ресурсы) и применительно к программам для ЭВМ и связанным с ними базам данным. В этой связи предлагается скорректировать положения статьи 45 ЗоАП с тем, чтобы обеспечить единый подход, унифицировать сроки предоставления прав. При этом недостаточно будет сузить сферу ее действия только на указанные два объекта (программы для ЭВМ, называемые в ЗоАП компьютерными программами, и базы данных), поскольку сегодня значительная часть программных продуктов имеет связанные с ним иные объекты авторского права и смежных прав (тексты, описания, визуальные описания), а, следовательно, необходимо обеспечить им единый правовой режим. Представляется, что максимально удобным с практической точки зрения было бы закрепление следующей редакции п. 3 ст. 45 ЗоАП: «если срок действия открытой лицензии не определен, то лицензионный договор считается заключенным в отношении произведений и объектов смежных прав на весь срок действия исключительного права». Это позволит и правообладателям, и пользователям иметь предсказуемые и понятные условия их деятельности, без необходимости отслеживания ситуации с правами на конкретный объект, полученный по открытой лицензии.

В заключение отметим, что использование открытых лицензий является реальностью современного времени, следствием активной цифровизации экономики. Их применение удобно и для правообладателей, которым не требуется согласовывать условия лицензий с каждым конкретным пользователем. Очевидны преимущества и для получателей лицензий, поскольку расширяются возможности

правомерного использования объектов авторского права и смежных прав. Вместе с тем имеющиеся на данный момент в законодательстве формулировки требуют определенного совершенствования, в связи с чем предложено их уточнение в части корректировки срока, на который считается предоставленной открытая лицензия, если правообладателем такой срок не оговорен.

Список литературы

1. Об авторском праве и смежных правах [Электронный ресурс]: Закона Республики Беларусь от 17.05.2011 № 262-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2023.

2. Петрушкевич А. А. Понятие, существенные условия и некоторые проблемы открытой лицензии в авторском праве // Интеллектуальная собственность в современном мире: вызовы времени и перспективы развития: материалы Международной научно-практической конференции: в 2 ч., Минск, 20 октября 2021 года. Ч. 2. Минск: Альфа-книга, 2021. С. 64–69.

3. Шакель Н. В. Проблемные аспекты заключения лицензионных договоров в упрощенном порядке (открытые лицензии) // Право интеллектуальной собственности Республики Беларусь: история становления и перспективы: сборник статей международного научно-практического круглого стола, Минск, 19 апреля 2022 г. Минск: Белорусский государственный университет, 2023. С. 114–121.

4. Янтикова Е. В. Правовая природа и механизмы применения открытых лицензий в Республике Беларусь // Интеллектуальная собственность в современном мире: вызовы времени и перспективы развития: материалы Международной научно-практической конференции: в 2 ч., Минск, 20 октября 2021 года. Часть 2. Минск: Альфа-книга, 2021. С. 287–295.

В. Н. Шельменков,
эксперт,
Московский государственный юридический университет
имени О. Е. Кутафина

РОЛЬ LEGAL TECH В МОДЕРНИЗАЦИИ ПРОФЕССИОНАЛЬНОЙ ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. В статье дается правовая оценка современным технологиям, обсуждается терминология LegaLtech, а также дается алгоритм, как автоматизировать процессы в компании. Приводятся примеры применения инновационных технологий в профессиональной юридической деятельности, связанные с разработкой отдельных решений LegalTech. Результатом станет значительное упрощение работы по определенным процедурам. Сервисы LegalTech помогут не только сэкономить время и средства специалистов, но и избежать нежелательных итогов, например, в виде отказа ФНС в регистрации, или признание недействительным решения о реорганизации юридического лица. Таким образом, нет причин

опасаться Legal tech, скорее наоборот – стоит изучать развитие технологий в юриспруденции и способствовать их созданию. Ведь только сталкиваясь на практике с проблемами в юридическом сопровождении, можно иметь представление в том, как такую проблему решить.

Ключевые слова: информационные системы, информационные технологии, базы данных, агрегаторы, LegalTech, предпринимательская деятельность, искусственный интеллект

THE ROLE OF LEGAL TECH IN MODERNIZING PROFESSIONAL LEGAL PRACTICE

Abstract. The article provides a legal assessment of modern technologies, discusses LegaLtech terminology, and also proposes an algorithm for how to automate processes in a company. The results of the application of innovative technologies in professional defense activities associated with the emergence of new LegalTech solutions are given. The result will be simplification of work on carrying out procedures. LegalTech services help not only save time and money on consultations, but also avoid undesirable results, for example, in the form of refusal of registration by the Federal Tax Service, or making invalid decisions on the reorganization of a legal entity. Thus, there is no reason to fear Legal tech; rather, on the contrary, it is worth studying the development of technologies in jurisprudence and contributing to their creation. After all, only by encountering problems in legal support in practice can you have an idea of how to solve such a problem.

Keywords: Information systems, information technologies, databases, aggregators, LegalTech, entrepreneurial activity, artificial intelligence

Введение. В настоящее время информационно-коммуникационные технологии являются неотъемлемой частью нашей жизни, без них ныне трудно представить себе существование и развитие человеческого мира. Как следствие, нельзя не отметить, что стремительная информатизация общества привела к явлению, известному как автоматизация рабочих процессов. Современная юриспруденция также не смогла избежать данной участи, а потому с каждым днем цифровизация юридической деятельности привлекает все больше интереса со стороны как ученых-правоведов, так и тех, кто далек от юридической профессии. Выполнение таких рутинных задач, как составление договоров, контроль документооборота, оформление лицензий, при помощи искусственного интеллекта, алгоритмы которого исключают возможность профессиональной ошибки, уже не фантазия, а реальность, к которой человечество успешно движется. Таким образом, одним из способов модернизации юриспруденции стали системы Legal tech.

Данному понятию можно дать определение Д. С. Гвоздецкого: «Legal tech – это программы, которые построены в том числе на искусственном интеллекте, позволяющие автоматизировать процедуру нормотворчества, анализировать большие массивы информации, определять вероятность применения нормативных правовых актов в правоприменительной практике, прогнозировать влияние

проектируемых актов на качество правового регулирования общественных отношений» [1].

По мнению А. В. Минбалеева о том, что «в качестве основных признаков LegalTech можно выделить следующие:

– специальная сфера применения LegalTech – правовая. Практически все сферы юридической деятельности сегодня связаны так или иначе с информационными технологиями, продуктами, решениями;

– направленность применения технологий и продуктов LegalTech на оптимизацию юридических процессов, замену человека автоматизированными средствами и решениями, высвобождение рутинных процессов;

– LegalTech выступают методом, инструментом решения тех или иных юридических задач с использованием различных информационных технологий, продуктов, решений;

– LegalTech реализуются посредством предоставления юридических услуг с использованием информационных технологий, а также услуг по предоставлению тех или иных технологических решений, продуктов, позволяющих осуществлять профессиональную юридическую деятельность» [2].

Юридическая индустрия достаточно традиционна по своей природе, и по этой причине многие ее работники настороженно относятся к новейшим технологиям. Тем не менее в последнее время системы Legal tech набирают обороты, особенно с учетом того, что недавняя пандемия COVID-19 затруднила доступ юридических и физических лиц к услугам профессионалов.

Цифровые инновации, таким образом, повысили эффективность и производительность работников юридических компаний и определили стратегию модернизации юриспруденции. Можно выделить несколько особо значимых «шагов» на пути к информатизации профессии:

1. Автоматизация. Передача процедур и обязанностей, которыми обычно озабочены практикующие юристы, в ведение информационных технологий – вот как достигается автоматизация правовой деятельности. Как правило, она требуется для сложной и однообразной работы, которая связана со сбором больших объемов данных, монотонными действиями, составлением и заполнением документов. Е. А. Канунникова и А. В. Лошкарев в своей научной статье объясняют важность этой технологии: «… автоматизация процессов юристов в перспективе позволит повысить качество и профессионализм их услуг, а использование машинного обучения и искусственных нейронных сетей – оптимизировать законодательство в части выявления устаревших и дублирующих норм права, коллизий между ними и спорных формулировок в нормативных актах» [3].

2. Анализ документов за меньшее время. Юристы вынуждены читать и анализировать огромное количество различных законов, договоров и иных документов, давать комментарии и делать пометки, чтобы иметь возможность тщательно консультировать клиентов. Искусственный интеллект вполне способен выполнять эту бумажную работу вместо человека. Процедура довольно проста: система отбирает необходимые документы с помощью фильтра, детально изучает их, выделяет главные положения и подготавливает для профессионалов. В результате это

ощутимо облегчает работу сотрудникам юридических фирм, поскольку машины могут давать практическую оценку документам и классифицировать их, не обращая внимания на область права и язык.

3. Упрощение процесса юридического исследования. Двадцать первый век – это цифровая энциклопедия, и поэтому практикующие юристы в нашу эру имеют практически неограниченный доступ к информации о судьях и судах, кодексах законов, правовых доктринах, толковании норм. Личный опыт в качестве основного источника знаний заменяют точные данные, получаемые благодаря Legal tech.

Эти инструменты юридических технологий помогут разобраться в неоднозначных аспектах дела, например, как часто конкретный судья выносит решение в порядке упрощенного судопроизводства или в какой суд клиенту стоит обратиться. Те, кто обращаются в юридические компании, хотят знать о предполагаемых судебных расходах и продолжительности дела, каковы их шансы на положительный исход. Юристы и раньше успешно использовали в полной мере все имеющиеся средства, но теперь, в связи с активным развитием Legal tech, у них есть гораздо больше того, что они могут предложить клиентам.

4. Снижение уровня стресса у работников. Юристы должны иметь дело с большим количеством клиентов, просматривать и корректировать множество документов, проводить юридические исследования, что невероятно сильно утомляет их. Инновационные технологии способны же помочь с выполнением данных процедур, чтобы профессионал мог сосредоточиться на творческом анализе ситуации и получать удовольствие от того, чем он занимается.

Инструменты Legal tech работают быстро и безошибочно, снижая нагрузку на юристов и экономя их время. Например, есть приложения, которые позволяют планировать задачи и своевременно выполнять их, такие, как OneNote и Todoist. Они отправляют уведомления в соответствии с настроенным пользователем электронным календарем, не давая пропустить важные события или пропустить дедлайн.

5. Возможность удаленной работы. С тех пор, как в нашу жизнь ворвалась пандемия COVID-19, а за ней и самоизоляция, многие компании перешли на удаленную работу, и юридические фирмы не стали исключением. Эта ситуация принудила юридическую отрасль к использованию цифровых технологий с помощью различных программ искусственного интеллекта. Вследствие этого сегодня профессионалы могут получить полноценный доступ к документам из дома и организовать видеоконференции для клиентов, что способствует более высокой производительности.

Однако нельзя не отметить и некоторые минусы Legal tech:

1. Угроза безработицы. Реальность такова, что машины справляются с рабочими делами куда эффективнее и быстрее людей. Выполнение таких задач, как проведение юридических исследований, проверки документов, искусственным интеллектом означает снижение потребности в человеческом капитале. Об этом свидетельствуют нынешние тенденции, прогнозируемые Gartner, Deloitte и Forbes, которые оценивают, что около 20 % работников в сфере юриспруденции

могут быть вытеснены программами искусственного интеллекта, что приведет, соответственно, к резкому снижению количества рабочих мест.

2. Постоянные финансовые затраты. Информатизация – это не одноразовое событие, а потому важно уяснить, что придется постоянно наращивать цифровой потенциал, что обходится недешево. Это означает, что те технологии, в которые фирмы инвестируют сегодня, через определенный промежуток времени потребуют замены, обновления, улучшения, поскольку новые системы Legal tech превратят их в неактуальные, устаревшие. Если же юридическая компания откажется от этого, то она легко потеряет конкурентоспособность и окажется в достаточно опасном положении на рынке.

3. Угроза информационной безопасности. Если в 2016 году киберпреступления совершались каждые 40 секунд, то в 2019 – уже каждые 14 секунд [4]. Основной целью, как правило, является хищение конфиденциальных данных, и юридические фирмы часто привлекательны в качестве объекта преступления. Компании внедряют цифровые инструменты для обмена документами, связи между юристами и клиентами. Больше возможностей цифрового доступа – больше возможностей для ошибок, упущений и взломов. Юридическая индустрия сталкивается с серьезной угрозой, стоимость киберстрахования стремительно растет, поэтому необходимость кибербезопасности нельзя отрицать.

Заключение. Таким образом, роль Legal tech в модернизации юриспруденции действительно неоспорима. Растущая эффективность выполнения задач, автоматизация процессов, снижение нагрузки на профессионалов – эти цифровые преимущества навсегда изменили облик индустрии и показали дальнейшие пути ее развития. Однако с данными новшествами связаны и немаловажные опасности. Фирмам теперь нужно постоянно беспокоиться о кибербезопасности и нести значительные затраты для того, чтобы не потерять возможность оставаться конкурентоспособными. Нет никаких сомнений в том, что технологии будут продолжать влиять на юридическую деятельность, но кому они принесут успех, а кого обанкротят, еще предстоит выяснить.

В конечном итоге LegalTech – это технологии, которые помогают юристам и компаниям упростить и ускорить процессы юридической работы.

Таким образом, нет причин опасаться LegalTech, скорее наоборот – стоит изучать развитие технологий в юриспруденции и способствовать их созданию. Ведь только сталкиваясь на практике с проблемами в юридическом сопровождении, можно иметь представление в том, как такую проблему решить [5].

Список литературы

1. Информационно-технологическое обеспечение юридической деятельности (LegalTech): учебник. М.: Проспект, 2022. 368 с.

2. Гвоздецкий Д. С. Legal Tech и ведомственное нормотворчество: перспективы // Образование. Наука. Научные кадры. 2020. № 4. С. 33–35.

3. Канунникова Е. А., Лошкарев А. В. Цифровизация юридической профессии: угрозы и возможности // Международный журнал гуманитарных и естественных наук. 2020. № 10-3. С. 103–105.

4. Приходько Д. В., Белькова А. А. Киберпреступность как глобальная проблема современности // Экономика и бизнес: теория и практика. 2021. №4-2. С. 90–93.
5. Шельменков В. Н., Гусев Д. А. Рецензия на монографию «Legaltech в сфере предпринимательской деятельности» // Теоретическая и прикладная юриспруденция. 2023. № 2 (16). С. 113–116.

Н. И. Шумакова,
доцент кафедры конституционного и административного права,
Южно-Уральский государственный университет (НИУ)

НЕ ТОЛЬКО ДИПФЕЙКИ: ОБЯЗАТЕЛЬНАЯ МАРКИРОВКА СИСТЕМ И ПРОДУКТОВ ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА КАК ЧАСТЬ ЭТИКИ ЕГО ИСПОЛЬЗОВАНИЯ

Аннотация. Статья посвящена необходимости законодательного закрепления обязательной маркировки систем и продуктов генеративного искусственного интеллекта. Анализируются результаты социологического опроса, целью которого являлось выявление мнения о важности принятия данной меры для защиты законных прав и интересов представителей творческих и культурных индустрий и потребителей продуктов этих индустрий. Делается вывод о положительном и негативном влиянии введения такой маркировки.

Ключевые слова: цифровые технологии, право, этика искусственного интеллекта, генеративный искусственный интеллект, регулирование искусственного интеллекта, дипфейки, риски генеративного искусственного интеллекта

NOT ONLY DEEPFAKES: OBLIGATORY LABELING OF GENERATIVE ARTIFICIAL INTELLIGENCE'S SYSTEMS AND PRODUCTS AS PART OF THE ETHIS OF USING IT

Abstract. The article explores the necessity of legal implementation of obligatory labeling of general artificial intelligence's systems and products. The author provides an analysis of a sociological survey the goal of which was to study the opinion of those involved in the creative and cultural industries as well as those who consume their products. In conclusion, the author provides pros and cons of the implementation of this measure.

Keywords: digital technologies, law, ethics of AI, generative AI, regulations of AI, deepfakes, risks of generative AI

Рост использования систем искусственного интеллекта сегодня можно назвать беспрецедентным, но вместе с ростом их использования растет и количество дискуссий о их негативном влиянии на те сферы, в которых они используются [6]. Отдельное место в этих дискуссиях занимает генеративный искусственный интеллект (далее – ГИИ), в число рисков применения которого входят засилие плагиаризма и систематическое нарушение авторских прав [7]. Более того, с развитием таких систем, как ChatGPT, Stable Diffusion, DreamStudio, DreamUp,

Midjourney и других ГИИ, все чаще вызывает обеспокоенность судьба творческой и культурной индустрий, само существование которых оказалось под угрозой. В частности, Комитет культуры, медиа и спорта Палаты общин Великобритании в одном из своих последних отчетов заостряет внимание на огромном потенциале новых цифровых технологий, отмечая, что несмотря на очевидные плюсы их развития, они становятся причиной новых рисков и проблем, требующих своевременного урегулирования. При этом Комитет отметил как возможность негативного влияния абстрактности формулировок в мерах регулирования использования ГИИ на права и законные интересы представителей творческих профессий, выявленную в рамках проведенного им расследования, так и очевидность причинения вреда в случае, если данные пробелы в законодательстве не будут устранены. Комитет также подчеркивает, что стремительное развитие ГИИ усугубляет так называемый «кризис аутентичности», а именно – делает практически невозможным установить происхождение подлинность онлайн-контента, в то же время призывая к стимулированию использования новых технических средств в творческом секторе [5].

Собственное расследование провел и британский Комитет науки, инноваций и технологий, также придя к выводу о том, что использование ГИИ может оказывать негативное влияние на сферу труда, а также нарушать авторские и интеллектуальные права [10]. С этими отчетами перекликаются как с требованиями, пожалуй, крупнейшей в истории Голливуда забастовки работников киноиндустрии [12], так и с коллективными исками [1, 3].

Американская гильдия авторов среди своих требований по защите будущего литературы и журналистики перечисляет получение разрешения на использование авторских материалов для обучения ГИИ, введение компенсации за такое использование, а также обязательность маркировки работ и произведений сгенерированных ГИИ. Интерес представляет и предположение зарубежных адвокатов о возможности взыскания морального вреда за причинение моральных страданий путем обесценивая художественных произведений. Обратить внимание стоит и на Китай. Так, Й. Ван и Х. Лу, рассуждая о трансформациях, претерпеваемых творческой индустрией, говорят о необходимости реформирования существующего законодательства и ссылаются на судебную практику, существующую на сегодняшний день в Китайской Народной Республике, согласно которой, выбор и порядок действий человека, участвующего в генерации произведения в определенных случаях приводят к тому, что сгенерированные результаты становятся объектом авторского права [11].

Отдельного упоминания заслуживает влияние использования ГИИ на средства массовой информации (далее – СМИ), а именно – на производство и потребление новостей, где возможно не только распространение опасной дезинформации, появление мошеннических СМИ, но и падение качества подачи новостного материала [7]. В то же время, если мы обратимся к мнению представителей российских творческих и культурных индустрий, высказанному в рамках «Горький fest» ранее в этом году, то заметим, что большинство из них пока не рассматривает ГИИ как реальную угрозу существования их профессий в виду того что ГИИ, как и любое вспомогательное техническое средство, не обладает способностью мыслить и чувствовать, а значит – не является творцом в полном смысле этого слова [14].

Решение части этих проблем недавно предложила компания Twilio, разработавшая специальный инструмент маркировки продуктов систем ГИИ, где конечными целями являются повышение доверия и обеспечение прозрачности, ответственности и подотчетности использования данных технологий, в том числе возможности получения информации о том, какие материалы использовались для обучения ГИИ и каков процент участия ГИИ в создании того или иного продукта [4]. Аналогичное решение предлагает глобальная инклюзивная инициатива Open Ethics Label [8] со ссылкой на Белую книгу Еврокомиссии «Об искусственном интеллекте: Европейский подход к совершенству и доверию» от 19.02.2022, предусматривающую добровольную маркировку [13]. В России же со схожей инициативой, хоть и преследуя несколько иные цели (защиту от возможных кибератак), в этом году к Министерству цифрового развития обратились представители РТУ МИРЭА, предложив маркировать специальным графическом знаком контент, созданный нейросетями [15], им, в свою очередь, вторит заместитель председателя Еврокомиссии В. Йоурова, рассматривающая обязательную маркировку продуктов ГИИ как средство защиты от распространения дезинформации [2].

Для того чтобы выявить мнение представителей творческой и культурной индустрий, а также потребителей продуктов этих индустрий, о необходимости уже не добровольной, а обязательной маркировки продуктов ГИИ в рамках защиты их законных прав и интересов, автором статьи был проведен социологический опрос, являющийся частью комплексного исследования автора по этике использования ГИИ в творческой и культурных индустриях.

Этика проведенного опроса: опрос был проведен в социальных сетях и мессенджерах с 1 июля по 30 августа 2023 г. на условиях полной анонимности, все участники были предупреждены о возможности использования полученных результатов в научно-исследовательской работе.

Программное обеспечение: опрос был произведен в Google Docs, статистические данные автоматически подсчитаны в Google Docs, для анализа результатов также было применено приложение Google Sheets.

География проведенного опроса:

1. Англоязычная аудитория: 109 человек из 17 стран (Великобритания, США, Австралия, Новая Зеландия, Швеция, Германия, Италия, Канада Франция, Сербия, Аргентина, Австрия, Нидерланды, Турция, Ирландия, ЮАР, Чехия).

2. Русскоязычная аудитория: 36 человек из 4 стран (Россия, Латвия, Молдова, Польша).

Результаты и обсуждение. Абсолютное большинство англоязычной аудитории (рис. 1), а именно – 87,2 % (95 человек), ответили, что продукты ГИИ должны подлежать обязательной маркировке, в то время как 8,3 % (9 человек) посчитали, что продукты ГИИ в такой маркировке не нуждаются, а 4,6 % (5 человек) ответили, что они не уверены в необходимости принятия таких мер. Среди русскоязычной аудитории (рис. 2) большинство респондентов также заявили о необходимости введения обязательной маркировки – 80,6 % (29 человек), в то же время здесь наблюдается как больший процент несогласных – 13,9 % (5 человек), так и больший процент неуверенных – 5,6 % (2 человека).

При этом количество англоязычных респондентов, непосредственно задействованных в культурной и творческой индустриях, составило 84,4 % (92 человека), а русскоязычных представителей культурных и творческих профессий – 72,2 % (26 человек).

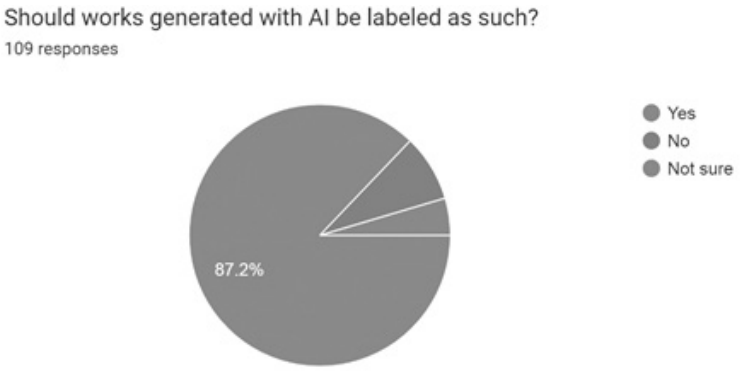

Рис. 1. Распределение ответов англоязычных респондентов на вопрос «Нуждаются ли работы, сгенерированные ИИ, в специальной маркировке?» (на английском вопрос был задан как “Should works generated with AI be labeled as such?”)

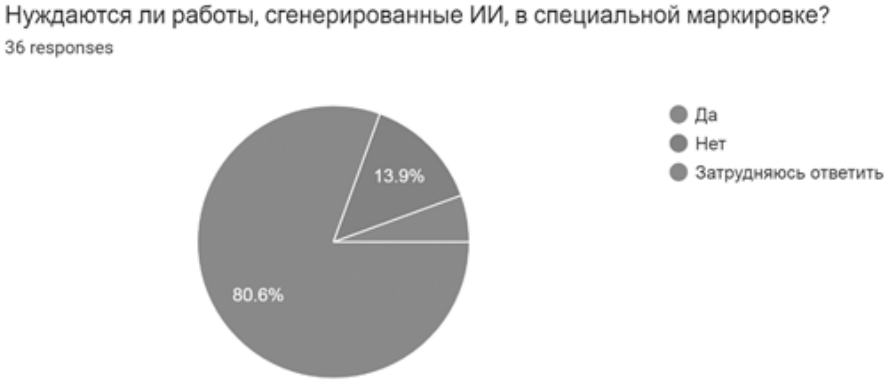

Рис. 2. Распределение ответов русскоязычных респондентов «Нуждаются ли работы, сгенерированные ИИ, в специальной маркировке?»

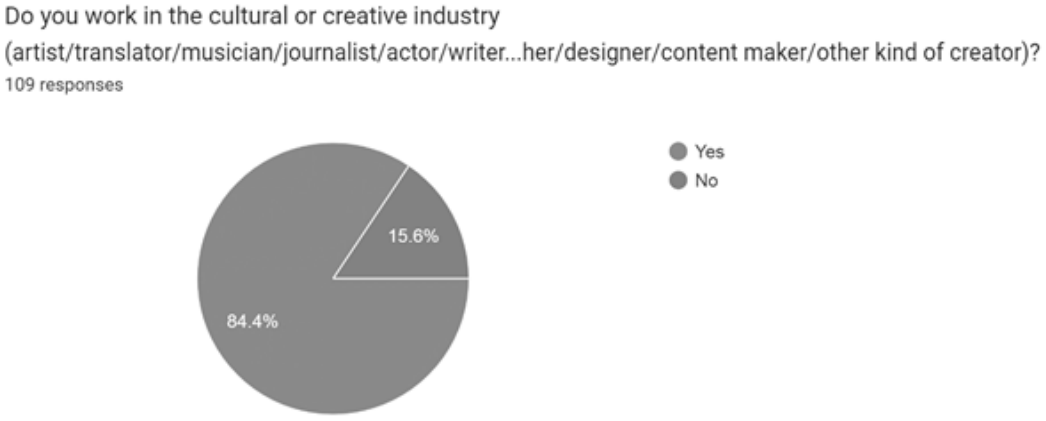

Рис. 3. Распределение ответов англоязычной аудитории «Являетесь ли Вы представителем культурных/творческих профессий?» (на английском вопрос был задан как “Do you work in the cultural or creative industry?”)

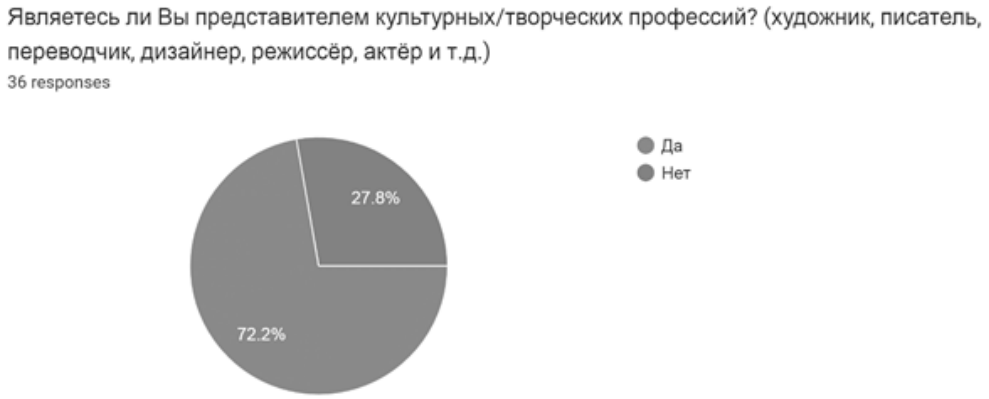

Рис. 4. Распределение ответов русскоязычных респондентов «Являетесь ли Вы представителем культурных/творческих профессий?»

Анализ полученных данных позволяет заключить, что абсолютное большинство респондентов считает необходимым введение обязательной маркировки продуктов/работ, созданных ГИИ. При этом данной точки зрения придерживаются и потребители продуктов творческой и культурных индустрий.

В то же время результаты опроса демонстрируют, что около 30 % русскоязычных респондентов не считают необходимым введение данной меры. От части это можно объяснить тем, что среди русскоязычных опрошенных выше и процент не задействованных в творческой и культурных индустриях. Также можно предположить, что на результат повлияло распространенное в России отношение к ГИИ как вспомогательному инструменту, неспособному к самостоятельному творчеству, а значит – не представляющему угрозы.

Исходя из результатов проведенного исследования, можно заключить, что законодательное закрепление обязательной маркировки систем и продуктов ГИИ способно стать ответом на целый ряд вызовов, связанных со стремительным ростом его использования. Данная мера повысит доверие как к производителям и владельцам систем ГИИ, так и непосредственно к самим работам, сгенерированным ГИИ. При этом прозрачность, обеспечиваемая маркировкой, позволит понять процент участия человека в создании того или иного произведения, установить, какие данные и в каком объеме были использованы для обучения ГИИ, а также даст представление об алгоритмах его работы. В свою очередь, это создаст почву для решения проблемы нарушения ГИИ авторских и интеллектуальных прав, дав возможность введения компенсаций для авторов, чьи материалы были использованы в процессе обучения систем ГИИ. Кроме того, обязательная маркировка должна снизить рост создания и распространения дипфейков и дезинформации, повысив ответственное отношение к использованию систем ГИИ и потреблению сгенерированных при их помощи продуктов. Дополнительно, обязательная маркировка ГИИ обеспечит защиту интересов потребителей, имеющих право на получение полной информации о приобретаемом/потребляемом продукте, либо же системе ГИИ, которую они собираются приобрести или использовать в своей работе.

К гипотетическим минусам введения обязательной маркировки можно отнести вероятность снижения интереса как к использованию ГИИ, так и его продуктов, что,

в свою очередь, неизбежно приведет к снижению прибыли компаний – производителей систем ГИИ, а значит, и к снижению темпов развития данных технологий.

Список литературы

1. AI authors – what a US lawsuit could mean for UK IP law // The Trademark Lawyer. URL: https://trademarklawyermagazine.com/ai-authors-what-a-us-lawsuit-could-mean-for-uk-ip-law

2. AI generated content should be labelled, EU Commissioner Jourova says // Reuters. URL: https://www.reuters.com/technology/ai-generated-content-should-be-labelled-eu-commissioner-jourova-says-2023-06-05

3. AI Image Generator - Copyright Litigation: The Joseph Saveri Law Firm, LLP. URL: https://www.saverilawfirm.com/our-cases/ai-artgenerators-copyright-litigation

4. AI Nutrition Fact Labels // AI Nutrition Facts. URL: https://nutrition-facts.ai

5. Connected tech: AI and creative technology: A House of commons report от 30.08.2023 № HC 1643 (ред. от 30.08.2023). URL: https://publications.parliament.uk/pa/cm5803/cmselect/cmcumeds/1643/report.html

6. Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., de Prado, M. L., Herrera-Viedma, E., & Herrera, F. Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation Information Fusion. 2023. November. URL: https://www.sciencedirect.com/science/article/pii/S1566253523002129

7. Irwin, P., Jones, D., & Fealy, S. What is ChatGPT and what do we do with it? Implications of the age of AI for nursing and midwifery practice and education: An editorial. Nurse Education Today. 2023. August. URL: https://www.sciencedirect.com/science/article/pii/S0260691723001296?via%3Dihub

8. Open Ethics Label: AI nutrition labels // Open Ethics. URL: https://openethics.ai/label

9. Sandrini, L., & Somogyi, R. (2023). Generative AI and deceptive news consumption. Economics Letters. 2023. November. URL: https://www.sciencedirect.com/science/article/pii/S0165176523003427

10. The governance of artificial intelligence: a House of commons report от 31.08.2023 № 9th Report Session (ред. 31.08.2023). URL: https://publications.parliament.uk/pa/cm5803/cmselect/cmsctech/1769/report.html

11. Wan, Y., & Lu, H. (2021). Copyright protection for AI-generated outputs: The experience from China. Computer Law & Security Review. 2021. September. URL: https://www.sciencedirect.com/science/article/abs/pii/S0267364921000546?via%3Dihub

12. We're Fighting for the Survival of Our Profession: SAG-AFRA strike [Электронный ресурс]. URL: https://www.sagaftrastrike.org/why-we-strike

13. White Paper on Artificial Intelligence: a European approach to excellence and trust от 19.02.2020 // European Comission. URL: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

14. На «ГОРЬКИЙ FEST» обсудили проблему участия нейросетей в кино // Бюллетень Кинопрокатчика. URL: https://www.kinometro.ru/photo/show/album/review_ai_10072023

15. Минцифры предложили ввести маркировку контента, созданного с помощью нейросетей // ТАСС. URL: https://tass.ru/ekonomika/17746919

А. А. Шутова,
кандидат юридических наук,
Казанский инновационный университет
имени В. Г. Тимирясова

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ ПРОТИВ БЕЗОПАСНОСТИ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗДРАВООХРАНЕНИИ

Аннотация. В представленной публикации понимаются некоторые проблемы противодействия преступлениям против безопасности технологий искусственного интеллекта в здравоохранении. Рассматривается вопрос о формировании определения понятия «искусственный интеллект» для целей уголовного закона, функциональной роли искусственного интеллекта в составах преступлений, а также проблемы, которые могут возникнуть в процессе квалификации преступлений против безопасности технологий искусственного интеллекта в здравоохранении.

Ключевые слова: правовое регулирование, охрана, уголовный закон, искусственный интеллект, сфера здравоохранения, медицинский работник, врач, медицинские изделия с искусственным интеллектом

COUNTERING CRIMES AGAINST THE SECURITY OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN HEALTHCARE

Abstract. The presented publication understands some of the problems of countering crimes against the security of artificial intelligence technologies in healthcare. The article considers the formation of the definition of the concept of “artificial intelligence” for the purposes of criminal law, the functional role of artificial intelligence in the composition of crimes, as well as problems that may arise in the process of qualifying crimes against the safety of artificial intelligence technologies in healthcare.

Keywords: legal regulation, protection, criminal law, artificial intelligence, healthcare, medical worker, doctor, medical devices with artificial intelligence

Введение. Система здравоохранения подвержена кардинальным изменения вследствие процессов форсированной цифровизации в обществе [1]. Цифровое здравоохранение в целом направлено на укрепление здоровья населения посредством использования инноваций, нацеленные на предоставление эффективных моделей для оказания медицинской помощи населению.

С учетом особой значимости сферы здравоохранения, в первую очередь направленной на охрану жизни и здоровья граждан, правовой режим уголовно-правовой охраны на данный момент требует своевременной трансформации и выработки наиболее эффективной модели. Полагаем, что цифровые технологии и инновации должны не только способствовать позитивному развитию сферы здравоохранения, но и вызывать доверие у пациентов и медицинских работников, а также не создавать опасения по поводу создания и применения подобных медицинских изделий. Сложившийся правовой механизм может привести к тому, что медицинские организации могут отказаться от внедрения технологий искусственного интеллекта в клиническую практику

под страхом привлечения их к административной ответственности, а их сотрудников – к уголовной. На основе изложенного считается необходимым выбрать оптимальную модель уголовно-правовой охраны здравоохранительных общественных отношений, осложненных применением технологии искусственного интеллекта.

Исключительный и совершенно новый характер технико-биологического (и иного) сосуществования искусственного интеллекта и его носителя вскрывает недостаточность уголовно-правовой охраны и необходимость ее оптимизации. В отличие от многих традиционных преступлений, уголовно наказуемые деяния в цифровой сфере можно легко распространять, повторять, что позволяет продавать преступные методы и предоставлять преступление как услугу [2. С. 128-129]. Технологии искусственного интеллекта все чаще интегрируется в преступную и вредоносную деятельность, расширяя существующие уязвимости и создавая при этом новые угрозы [3. С. 108].

Основная часть. Проблема № 1. Определение понятия «искусственный интеллект» для целей уголовного закона. На данный момент уголовное законодательство Российской Федерации понятие «искусственный интеллект» и его производные не использует. Кроме того, отсутствуют и составы преступлений, связанные с совершением общественно опасных деяний с использованием искусственного интеллекта, несмотря на то, что все чаще цифровыми технологиями стали злоупотреблять злоумышленники. С нашей точки зрения, необходимость в выработке дефиниции для целей уголовно-правовой охраны общественных отношений, возникающих в связи с применением новой цифровой технологии от противоправных посягательств, отсутствует. Обоснованием нашего умозаключения служит то, что легальное определение понятия «искусственный интеллект» сформировано и, по нашему мнению, свидетельствует о его комплексном характере, относящемся к различным сферам его применения (военная промышленность, здравоохранение, сельское хозяйство, образование и т. д.), в связи с этим выработка его для верного и единообразного толкования норм уголовного законодательства представляется нам не целесообразной. Диспозиции уголовно-правовых норм Особенной части Уголовного кодекса Российской Федерации (далее – УК РФ) [4], которые будут содержать в себе термин «искусственный интеллект», будут считаться бланкетными, что потребует от правоприменителя для верной квалификации содеянного отсылки к норме правового акта, раскрывающего его содержание применительно для дургих отраслей права, в том числе и уголовного.

Проблема № 2. Функциональная роль технологий искусственного интеллекта в составах преступлений. Уголовный закон России не содержит в себе ни одной специальной нормы, посвященной искусственному интеллекту как самостоятельному признаку состава преступления. Однако исходя из своей природы, искусственный интеллект может выступать предметом, средством и орудием совершения преступления. Несомненно, вопрос о правосубъектности искусственного интеллекта уже поднимается многими авторами [5], однако возможность привлечения его к уголовной ответственности повлечет кардинальную трансформацию действующего уголовного закона и, по нашему мнению, пока является преждевременным. По нашему мнению, современный потенциал искусственного интеллекта исключает вопрос о его уголовной правосубъектности. Хотя общественно опасная деятельность носителя нечеловеческого интеллекта может иметь место, однако способность

к его внутреннему (психическому) восприятию, являющаяся предпосылкой уголовной ответственности, у искусственного интеллекта отсутствует.

Таким образом, поскольку использование искусственного интеллекта необходимо злоумышленнику для непосредственного воздействия на объект преступления либо для облегчения воздействия, технологии искусственного интеллекта выступают в качестве орудий или средств совершения преступления.

Проблема № 3. Особенности квалификации преступлений против цифровой безопасности технологий искусственного интеллекта в системе здравоохранения. Развитие технологий искусственного интеллекта и их активное использование в системе здравоохранения на различных этапах оказания медицинской помощи свидетельствует о дальнейшей интеграции цифровой технологии, а также поднимает вопросы об эффективности правового регулирования подобных отношений. Стоит согласиться с мнением авторов, полагающих то, что стремительное распространение телемедицины в клинической практике и возрастающая роль искусственного интеллекта ставят перед юристами множество проблем [6. С. 314]. Именно поэтому авторы предлагают пока разработать и принять этические принципы создания (разработки) и использования медицинских изделий на основе технологий искусственного интеллекта, которые, по их мнению, позволят сформировать эффективный правовой режим регулирования подобных правоотношений [7].

Если технология искусственного интеллекта будет воплощена в медицинском изделии, к примеру, в медицинском роботе, оснащенном технологиями искусственного интеллекта, то он уже будет являться вещью материального мира, на которого распространяются отношения собственности. Следовательно, при посягательстве на указанные предметы материального мира, характеризующиеся признаком вещи, будет распространяться положения 21 главы УК РФ. Если посягательство характеризовалось умышленным уничтожением или повреждением чужого имущества, то указанное противоправное деяние можно квалифицировать как преступление, предусмотренное ст. 167 УК РФ. Предметом данного преступления является чужое имущество, в данном случае – медицинский робот, оснащенный технологией искусственного интеллекта.

В контексте современного уровня развития технологий искусственного интеллекта действующие уголовно-правовые запреты могут устанавливать ответственность за некоторые преступления, связанные с искусственным интеллектом. Злоумышленники, используя возможность интеллектуального робота к обучению, могут запрограммировать его на эффективное распознавание идентификационного кода данных изображения. Подобный навык может помочь субъектам получить доступ к личным аккаунтам и паролям пользователей на различных веб-сайтах. Указанные противоправные деяния подлежат уголовно-правовой оценке как незаконный доступ к компьютерной информации, содержащей персональные данные о частной жизни, совершенный умышленно и заведомо в корыстных или личных целях, предусматривающий причинение ущерба правам и законным интересам граждан (ст. 137 и 272 УК РФ).

Кроме того, сегодня, с развитием технологий искусственного интеллекта и в сочетании со знаниями биологии и неврологи были созданы протезы и экзоскелеты с искусственным интеллектом [8. С. 39], которые могут помочь людям решить проблемы и уменьшить их страдания. Если человек уничтожит

искусственный интеллект-протез, который взаимодействует с человеческим телом, это может причинить большие физические и психические страдания его владельцу. Следовательно, если мы рассматриваем протезы с искусственным интеллектом как собственность человека (имущество), а их повреждение – это просто уничтожение или повреждение чужого имущества, то квалификация будет зависеть от значительности причиненного ущерба (для ч. 1 ст. 167 УК РФ характерен «значительный ущерб», в ином случае – наступает административная ответственность). Однако квалификация может измениться, если мы будет рассматривать протез с искусственным интеллектом в качестве части тела человека. Представляется весьма вероятным, что повреждение протеза приведет к причинению вреда здоровью человека. Однако согласно ст. 115 УК РФ лицо привлекается к уголовной ответственности только при причинении кратковременного расстройства здоровья или незначительной стойкой утраты общей трудоспособности. Поэтому повреждение протеза, оснащенного технологией искусственного интеллекта, которое не вызвало кратковременных проблем со здоровьем или незначительной потери общей трудоспособности в результате незначительной травмы или мелкого телесного повреждения, не будет подлежать уголовно-правовой оценке. Одновременно с развитием технологий искусственного интеллекта протезы становятся дешевле. Однако, по нашему мнению, цель применения протезов и экзоскелетов с искусственным интеллектом не может сравниться с понятием значительного ущерба, который требуется устанавливать в качестве признака состава преступления при умышленном уничтожении или повреждении чужого имущества. Действующий уголовный закон России не определяет ответственность за повреждение искусственных протезов других людей.

Заключение. Медицина является одной из самых важных сфер по причине ее направленности на охрану наиболее значимых благ – жизни и здоровья граждан посредством использования новых инновационных подходов, нацеленных на предоставление рациональных и эффективных моделей для оказания медицинской помощи. Именно поэтому применение технологий искусственного интеллекта можно назвать новым революционным решением в традиционной системе здравоохранения.

Применение технологий искусственного интеллекта в здравоохранении вызывает множество вопросов, связанных с выбором оптимальной модели правового регулирования и возложением юридической ответственности на субъектов, вовлеченных в процесс их использования (разработчики, медицинские работники, их применяющие). При этом учитывая особую ценность жизни и здоровья граждан, мерам уголовной ответственности, призванным охранять наиболее важные общественные отношения, будет отдаваться превалирующее значение.

Список литературы

1. Шутова А. А. Запрос на уголовно-правую охрану робототехники и искусственного интеллекта в здравоохранении / А. А. Шутова // Актуальные проблемы науки в исследованиях студентов, ученых, практиков: Сборник научных статей по результатам Международной научно-практической конференции, Ижевск, 26-27 апреля 2023 года. Ижевск: Ижевский институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования

«Всероссийский государственный университет юстиции (РПА Минюста России)», 2023. С. 1978–1984.

2. Бегишев И. Р. Искусственный интеллект и уголовный закон / И. Р. Бегишев, З. И. Хисамова. Москва: Проспект, 2021. 192 с. EDN: DZCJKJ.

3. Бегишев И. Р. Правовые средства обеспечения безопасности цифровых архивов в условиях внедрения технологий искусственного интеллекта / И. Р. Бегишев // Вестник Юридического института МИИТ. 2021. № 2 (34). С. 108–116.

4. Уголовный кодекс Российской Федерации: федеральный закон от 13 июня 1996 г. № 63-ФЗ // СПС «КонсультантПлюс».

5. Филипова И. А. Будущее искусственного интеллекта: объект или субъект права? / И. А. Филипова, В. Д. Коротеев // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 359–386. EDN: IMMOAM.

6. Галлезе-Нобиле К. Правовые аспекты использования искусственного интеллекта в телемедицине / К. Галлезе-Нобиле // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 314–336. EDN: VSKCFB.

7. Шутова А. А., Бегишев И. Р. Инициативный проект Этического кодекса субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе технологий искусственного интеллекта: препринт № 1 за 2023 г. / А. А. Шутова, И. Р. Бегишев. Казань : Изд-во «Познание» Казанского инновационного университета, 2023. 16 с. DOI: 10.21202/978-5-8399-0803-1_2023_1_16

8. Шутова А. А. Медицинские роботы: правовые, этические и социальные проблемы // Безопасность бизнеса. 2023. № 3. С. 39–43.

Е. А. Яковлева,
ассистент,
Удмуртский государственный университет

ВЛИЯНИЕ ДОКТРИНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ НА СОЗДАНИЕ ЦИФРОВОЙ ДОВЕРЕННОЙ СРЕДЫ ФЕДЕРАЛЬНОГО ОРГАНА ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

Аннотация. В статье содержится обоснование создания цифровой доверенной среды в федеральном органе исполнительной власти как составной части системы обеспечения информационной безопасности. Раскрываются положительные стороны создания цифровой доверенной среды, а также правовые основания для обеспечения ее безопасности. Анализ положений Доктрины информационной безопасности Российской Федерации показывает основные направления и особенности, которые оказывают непосредственное влияние на создание цифровой доверенной среды федерального органа исполнительной власти.

Ключевые слова: право, цифровая доверенная среда, федеральный орган исполнительной власти, Доктрина, информационная безопасность, защита информации, Интернет, информационные угрозы

INFLUENCE OF THE INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION TO CREATE A DIGITAL TRUSTED ENVIRONMENT OF THE FEDERAL EXECUTIVE AUTHORITY

Abstract. This article contains the rationale for creating a digital trusted environment in the federal executive body as part of the information security system. The positive aspects of creating a digital trusted environment, as well as the legal grounds for ensuring its security, are revealed. Analysis of the provisions of the Doctrine of Information Security of the Russian Federation shows the main directions and features that have a direct impact on the creation of a digital trusted environment of federal executive authority.

Keywords: law, digital trusted environment, federal executive body, Doctrine, information security, information protection, Internet, threats

Сегодня деятельность по обеспечению международной и национальной информационной безопасности в эпоху общемирового информационного общества становится действующим механизмом, обеспечивающим правовой порядок в цифровом пространстве. В этой связи институты государственной власти призваны обеспечивать, поддерживать и следить за незаконной деятельностью в киберпространстве с целью защиты законных интересов, прав и свобод граждан, общества и государства.

В последнее время отмечается повышение угроз безопасности РФ в информационном пространстве, чему способствует стремительное развитие и внедрение информационных технологий во все сферы человеческой жизни и развивающийся цивилизационный кризис. Постоянное увеличение информационных атак в цифровом поле наносит колоссальный ущерб личности, обществу и государству. В связи с чем, с целью недопущения реализации угроз информационной безопасности и эффективного противодействия им была разработана и утверждена Доктрина информационной безопасности РФ [1], которая направлена на осуществление организационно-правовых, экономических, контрразведывательных и других мер по обнаружению, предотвращению и ликвидации внешних и внутренних угроз.

Доктрина информационной безопасности РФ (далее – Доктрина) обязывает государственные органы решать задачи по обеспечению информационной безопасности с помощью организационно-правовых, инженерно-технических, программно-аппаратных и криптографических средств и мер защиты информации, что является противодействием негативным процессам информационной среды, имеющим огромную значимость в достижении национальной безопасности РФ [1].

Система обеспечения информационной безопасности представляет собой «совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность и используемых ими средств обеспечения информационной безопасности» [3]. Совокупность мер по обеспечению безопасности объектов информатизации, сайтов государственных органов в сети Интернет, сетей связи и информационных систем необходимы для защиты в национальном информационном пространстве.

Согласно пункту 9 Доктрины: «Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации» [1]. Цифровая доверенная среда, как мы ранее писали – это «сложившееся, устоявшееся и одновременно защищенное пространство, которое сочетает в себе совокупность правовых механизмов применительно к современным цифровым технологиям, обеспечивающим безопасность циркулирующих данных» [6. С. 7–10]. Приведенное понятие и его дефиниция соответствует понятию «информационная безопасность», исходя из его определения, используемого в Доктрине: «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [1].

Так, цифровая доверенная среда представляет собой информационное пространство, в котором обеспечивается состояние защищенности информации от внешних и внутренних угроз для обеспечения безопасности законных интересов, прав и свобод человека и гражданина, общества и государства, что должно являться неотъемлемой частью ФОИВ для обеспечения безопасности данных, используемых в нем. Безусловно, цифровая доверенная среда имеет ключевое значение не только для обеспечения информационной безопасности, но и для национальной безопасности РФ. Вместе с тем это лежит за пределами настоящего исследования.

Стоит выделить основные этапы создания цифровой доверенной среды:

1. Проанализировать нормативную правовую базу в сфере информационной безопасности и информационных технологий и разработать нормативное и методическое обеспечение;

2. Утвердить концепцию цифровой доверенной среды;

3. Осуществить пилотное внедрение;

4. Модернизировать и интегрировать сервисы цифровой доверенной среды;

5. Ввести в эксплуатацию, по случаю пройденных мероприятий по ее внедрению.

Такой минимальный набор действий по созданию и внедрению цифровой доверенной среды в ФОИВ позволит осуществлять оперативность и контроль за законной деятельностью органов исполнительной власти, с целью ими недопущения нарушения прав граждан.

Положительным моментом влияния Доктрины на создание цифровой доверенной среды федерального органа исполнительной власти является тот факт, что доктрина – это политико-правовой документ, который является элементом законодательной системы РФ и выступает правовым регулятором общественных отношений в сфере информационной безопасности и правоприменительной практики. Следует также отметить, что некоторые положения Доктрины являются нормами права, например, подпункт «а» пункта 34: «законность общественных отношений

в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом» [1] и непосредственно взаимосвязаны с конституционными положениями. Такой принцип прямо пропорционален принципу правового регулирования отношений в сфере информации, информационных технологий и защиты информации Федеральный закон от 27.07.2006 № 149-ФЗ Об информации, информационных технологиях и о защите информации: «свобода поиска, получения, передачи, производства и распространения информации любым законным способом» [5]. Вместе с тем для обеспечения указанных свобод важны и ценностные измерения развития информационного права России [4. С. 53-59].

В заключении стоит отметить, что цифровая доверенная среда федерального органа исполнительной власти – это система, созданная и функционирующая по всем требованиям информационной безопасности, которая наделена специальными условиями для безопасной обработки цифровых данных. Цифровая доверенная среда усиливает эффективность защиты прав и законных интересов граждан, с целью повышения качества услуг в федеральном органе исполнительной власти, за счет чего повышается доверие к государственным структурам.

Таким образом, цифровая доверенная среда осуществляется на основе законодательной, правоприменительной, правоохранительной, судебной форм деятельности государственных органов власти, где основной их задачей является деятельность по обеспечению информационной безопасности.

Созданная и внедренная цифровой доверенной среды в федеральном органе исполнительной власти влечет за собой оперативность и контроль за законной деятельностью органов исполнительной власти, с целью ими недопущения нарушения прав граждан.

Для осуществления данных действий требуется исследование правовых вопросов в данной области в целях осмысления правовой природы цифровой доверенной среды и приоритетных направлений дальнейшего совершенствования информационного законодательства в части обеспечения информационной безопасности.

В качестве основного критерия оценивания зрелости цифровой доверенной среды федерального органа исполнительной власти целесообразно рассматривать совокупность параметров, отражающих соответствие используемых программно-аппаратных, инженерно-технических и иных средств защиты, а также самой системы предъявляемым требованиям.

Таким образом, следует согласиться, что цифровая доверенная среда должна представлять собой сложившееся и устойчивое к внешним и внутренним угрозам цифровое пространство, направленное на защиту объектов информационной среды, в результате функционирования которого закладываются доверительные правоотношения между субъектами информационного взаимодействия, регулируемое совокупностью специальных правовых норм, обеспечивающих информационную безопасность данных цифровой среды и процессов взаимодействия [2].

Список литературы

1. Доктрина информационной безопасности Российской Федерации, утв. Указом Президента РФ от 05.12.2016 № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

2. Камалова Г. Г. Правовые проблемы формирования цифровой доверенной среды // Вызовы информационного общества: тенденции развития правового регулирования цифровых трансформаций: монография по материалам 3.0 международной научно-практической конференции. Саратов, 2022.

3. Козырев С. И. Некоторые аспекты преподавания дисциплины «Информационная безопасность» в разрезе формирования профессиональных качеств специалистов и вызовов современности // Вопросы педагогики. 2022. № 3-1. С. 123–128.

4. Полякова Т. А., Камалова Г. Г. Ценностные изменения развития информационного права России // Правовое государство: теория и практика. 2023. № 2(72). С. 53-59.

5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3448.

6. Яковлева Е. А. Правовые проблемы цифровой доверенной среды // Вестник Удмуртского университета. Серия Экономика и право. 2023. Т. 33, № 1. С. 181–186.

ЭТИЧЕСКИЙ КОДЕКС СУБЪЕКТОВ, ОСУЩЕСТВЛЯЮЩИХ ДЕЯТЕЛЬНОСТЬ ПО СОЗДАНИЮ, ПРИМЕНЕНИЮ И УТИЛИЗАЦИИ МЕДИЦИНСКИХ ИЗДЕЛИЙ НА ОСНОВЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. Вниманию юристов – ученых и практиков, медицинских работников, членов комитетов по клинической этике, специалистов по медицинской этике, представителей правотворческих органов, государственных ведомств, бизнес-сообщества и общественных организаций, пациентов, а также широкого круга читателей, интересующихся вопросами цифровой трансформации системы здравоохранения, предложен первый в Российской Федерации проект Этического кодекса субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе технологий искусственного интеллекта. Принципы, отраженные в Этическом кодексе, могут служить основой для развития системы правового регулирования технологий искусственного интеллекта в здравоохранении.

Ключевые слова: здравоохранение, медицина, медицинская помощь, медицинская услуга, медицинская этика, медицинский работник, медицинское изделие, искусственный интеллект, пациент, право, принцип, производитель, разработчик, цифровые технологии, этика, этический кодекс

ETHICAL CODE OF SUBJECTS, CARRYING OUT ACTIVITIES ON CREATION, APPLICATION AND DISPOSAL MEDICAL DEVICES BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Abstract. To the attention of lawyers, scientists and practitioners, medical professionals, members of clinical ethics committees, medical ethics specialists, representatives of law–making bodies, government departments, the business community and public organizations, patients, as well as a wide range of readers interested in the digital transformation of the healthcare system, the first draft of the Ethical Code of Subjects in the Russian Federation is proposed. carrying out activities for the creation, use and disposal of medical devices based on artificial intelligence technologies. The principles reflected in the Code of Ethics can serve as a basis for the development of a system of legal regulation of artificial intelligence technologies in healthcare.

Keywords: healthcare, medicine, medical care, medical service, medical ethics, medical worker, medical device, artificial intelligence, patient, law, principle, manufacturer, developer, digital technology, ethics, code of ethics

1. Преамбула

Учитывая важную роль цифровых инноваций и технологий в системе здравоохранения и традиционно большое значение этических принципов в медицине, руководствуясь общепризнанными нравственными принципами и нормами медицинского сообщества, документами по медицинской этике и отраслевыми стандартами в сфере классификации, регистрации и сертификации медицинских изделий на основе технологий искусственного интеллекта и правилами контроля качества производства таких изделий, принимается настоящий Этический кодекс субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе технологий искусственного интеллекта (далее – Этический кодекс).

2. Общие положения

2.1. Этический кодекс представляет собой свод общих принципов профессиональной служебной этики и основных правил служебного поведения, которыми должны руководствоваться субъекты, осуществляющие деятельность по созданию, применению и утилизации медицинских изделий на основе технологий искусственного интеллекта [1, 2].

2.2. Целью Этического кодекса является установление этических норм и правил служебного поведения субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе технологий искусственного интеллекта, содействие укреплению авторитета медицинских работников, повышение доверия пациентов к технологиям искусственного интеллекта и предотвращение потенциальных негативных последствий в результате их применения.

2.3. Принципы, указанные в Этическом кодексе, служат основой для развития системы правового регулирования технологий искусственного интеллекта в здравоохранении.

2.4. Медицинские изделия на основе технологий искусственного интеллекта должны разрабатываться, производиться и применяться исключительно в целях оказания медицинской помощи (медицинской услуги) или в научно-исследовательских целях.

2.5. Медицинским работникам запрещено принуждать пациента применять медицинские изделия на основе технологий искусственного интеллекта в отношении него, если это не продиктовано условиями крайней необходимости.

2.6. Медицинские организации должны предоставлять финансовую поддержку для исследований и разработок в области технологий искусственного интеллекта, а также для их внедрения в клиническую практику.

3. Специальные положения

3.1. Этический кодекс не умаляет достоинство и действия кодексов профессиональной этики медицинских работников, а дополняет и раскрывает особенности их деятельности при применении ими медицинских изделий на основе технологий искусственного интеллекта.

3.2. Должностное лицо предприятия, учреждения, организации разработчика (производителя) медицинских изделий на основе технологий искусственного интеллекта обязано ознакомиться с положениями Этического кодекса и соблюдать их в процессе своей профессиональной деятельности.

3.3. Медицинский работник, работающий в медицинской организации, обязан ознакомиться с положениями Этического кодекса и соблюдать их в процессе своей профессиональной деятельности.

3.4. Каждый медицинский работник должен принимать все необходимые меры для соблюдения положений Этического кодекса, а каждый пациент вправе ожидать от него поведения, соответствующего положениям Этического кодекса.

3.5. Знание и соблюдение медицинскими работниками положений Этического кодекса является одним из критериев оценки качества их профессиональной деятельности и служебного поведения.

4. Этические принципы разработчиков и производителей медицинских изделий на основе технологий искусственного интеллекта

4.1. Принцип благополучия

Разработка и производство медицинских изделий на основе технологии искусственного интеллекта должны быть направлены на благо пациентов и общества, а не только интересам бизнеса.

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта должны убедиться, что их продукты обеспечивают клиническую эффективность, повышают качество медицинской помощи (медицинской услуги) и улучшают здоровье пациентов.

4.2. Принцип безопасной разработки

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта должны проводить верификацию всех алгоритмов и моделей искусственного интеллекта, использующихся в медицинском изделии.

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта должны убедиться, что их продукты работают корректно и не могут нанести вреда пациентам и обществу.

4.3. Принцип безопасного внедрения

Внедрение медицинских изделий на основе технологий искусственного интеллекта в клиническую практику должно быть обосновано и основано на доказательной медицине, а также на методах проверки, воспроизводимости и надежности.

4.4. Принцип безопасного применения

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта должны обеспечить качественную установку, настройку, обслуживание и ремонт продуктов на постоянной основе с соблюдением протоколов безопасности.

Документация по безопасному применению медицинских изделий на основе технологий искусственного интеллекта должна быть ясной и доступной.

4.5. Принцип согласованности

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта должны убедиться, что алгоритмы и модели искусственного интеллекта, применяемые в таком изделии, должны быть разработаны таким образом, чтобы они давали единые и последовательные результаты при анализе медицинских данных.

Это позволит медицинским работникам проводить более точный анализ больших объемов данных медицинских исследований и использовать методы

машинного обучения и статистического анализа в целях нахождения закономерностей, которые помогут им диагностировать и лечить заболевания пациентов.

4.6. Принцип алгоритмической прозрачности

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта должны гарантировать, что их продукты разработаны с учетом прозрачности и объяснимости результатов.

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта должны предоставлять медицинским работникам полную информацию о том, как работает их продукт, какие алгоритмы и модели искусственного интеллекта используются в продукте, какие данные были использованы для обучения и как они были обработаны.

4.7. Принцип равенства

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта должны стремиться к тому, чтобы алгоритмы и модели искусственного интеллекта, используемые в продукте, были полностью непредвзятыми и основывались на полных и репрезентативных данных.

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта должны поощрять использование открытых алгоритмов и свободных данных, поскольку они могут дать возможность всем, независимо от их социального статуса или национальности, иметь доступ к надежным и проверенным алгоритмам искусственного интеллекта, способствовать повышению равенства.

4.8. Принцип запрета на дискриминацию

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта во избежание возможной дискриминации на основе религиозных, этнических, культурных, социальных, сексуальных и иных признаков, должны убедиться, что набор данных, используемых для предварительного обучения алгоритмов и моделей искусственного интеллекта, используемых в продукте, является репрезентативным и соответствует разнообразию населения.

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта должны проводить рандомизированные доклинические и клинические исследования (испытания) продукта в целях установления правильности и эффективности используемых алгоритмов и моделей искусственного интеллекта.

4.9. Принцип ответственности

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта должны убедиться в том, что их продукты соответствуют высоким стандартам качества и безопасности, перед тем как предоставлять их на рынок.

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта должны быть готовы взять на себя ответственность за любые проблемы, возникающие из-за некорректного использования продукта.

4.10. Принцип послерегистрационного мониторинга

Производитель медицинских изделий на основе технологий искусственного интеллекта после регистрации продукта и вывода его на рынок должен осуществлять непрерывный мониторинг его работы в целях выявления побочные эффектов или непредвиденные реакции при его применении.

Послерегистрационный мониторинг медицинских изделий на основе технологий искусственного интеллекта осуществляет федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере здравоохранения.

4.11. Принцип подконтрольности

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта должны осуществлять строгий контроль выведенных на рынок продуктов на соответствие требованиям безопасности, надежности и эффективности.

В ходе испытаний медицинских изделий на основе технологий искусственного интеллекта не должны создаваться условия, которые могут угрожать жизни и здоровью человека.

5. Этические принципы медицинских работников по применению медицинских изделий на основе технологий искусственного интеллекта

5.1. Принцип созидания и улучшения качества

Медицинские работники должны применять медицинские изделия на основе технологий искусственного интеллекта исключительно в целях оказания медицинской помощи (медицинской услуги).

Применение медицинских изделий на основе технологий искусственного интеллекта может значительно улучшить качество медицинской помощи (медицинской услуги), ускорить процесс медицинского обследования или помочь в выборе наилучшего метода лечения для пациента.

5.2. Принцип безопасности

Применение медицинских изделий на основе технологий искусственного интеллекта должно быть надежным и безопасным, а получаемые на их основе результаты не должны быть направлены на причинение вреда жизни и здоровью пациентам.

Медицинские работники должны обеспечить создание прозрачной системы доклинических и клинических исследований (испытаний), которые гарантируют соответствие таких изделий высоким стандартам качества и безопасности.

5.3. Принцип запрета на полную автоматизацию

Решение, принятое медицинским работником, сформированное на данных медицинского изделия на основе технологий искусственного интеллекта, не должно противоречить стандартами оказания медицинской помощи и не может быть единственным основанием для полностью автоматической постановки диагноза, назначения лечения и проведения медицинского обследования.

Алгоритмы и модели искусственного интеллекта, использующиеся в медицинском изделии, могут применяться для помощи медицинским работникам в принятии точных диагностических и лечебных решений, однако окончательное решение всегда принимает медицинский работник, основываясь на своих знаниях, опыте и суждениях.

5.4. Принцип добровольного информированного согласия

Медицинские работники должны извещать пациентов обо всех аспектах их медицинского обследования и лечения, включая возможное применение медицинского изделия на основе технологий искусственного интеллекта, с их согласия.

Согласие на применение медицинских изделий на основе технологий искусственного интеллекта должно быть добровольным.

Пациент должен быть извещен о том, какие медицинские изделия на основе технологий искусственного интеллекта будут применяться в его медицинском обследовании и лечении, как они работают, какие преимущества и риски они представляют, а также как они будут влиять на его здоровье и общее состояние.

5.5. Принцип квалификации медицинских работников

Медицинские работники должны знать и соблюдать действующие нормативные правовые акты, регулирующие их профессиональную деятельность, должны быть обучены применению медицинских изделий на основе технологий искусственного интеллекта, знать стандарты оказания медицинской помощи с применением медицинских изделий на основе технологий искусственного интеллекта.

Медицинские работники имеют право на профессиональную подготовку или повышение квалификации по программам «Применение медицинских изделий на основе технологий искусственного интеллекта» в системе непрерывного медицинского образования на бесплатной основе.

5.6. Принцип хранения и защиты данных

Медицинские работники должны хранить персональные данные пациентов в базе данных с учетом требований информационной безопасности.

5.7. Принцип конфиденциальности данных

Медицинские работники должны известить пациентов о том, что их персональные данные собираются и обрабатываются.

Сведения о факте обращения пациента за оказанием ему медицинской помощи (медицинской услуги) с применением медицинских изделий на основе технологий искусственного интеллекта, состоянии его здоровья и диагнозе, иные сведения, полученные при высокотехнологическом медицинском вмешательстве, составляют врачебную тайну.

5.8. Принцип соответствия

Медицинские изделия на основе технологий искусственного интеллекта должны соответствовать действующим стандартам оказания медицинской помощи.

5.9. Принцип защиты прав пациентов

Пациент имеет право на защиту своих прав и интересов при применении в отношении него медицинских изделий на основе технологий искусственного интеллекта.

Медицинские работники должны извещать пациентов о том, какие медицинские изделия на основе технологий искусственного интеллекта используются в их медицинском обследовании и лечении и какие побочные эффекты или непредвиденные реакции при его применении возможны.

При применении медицинских изделий на основе технологий искусственного интеллекта необходимо минимизировать риски возможных негативных последствий для пациентов.

5.10. Принцип защиты прав медицинских работников

Медицинский работник имеет право на защиту своих прав и интересов при применении медицинских изделий на основе технологий искусственного интеллекта в отношении пациентов.

При применении медицинских изделий на основе технологий искусственного интеллекта необходимо минимизировать риски возможных негативных последствий для медицинских работников.

5.11. Принцип эмпатии

Медицинские работники должны проявлять сочувствие и понимание к пациентам, учитывать интерес к их психологическому и эмоциональному состоянию при предоставлении медицинской помощи (медицинской услуги) с применением медицинских изделий на основе технологий искусственного интеллекта.

5.12. Принцип алгоритмической прозрачности

Медицинские работники должны понимать, как медицинское изделие на основе технологий искусственного интеллекта сгенерировало рекомендацию для медицинского обследования и лечения пациента.

Список литературы

1. Шутова А. А., Бегишев И. Р. Инициативный проект Этического кодекса субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе технологий искусственного интеллекта: препринт № 1 за 2023 г. / А. А. Шутова, И. Р. Бегишев. Казань : Изд-во «Познание» Казанского инновационного университета, 2023. 16 с. DOI: 10.21202/978-5-8399-0803-1_2023_1_16

2. Шутова А. А., Бегишев И. Р. Проект Этического кодекса субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе технологий искусственного интеллекта // Russian Journal of Economics and Law. 2023. Т. 17, № 4. С. 750–785.

Разработан: **А. А. Шутова**, кандидат юридических наук, Казанский инновационный университет имени В. Г. Тимирясова; **И. Р. Бегишев**, доктор юридических наук, доцент, Казанский инновационный университет имени В. Г. Тимирясова.

ЭТИЧЕСКИЙ КОДЕКС СУБЪЕКТОВ, ОСУЩЕСТВЛЯЮЩИХ ДЕЯТЕЛЬНОСТЬ ПО СОЗДАНИЮ, ПРИМЕНЕНИЮ И УТИЛИЗАЦИИ МЕДИЦИНСКИХ ИЗДЕЛИЙ НА ОСНОВЕ ТЕХНОЛОГИЙ РОБОТОТЕХНИКИ

Аннотация. Вниманию юристов – ученых и практиков, медицинских работников, членов комитетов по клинической этике, специалистов по медицинской этике, представителей правотворческих органов, государственных ведомств, бизнес-сообщества и общественных организаций, пациентов, а также широкого круга читателей, интересующихся вопросами цифровой трансформации системы здравоохранения, предложен первый в Российской Федерации проект Этического кодекса субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе технологий робототехники. Принципы, отраженные в Этическом кодексе, могут служить основой для развития системы правового регулирования технологий робототехники в здравоохранении.

Ключевые слова: здравоохранение, медицина, медицинская помощь, медицинская услуга, медицинская этика, медицинский работник, медицинская робототехника, медицинское изделие, медицинский робот, робототехника, искусственный интеллект, пациент, право, принцип, производитель, разработчик, цифровые технологии, этика, этический кодекс

ETHICAL CODE OF SUBJECTS, CARRYING OUT ACTIVITIES ON CREATION, APPLICATION AND DISPOSAL MEDICAL DEVICES BASED ON ROBOTICS TECHNOLOGIES

Abstract. To the attention of lawyers, scientists and practitioners, medical professionals, members of clinical ethics committees, medical ethics specialists, representatives of law–making bodies, government departments, the business community and public organizations, patients, as well as a wide range of readers interested in the digital transformation of the healthcare system, the first draft of the Ethical Code of Subjects in the Russian Federation is proposed. Carrying out activities for the creation, use and disposal of medical devices based on robotics technologies. The principles reflected in the Code of Ethics can serve as a basis for the development of a system of legal regulation of robotics technologies in healthcare.

Keywords: healthcare, medicine, medical care, medical service, medical ethics, medical worker, medical robotics, medical device, medical robot, robotics, artificial intelligence, patient, law, principle, manufacturer, developer, digital technologies, ethics, code of ethics

1. Преамбула

Учитывая важную роль цифровых инноваций и технологий в системе здравоохранения и традиционно большое значение этических принципов в медицине, руководствуясь общепризнанными нравственными принципами и нормами медицинского сообщества, документами по медицинской этике и отраслевыми стандартами в сфере классификации, регистрации и сертификации медицинских изделий на основе технологий робототехники и правилами контроля качества производства таких изделий, принимается настоящий Этический кодекс субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе технологий робототехники (далее – Этический кодекс).

2. Общие положения

2.1. Этический кодекс представляет собой свод общих принципов профессиональной служебной этики и основных правил служебного поведения, которыми должны руководствоваться субъекты, осуществляющие деятельность по созданию, применению и утилизации медицинских изделий на основе технологий робототехники [1].

2.2. Целью Этического кодекса является установление этических норм и правил служебного поведения субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе технологий робототехники, содействие укреплению авторитета медицинских работников, повышение доверия пациентов к технологиям робототехники и предотвращение потенциальных негативных последствий в результате их применения.

2.3. Принципы, указанные в Этическом кодексе, служат основой для развития системы правового регулирования технологий робототехники в здравоохранении.

2.4. Медицинские изделия на основе технологий робототехники должны разрабатываться, производиться и применяться исключительно в целях оказания медицинской помощи (медицинской услуги) или в научно-исследовательских целях.

2.5. Медицинским работникам запрещено принуждать пациента применять медицинские изделия на основе технологий робототехники в отношении него, если это не продиктовано условиями крайней необходимости.

2.6. Медицинские изделия на основе технологий робототехники не должны использоваться для придания человеку новых способностей, влекущих ограничение конкуренции.

2.7. Медицинские организации должны предоставлять финансовую поддержку для исследований и разработок в области технологий робототехники, а также для их внедрения в клиническую практику.

3. Специальные положения

3.1. Этический кодекс не умаляет достоинство и действия кодексов профессиональной этики медицинских работников, а дополняет и раскрывает особенности их деятельности при применении ими медицинских изделий на основе технологий робототехники.

3.2. Должностное лицо предприятия, учреждения, организации разработчика (производителя) медицинских изделий на основе технологий робототехники обязано ознакомиться с положениями Этического кодекса и соблюдать их в процессе своей профессиональной деятельности.

3.3. Медицинский работник, работающий в медицинской организации, обязан ознакомиться с положениями Этического кодекса и соблюдать их в процессе своей профессиональной деятельности.

3.4. Каждый медицинский работник должен принимать все необходимые меры для соблюдения положений Этического кодекса, а каждый пациент вправе ожидать от него поведения, соответствующего положениям Этического кодекса.

3.5. Знание и соблюдение медицинскими работниками положений Этического кодекса является одним из критериев оценки качества их профессиональной деятельности и служебного поведения.

4. Этические принципы разработчиков и производителей медицинских изделий на основе технологий робототехники

4.1. Принцип благополучия

Разработка и производство медицинских изделий на основе технологии робототехники должны быть направлены на благо пациентов и общества, а не только интересы бизнеса.

Разработчики и производители медицинских изделий на основе технологий робототехники должны убедиться, что их продукты обеспечивают клиническую эффективность, повышают качество медицинской помощи (медицинской услуги) и улучшают здоровье пациентов.

4.2. Принцип ответственности

Разработчики и производители медицинских изделий на основе технологий робототехники должны убедиться в том, что их продукты соответствуют высоким стандартам качества и безопасности, перед тем как предоставлять их на рынок.

Разработчики и производители медицинских изделий на основе технологий искусственного интеллекта должны быть готовы взять на себя ответственность за любые проблемы, возникающие из-за некорректного использования продукта.

4.3. Принцип алгоритмической прозрачности

Разработчики и производители медицинских изделий на основе технологий робототехники должны гарантировать, что их продукты разработаны с учетом прозрачности и объяснимости результатов.

Разработчики и производители медицинских изделий на основе технологий робототехники должны предоставлять медицинским работникам полную информацию о том, как работает их продукт и какие результаты стоит от него ожидать.

4.4. Принцип безопасной разработки

Разработчики и производители медицинских изделий на основе технологий робототехники должны убедиться, что их продукты работают корректно и не могут нанести вреда пациентам и обществу.

4.5. Принцип безопасного внедрения

Внедрение медицинских изделий на основе технологий робототехники в клиническую практику должно быть обосновано и основано на доказательной медицине, а также на методах проверки, воспроизводимости и надежности.

4.6. Принцип безопасного применения

Разработчики и производители медицинских изделий на основе технологий робототехники должны обеспечить качественную установку, настройку, обслуживание и ремонт продуктов на постоянной основе с соблюдением протоколов безопасности.

Документация по безопасному применению медицинских изделий на основе технологий робототехники должна быть ясной и доступной.

4.7. Принцип оценки рисков информационной безопасности

Разработчики и производители медицинских изделий на основе технологий робототехники должны обеспечить оценку рисков информационной безопасности продукта в целях прогнозирования возникновения возможных угроз информационной безопасности продукта и выработки мер по повышению устойчивости его функционирования при проведении в отношении них компьютерных атак.

4.8. Принцип обеспечения информационной безопасности

Разработчики и производители медицинских изделий на основе технологий робототехники должны обеспечить защищенность компьютерной программы продукта средствами, обеспечивающих их устойчивое функционирование при проведении в отношении них компьютерных атак.

Разработчики и производители медицинских изделий на основе технологий робототехники должны обеспечить готовность к обнаружению, предупреждению и ликвидации последствий компьютерных атак.

4.9. Принцип оценки рисков технологической безопасности

Разработчики и производители медицинских изделий на основе технологий робототехники должны обеспечить оценку рисков технологической безопасности продукта в целях прогнозирования возникновения возможных угроз технологической безопасности продукта и выработки мер по повышению устойчивости его функционирования при авариях и последствиях указанных аварий.

4.10. Принцип обеспечения технологической безопасности

Разработчики и производители медицинских изделий на основе технологий робототехники должны обеспечить защищенность механической части продукта от аварий и последствий указанных аварий, обеспечивающее их устойчивое функционирование.

Разработчики и производители медицинских изделий на основе технологий робототехники должны обеспечить готовность к обнаружению, предупреждению и ликвидации последствий аварий.

4.11. Принцип послерегистрационного мониторинга

Производитель медицинских изделий на основе технологий робототехники после регистрации продукта и вывода его на рынок должен осуществлять непрерывный мониторинг его работы в целях выявления побочных эффектов или непредвиденных реакции при его применении.

Послерегистрационный мониторинг медицинских изделий на основе технологий робототехники осуществляет федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере здравоохранения.

4.12. Принцип подконтрольности

Разработчики и производители медицинских изделий на основе технологий робототехники должны осуществлять строгий контроль выведенных на рынок продуктов на соответствие требованиям безопасности, надежности и эффективности.

В ходе испытаний медицинских изделий на основе технологий робототехники не должны создаваться условия, которые могут угрожать жизни и здоровью людей.

5. Этические принципы медицинских работников по применению медицинских изделий на основе технологий робототехники

5.1. Принцип созидания и улучшения качества

Медицинские работники должны применять медицинские изделия на основе технологий робототехники исключительно в целях оказания медицинской помощи (медицинской услуги).

Применение медицинских изделий на основе технологий робототехники может значительно улучшить качество медицинской помощи (медицинской услуги).

5.2. Принцип безопасности

Применение медицинских изделий на основе технологий робототехники должно быть надежным и безопасным, а получаемые на их основе результаты не должны быть направлены на причинение вреда жизни и здоровью пациентам.

Медицинские работники должны обеспечить создание прозрачной системы доклинических и клинических исследований (испытаний), которые гарантируют соответствие таких изделий высоким стандартам качества и безопасности. 5.3. Принцип запрета на полную автоматизацию

Медицинские изделия на основе технологий робототехники должны применяться в качестве помощи медицинским работникам, а не заменять их.

Медицинский работник в любой момент должен отказаться от применения медицинских изделий на основе технологий робототехники, если это стало противоречить целям оказания медицинской помощи.

5.4. Принцип добровольного информированного согласия

Медицинские работники должны извещать пациентов обо всех аспектах их медицинского обследования и лечения, включая возможное применение медицинского изделия на основе технологий искусственного интеллекта, с их согласия.

Согласие на использование медицинских изделий на основе технологий робототехники должно быть добровольным.

Пациент должен быть извещен о том, какие медицинские изделия на основе технологий робототехники будут применяться в его медицинском обследовании и лечении, как они работают, какие преимущества и риски они представляют, а также как они будут влиять на его здоровье и общее состояние.

5.5. Принцип квалификации медицинских работников

Медицинские работники должны знать и соблюдать действующие нормативные правовые акты, регулирующие их профессиональную деятельность, должны быть обучены применению медицинских изделий на основе технологий робототехники, знать стандарты оказания медицинской помощи с применением медицинских изделий на основе технологий робототехники.

Медицинские работники имеют право на профессиональную подготовку или повышение квалификации по программам «Применение медицинских изделий на основе технологий робототехники» в системе непрерывного медицинского образования на бесплатной основе.

5.6. Принцип хранения и защиты данных

Медицинские работники должны хранить персональные данные пациентов в базе данных с учетом требований информационной безопасности.

5.7. Принцип конфиденциальности данных

Медицинские работники должны известить пациентов о том, что их персональные данные собираются и обрабатываются.

Сведения о факте обращения пациента за оказанием ему медицинской помощи (медицинской услуги) с применением медицинских изделий на основе технологий робототехники, состоянии его здоровья и диагнозе, иные сведения, полученные при высокотехнологическом медицинском вмешательстве, составляют врачебную тайну.

5.8. Принцип соответствия

Медицинские изделия на основе технологий робототехники должны соответствовать действующим стандартам оказания медицинской помощи.

5.9. Принцип защиты прав пациентов

Пациент имеет право на защиту своих прав и интересов при применении в отношении него медицинских изделий на основе технологий робототехники.

Медицинские работники должны извещать пациентов о том, какие медицинские изделия на основе технологий робототехники используются в их медицинском обследовании и лечении и какие побочные эффекты или непредвиденные реакции при их применении возможны.

При применении медицинских изделий на основе технологий робототехники необходимо минимизировать риски возможных негативных последствий для пациентов.

5.10. Принцип защиты прав медицинских работников

Медицинский работник имеет право на защиту своих прав и интересов при применении медицинских изделий на основе технологий робототехники в отношении пациентов.

При применении медицинских изделий на основе технологий робототехники необходимо минимизировать риски возможных негативных последствий для медицинских работников.

5.11. Принцип эмпатии

Медицинские работники должны проявлять сочувствие и понимание к пациентам, учитывать интерес к их психологическому и эмоциональному состоянию при предоставлении медицинской помощи (медицинской услуги) с применением медицинских изделий на основе технологий робототехники.

5.12. Принцип смены парадигмы

Применение медицинских изделий на основе технологий робототехники не должно приводить к замене отношений «врач-пациент» отношениями «медицинский робот-пациент».

5.12. Принцип алгоритмической прозрачности

Медицинские работники должны понимать, как медицинское изделие на основе технологий робототехники оказало помощь в медицинском обследовании и лечении пациента.

6. Этические принципы субъектов, осуществляющих деятельность по утилизации медицинских изделий на основе технологий робототехники

6.1. Принцип естественной утилизации

Медицинские изделия на основе технологий робототехники с истекшими сроками годности должны быть утилизированы.

В этом случае должно быть организовано уничтожение персональных данных пациентов и иной служебной информации, обращавшейся в медицинском изделии на основе технологий робототехники.

6.2. Принцип специальной утилизации

Медицинские изделия на основе технологий робототехники, с истекшими сроками годности, могут быть использованы в научных и образовательных целях, не связанных с оказанием медицинской помощи (медицинской услуги).

В этом случае должно быть организовано обезличивание персональных данных пациентов, обращавшихся в медицинском изделии на основе технологий робототехники.

Список литературы

1. Шутова А. А., Бегишев И. Р. Инициативный проект Этического кодекса субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе технологий искусственного интеллекта: препринт № 2 за 2023 г. Казань : Изд-во «Познание» Казанского инновационного университета, 2023. 15 с. DOI: 10.21202/978-5-8399-0803-1_2023_2_15

Разработан: **А. А. Шутова**, кандидат юридических наук, Казанский инновационный университет имени В. Г. Тимирясова; **И. Р. Бегишев**, доктор юридических наук, доцент, Казанский инновационный университет имени В. Г. Тимирясова.

ЭТИЧЕСКИЙ КОДЕКС СУБЪЕКТОВ, ОСУЩЕСТВЛЯЮЩИХ ДЕЯТЕЛЬНОСТЬ ПО СОЗДАНИЮ, ПРИМЕНЕНИЮ И УТИЛИЗАЦИИ МЕДИЦИНСКИХ ИЗДЕЛИЙ НА ОСНОВЕ БИОПРИНТНЫХ ТЕХНОЛОГИЙ, ПО ВЗАИМОДЕЙСТВИЮ С ПАЦИЕНТАМИ И ДОНОРАМИ КЛЕТОК, ПО ОБОРОТУ ДОНОРСКИХ КЛЕТОК, БИОЧЕРНИЛ И БИОПРИНТНЫХ ТКАНЕВЫХ (ОРГАННЫХ) КОНСТРУКТОВ

Аннотация. Вниманию юристов – ученых и практиков, медицинских работников, членов комитетов по клинической этике, специалистов по медицинской этике, представителей правотворческих органов, государственных ведомств, бизнес-сообщества и общественных организаций, пациентов, а также широкого круга читателей, интересующихся вопросами цифровой трансформации системы здравоохранения, предложен первый в Российской Федерации проект Этического кодекса субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе биопринтных технологий, по взаимодействия с пациентами и донорами клеток, по обороту донорских клеток, биочернил и биопринтных тканевых (органных) конструктов. Принципы, отраженные в Этическом кодексе, могут служить основой для развития системы правового регулирования биопринтных технологий.

Ключевые слова: 3D-биопечать, 3D-биопринтер, биопринтная ткань, биопринтные технологии, биопринтный орган, биочернила, донор, здравоохранение, клетка, конструкт, медицина, медицинская помощь, медицинская услуга, медицинская этика, медицинский работник, медицинское изделие, пациент, право, принцип, производитель, процедура, разработчик, цифровые технологии, этика, этический кодекс

ETHICAL CODE OF SUBJECTS, CARRYING OUT ACTIVITIES ON THE CREATION, APPLICATION AND DISPOSAL OF MEDICAL DEVICES BASED ON BIOPRINT TECHNOLOGIES, ON INTERACTION WITH PATIENTS AND CELL DONORS, ACCORDING TO THE TURNOVER OF DONOR CELLS, BIOCHERNILS AND BIOPRINTED TISSUE (ORGAN) CONSTRUCTS

Abstract. Attention of lawyers – scientists and practitioners, medical professionals, members of clinical ethics committees, medical ethics specialists, representatives of law-making bodies, government departments, the business community and public organizations, patients, as well as a wide range of readers interested in the digital transformation of the healthcare system, the first draft of the Ethical Code of subjects engaged in the activities of the Russian Federation has been proposed. creation, application and disposal of medical devices based on bioprint technologies, interaction with patients and cell donors, according to the turnover of donor cells, biochernils and bioprinted tissue (organ) constructs. The principles reflected in the Code of Ethics can serve as a basis for the development of a system of legal regulation of bioprint technologies.

Keywords: 3D-bioprinting, 3D-bioprinter, bioprinting tissue, bioprinting technologies, bioprinting organ, bio-ink, donor, healthcare, cell, construct, medicine, medical care, medical service, medical ethics, medical worker, medical device, patient, law, principle, manufacturer, procedure, developer, digital technologies, ethics, code of ethics

1. Преамбула

Учитывая важную роль медицинских инноваций и цифровых технологий в системе здравоохранения и традиционно большое значение этических принципов в медицине, руководствуясь общепризнанными нравственными принципами и нормами медицинского сообщества, документами по медицинской этике и отраслевыми стандартами в сфере классификации, регистрации и сертификации медицинских изделий на основе биопринтных технологий и правилами контроля качества производства таких изделий, принимается настоящий Этический кодекс субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе биопринтных технологий, по взаимодействию с пациентами и донорами клеток, по обороту донорских клеток, биочернил и биопринтных тканевых (органных) конструктов (далее – Этический кодекс).

2. Основные понятия

2.1. Биопринтные технологии – совокупность методов разработки и производства тканевых (органных) конструктов на основе биочернил с использованием 3D-биопринтера.

2.2. Биопринтные тканевые (органные) конструкты – ткань или орган, созданные посредством использования биопринтной технологии и предназначенные для замены больной либо несостоятельной части тела человека (животного).

2.3. Биочернила – смесь, состоящая из донорских клеток и синтетических субстанций, имитирующих внеклеточный матрикс, используемая для производства тканевых (органных) конструктов.

2.4. Донорская клетка – элементарная система, способная к размножению и взаимодействию с синтетическими субстанциями для производства биочернил, полученная от живого донора, трупа или животного.

3. Общие положения

3.1. Этический кодекс представляет собой свод общих принципов профессиональной служебной этики и основных правил служебного поведения, которыми должны руководствоваться субъекты, осуществляющие деятельность по созданию, применению и утилизации медицинских изделий на основе биопринтных технологий, по взаимодействию с пациентами и донорами клеток, по обороту донорских клеток, биочернил и биопринтных тканевых (органных) конструктов [1].

3.2. Целью Этического кодекса является установление этических норм и правил служебного поведения субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе биопринтных технологий, по взаимодействию с пациентами и донорами клеток, по обороту донорских клеток, биочернил и биопринтных тканевых (органных) конструктов, содействие укреплению авторитета медицинских работников, повышение доверия

пациентов к биопринтным технологиям и предотвращение потенциальных негативных последствий в результате их применения.

3.3. Принципы, указанные в Этическом кодексе, служат основой для развития системы правового регулирования биопринтных технологий.

3.4. Медицинские изделия на основе биопринтных технологий должны разрабатываться, производиться и применяться исключительно в целях оказания медицинской помощи (медицинской услуги) или в научно-исследовательских целях.

3.5. Медицинским работникам запрещено принуждать пациента применять медицинские изделия на основе биопринтных технологий в отношении него, если это не продиктовано условиями крайней необходимости.

3.6. Медицинские работники должны сокращать количество доклинических и клинических исследований (испытаний) на животных.

3.7. Медицинские организации должны предоставлять финансовую поддержку для исследований и разработок в области биопринтных технологий, а также для их внедрения в клиническую практику.

4. Специальные положения

4.1. Этический кодекс не умаляет достоинство и действия кодексов профессиональной этики медицинских работников, а дополняет и раскрывает особенности их деятельности при применении ими медицинских изделий на основе биопринтных технологий.

4.2. Должностное лицо предприятия, учреждения, организации разработчика (производителя) медицинских изделий на основе биопринтных технологий обязано ознакомиться с положениями Этического кодекса и соблюдать их в процессе своей профессиональной деятельности.

4.3. Медицинский работник, работающий в медицинской организации, обязан ознакомиться с Этическим кодексом и соблюдать его в процессе своей профессиональной деятельности.

4.4. Каждый медицинский работник должен принимать все необходимые меры для соблюдения положений Этического кодекса, а каждый пациент и донор клеток вправе ожидать от него поведения, соответствующего положениям Этического кодекса.

4.5. Знание и соблюдение медицинскими работниками положений Этического кодекса является одним из критериев оценки качества их профессиональной деятельности и служебного поведения.

5. Этические принципы оборота донорских клеток

5.1. Принцип взятия клеток

Медицинские работники должны организовать процедуру взятия донорских клеток в соответствии со стандартами оказания медицинской помощи (медицинской услуги).

5.2. Принцип качества

Медицинские работники должны осуществлять исследование качества донорских клеток на жизнеспособность и способность к размножению.

5.3. Принцип тестирования

Медицинские работники должны осуществлять тестирование донорских клеток на наличие вирусной, бактериальной, протозойной, грибковой и прионной инфекции.

5.4. Принцип биохранения

Медицинские работники должны обеспечить безопасное хранение донорских клеток в биобанке.

5.5. Принцип транспортировки

Медицинские работники должны обеспечить безопасную транспортировку донорских клеток.

5.6. Принцип клинической эффективности

Медицинские работники должны обеспечить клиническую эффективность применения донорских клеток.

5.7. Принцип объекта гражданских прав

Донорские клетки, взятые для производства биопринтных тканевых (органных) конструктов, являются объектами гражданских прав.

6. Этические принципы оборота биочернил

6.1. Принцип разработки

Медицинские работники должны организовать процедуру разработки биочернил в соответствии со стандартами оказания медицинской помощи (медицинской услуги).

6.2. Принцип применения

Медицинские работники должны организовать процедуру применения биочернил в соответствии со стандартами оказания медицинской помощи (медицинской услуги).

6.3. Принцип качества

Медицинские работники должны осуществлять исследование качества биочернил на жизнеспособность.

6.4. Принцип тестирования

Медицинские работники должны осуществлять тестирование биочернил на наличие вирусной, бактериальной, протозойной, грибковой и прионной инфекции.

6.5. Принцип биохранения

Медицинские работники должны обеспечить безопасное хранение биочернил в биобанке.

6.6. Принцип транспортировки

Медицинские работники должны обеспечить безопасную транспортировку биочернил.

6.7. Принцип клинической эффективности

Медицинские работники должны обеспечить клиническую эффективность применения биочернил.

6.8. Принцип объекта гражданских прав

Биочернила являются объектами гражданских прав.

7. Этические принципы оборота биопринтных тканевых (органных) конструктов

7.1. Принцип доклинических исследований (испытаний)

Медицинские работники должны организовать процедуру доклинических исследований (испытаний) биопринтных тканевых (органных) конструктов в соответствии со стандартами оказания медицинской помощи (медицинской услуги).

7.2. Принцип клинических исследований (испытаний)

Медицинские работники должны организовать процедуру клинических исследований (испытаний) биопринтных тканевых (органных) конструктов в соответствии со стандартами оказания медицинской помощи (медицинской услуги).

7.3. Принцип трансплантации

Медицинские работники должны организовать процедуру трансплантации биопринтных тканевых (органных) конструктов в соответствии со стандартами оказания медицинской помощи (медицинской услуги).

7.4. Принцип качества

Медицинские работники должны осуществлять исследование качества биопринтных тканевых (органных) конструктов на жизнеспособность и способность к трансплантации.

7.5. Принцип тестирования

Медицинские работники должны осуществлять тестирование биопринтных тканевых (органных) конструктов на наличие вирусной, бактериальной, протозойной, грибковой и прионной инфекции.

7.6. Принцип биохранения

Медицинские работники должны обеспечить безопасное хранение биопринтных тканевых (органных) конструктов в биобанке.

7.7. Принцип транспортировки

Медицинские работники должны обеспечить безопасную транспортировку биопринтных тканевых (органных) конструктов.

7.8. Принцип клинической эффективности

Медицинские работники должны обеспечить клиническую эффективность применения биопринтных тканевых (органных) конструктов.

7.9. Принцип переносимости

Медицинские работники должны учитывать переносимость трансплантируемых в организм пациента биопринтных тканевых (органных) конструктов.

7.10. Принцип доступности результатов исследований (испытаний)

Результаты доклинических и клинических исследований (испытаний) биопринтных тканевых (органных) конструктов подлежат обязательному опубликованию в научных журналах.

7.11. Принцип доступности результатов трансплантации

Результаты трансплантации биопринтных тканевых (органных) конструктов подлежат обязательному опубликованию в научных журналах.

7.12. Принцип объектов гражданских прав

Биопринтные тканевые (органные) конструкты до завершения процедуры трансплантации являются объектами гражданских прав.

8. Этические принципы взаимодействия с донорами клеток

8.1. Принцип анамнеза

Медицинские работники перед назначением процедуры выбора донора клеток должны исследовать его здоровье и изучить анамнез донора.

8.2. Принцип добровольного донорства

Процедура взятия клеток у донора осуществляется на добровольной основе.

Добровольное донорство клеток возможно за плату.

8.3. Принцип запрета на принуждение

Запрещено оказывать давление на донора для получения его клеток в целях производства биочернил, угрозы применения к нему насилия, убийства, иные формы принуждения, влекущие уголовную ответственность в соответствии с законодательством Российской Федерации.

8.4. Принцип этического соответствия

Медицинские работники в процессе процедуры выбора донора клеток должны учитывать его религиозные, культурные и социальные убеждения.

8.5. Принцип генетического соответствия

Медицинские работники в процессе процедуры выбора донора клеток должны учитывать генетические заболевания донора клеток и его родственников.

8.6. Принцип наследственного соответствия

Медицинские работники в процессе процедуры выбора донора клеток должны учитывать наследственные заболевания донора клеток и его родственников.

8.7. Принцип гистосовместимости

Медицинские работники перед назначением процедуры выбора донора клеток должны осуществлять тестирование на гистосовместимость.

8.8. Принцип биологической совместимости

Медицинские работники перед назначением процедуры выбора донора клеток должны осуществлять тестирование на биологическую совместимость.

8.9. Принцип инфекционной реакции

Медицинские работники должны устранять риски, связанные с введением вирусной, бактериальной, протозойной, грибковой и прионной инфекции в организм донора клеток.

8.10. Принцип иммунологической реакции

Медицинские работники должны устранять риски, связанные с иммунологической реакцией и иммунным ответом организма донора клеток.

8.11. Принцип аллергической реакции

Медицинские работники должны устранять риски, связанные с аллергической реакцией организма донора клеток.

8.12. Принцип информированного согласия

Донор клеток должен быть извещен об осуществлении в отношении него процедуры взятии донорских клеток, о возможных побочных эффектах и непредвиденных реакциях.

Донор клеток должны быть извещен о том, каким образом и в каких целях будут использованы его донорские клетки.

Процедура взятия донорских клеток допускается при наличии информированного согласия донора.

8.13. Принцип защиты прав и интересов

Донор клеток имеет право на защиту своих прав и интересов при осуществлении процедуры взятии донорских клеток.

8.14. Принцип хранения и защиты данных

Медицинские работники должны хранить персональные данные доноров клеток в базе данных с учетом требований информационной безопасности.

8.15. Принцип конфиденциальности данных

Медицинские работники должны известить доноров клеток о том, что их персональные данные собираются и обрабатываются.

Сведения о донорах клеток, состоянии их здоровья, иные сведения, полученные в ходе процедуры взятия клеток у донора, составляют врачебную тайну.

8.16. Принцип пропаганды донорства

Медицинские работники должны осуществлять пропаганду донорства на постоянной основе в целях привлечения потенциальных доноров к сдаче клеток.

9. Этические принципы взаимодействия с пациентами

9.1. Принцип анамнеза

Медицинские работники перед назначением процедуры трансплантации биопринтных тканевых (органных) конструктов должны исследовать здоровье и изучить анамнез пациента.

9.2. Принцип сохранения здоровья пациента

Пациенты могут являться донорами своих клеток для последующего производства биопринтных тканевых (органных) конструктов, если им не установлен запрет по медицинским показаниям.

9.3. Принцип этического соответствия

Медицинские работники в процессе процедуры выбора донора клеток должны учитывать религиозные, культурные или социальные убеждения пациента.

9.4. Принцип генетического соответствия

Пациент должен быть извещен о наличии генетических заболеваний у донора клеток и его родственников.

9.5. Принцип наследственного соответствия

Пациент должен быть извещен о наличии наследственных заболеваний у донора клеток и его родственников.

9.6. Принцип гистосовместимости

Медицинские работники перед назначением процедуры трансплантации биопринтных тканевых (органных) конструктов должны осуществлять тестирование на гистосовместимость.

9.7. Принцип биологической совместимости

Медицинские работники перед назначением процедуры трансплантации биопринтных тканевых (органных) конструктов должны осуществлять тестирование на биологическую совместимость.

9.8. Принцип инфекционной реакции

Медицинские работники должны устранять риски, связанные с введением вирусной, бактериальной, протозойной, грибковой и прионной инфекции в организм пациента.

9.9. Принцип иммунологической реакции

Медицинские работники должны устранять риски, связанные с иммунологической реакцией и иммунным ответом организма пациента.

9.10. Принцип аллергической реакции

Медицинские работники должны устранять риски, связанные с аллергической реакцией организма пациента.

9.11. Принцип информированного согласия

Пациент должен быть извещен о применении в отношении него медицинских изделий на основе биопринтных технологий, о возможных побочных эффектах и непредвиденных реакциях.

Процедура трансплантации биопринтных тканевых (органных) конструктов допускается при наличии информированного согласия пациента.

9.12. Принцип защиты прав и интересов

Пациент имеет право на защиту своих прав и интересов при применении в отношении него медицинских изделий на основе биопринтных технологий.

9.13. Принцип хранения и защиты данных

Медицинские работники должны хранить персональные данные пациентов в базе данных с учетом требований информационной безопасности.

9.14. Принцип конфиденциальности данных

Медицинские работники должны известить пациентов о том, что их персональные данные собираются и обрабатываются.

Сведения о пациента, состоянии их здоровья, иные сведения, полученные в ходе процедуры трансплантации биопринтных тканевых (органных) конструктов, составляют врачебную тайну.

9.15. Принцип цифровой модели пациента

Разработка и применение цифровой модели пациента осуществляется медицинскими работниками в соответствии со стандартами оказания медицинской помощи (медицинской услуги).

9.16. Принцип послеоперационного наблюдения

Медицинские работники должны осуществлять послеоперационный уход и контроль пациентов в соответствии со стандартами оказания медицинской помощи (медицинской услуги).

10. Этические принципы разработчиков и производителей медицинских изделий на основе биопринтных технологий

10.1. Принцип благополучия

Разработка и производство медицинских изделий на основе биопринтных технологий должны быть направлены на благо пациентов и общества, а не только на достижения интересов бизнеса.

Разработчики и производители медицинских изделий на основе биопринтных технологий должны убедиться, что их продукты обеспечивают клиническую эффективность, повышают качество медицинской помощи (медицинской услуги) и улучшают здоровье пациентов.

10.2. Принцип безопасной разработки

Разработчики и производители медицинских изделий на основе биопринтных технологий при разработке и производстве продуктов должны обеспечивать безопасность жизни и здоровья человека, окружающей среды, интересов собственности.

10.3. Принцип безопасного внедрения

Внедрение медицинских изделий на основе биопринтных технологий в клиническую практику должно быть обосновано и основано на доказательной медицине, а также на методах проверки, воспроизводимости и надежности.

10.4. Принцип безопасного применения

Разработчики и производители медицинских изделий на основе биопринтных технологий должны обеспечить качественную установку, настройку, обслуживание и ремонт продуктов на постоянной основе с соблюдением протоколов безопасности.

Документация по безопасному применению медицинских изделий на основе биопринтных технологий должна быть ясной и доступной.

10.5. Принцип ограничения конкуренции

Медицинские изделия на основе биопринтных технологий не должны использоваться для придания человеку новых способностей, влекущих ограничение конкуренции.

10.6. Принцип прозрачности и объяснимости

Разработчики и производители медицинских изделий на основе биопринтных технологий должны гарантировать, что их продукты разработаны с учетом прозрачности и объяснимости процедуры и результатов.

Разработчики и производители медицинских изделий на основе биопринтных технологий должны предоставлять медицинским работникам полную информацию о том, как работает их продукт и какие результаты стоит от него ожидать.

10.7. Принцип послерегистрационного мониторинга

Производители медицинских изделий на основе биопринтных технологий после регистрации продукта и вывода его на рынок должны осуществлять постоянный мониторинг его работы в целях выявления побочных эффектов или непредвиденных реакции при его применении.

10.8. Принцип контроля

Разработчики и производители медицинских изделий на основе биопринтных технологий должны осуществлять контроль выведенных на рынок продуктов на соответствие требованиям безопасности, надежности и эффективности.

В ходе испытаний медицинских изделий на основе биопринтных технологий не должны создаваться условия, которые могут угрожать жизни и здоровью человека.

10.9. Принцип ответственности

Разработчики и производители медицинских изделий на основе биопринтных технологий должны убедиться в том, что их продукты соответствуют высоким стандартам качества и безопасности, перед тем как предоставлять их на рынок.

Разработчики и производители медицинских изделий на основе биопринтных технологий должны быть готовы взять на себя ответственность за любые проблемы, возникающие из-за некорректного использования продукта.

11. Этические принципы медицинских работников по применению медицинских изделий на основе биопринтных технологий

11.1. Принцип созидания

Медицинские работники должны применять медицинские изделия на основе биопринтных технологий исключительно в целях оказания медицинской помощи (медицинской услуги).

11.2. Принцип безопасности

Применение медицинских изделий на основе биопринтных технологий должно быть надежным и безопасным, а получаемые на их основе результаты не должны быть направлены на причинение вреда жизни и здоровью пациентам.

Медицинские работники должны обеспечить создание прозрачной системы доклинических и клинических исследований (испытаний), которые гарантируют соответствие таких изделий высоким стандартам качества и безопасности.

11.3. Принцип добровольного информированного согласия

Медицинские работники должны информировать пациентов обо всех аспектах их медицинского обследования и вмешательства при применении в отношении них медицинских изделий на основе биопринтных технологий.

11.4. Принцип квалификации медицинских работников

Медицинские работники должны знать и соблюдать действующие нормативные правовые акты, регулирующие их профессиональную деятельность, должны быть обучены применению медицинских изделий на основе биопринтных технологий, знать стандарты оказания медицинской помощи (медицинской услуги) с использованием медицинских изделий на основе биопринтных технологий.

Медицинские работники имеют право на профессиональную подготовку или повышение квалификации по программам «Применение медицинских изделий на основе биопринтных технологий» в системе непрерывного медицинского образования на бесплатной основе.

11.5. Принцип соответствия

Медицинские изделия на основе биопринтных технологий должны соответствовать действующим стандартам оказания медицинской помощи (медицинской услуги).

11.6. Принцип защиты прав и интересов медицинских работников

Медицинский работник имеет право на защиту своих прав и интересов при применении медицинских изделий на основе биопринтных технологий.

При применении медицинских изделий на основе биопринтных технологий необходимо минимизировать риски возможных негативных последствий для медицинских работников.

11.7. Принцип государственного контроля

Деятельность по процедуре трансплантации биопринтных тканевых (органных) конструктов подлежит лицензированию.

12. Этические принципы субъектов, осуществляющих деятельность по утилизации медицинских изделий на основе технологий медицинской робототехники

12.1. Принцип естественной утилизации

Медицинские изделия на основе биопринтных технологий с истекшими сроками годности должны быть утилизированы с учетом требований биологической безопасности.

В этом случае должно быть организовано уничтожение персональных данных пациентов и иной служебной информации, обращавшейся в медицинском изделии на основе биопринтных технологий.

12.2. Принцип специальной утилизации

Медицинские изделия на основе биопринтных технологий, с истекшими сроками годности, могут быть использованы в научных и образовательных целях, не связанных с оказанием медицинской помощи (медицинской услуги).

В этом случае должно быть организовано обезличивание персональных данных пациентов, обращавшихся в медицинском изделии на основе биопринтных технологий.

Список литературы

1. Шутова А. А., Бегишев И. Р. Инициативный проект этического кодекса субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе биопринтных технологий, по взаимодействию с пациентами и донорами клеток, по обороту донорских клеток, биочернил и биопринтных тканевых (органных) конструктов: препринт № 3 за 2023 г. Казань: Изд-во «Познание» Казанского инновационного университета, 2023. 23 с. DOI: 10.21202/978-5-8399-0803-1_2023_3_23

Разработан: **А. А. Шутова**, кандидат юридических наук, Казанский инновационный университет имени В. Г. Тимирясова; **И. Р. Бегишев**, доктор юридических наук, доцент, Казанский инновационный университет имени В. Г. Тимирясова.

СОДЕРЖАНИЕ | CONTENTS

СПЕЦИАЛЬНЫЕ ВОПРОСЫ РЕГУЛИРОВАНИЯ И ОХРАНЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ | SPECIAL ISSUES OF REGULATION AND PROTECTION OF DIGITAL TECHNOLOGIES

ПРИЛОЖЕНИЕ | APPENDIX

Научное издание

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
II Международной научно-практической конференции

22 сентября 2023 г.
г. Казань

В шести томах
Том 6

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

Главный редактор *Г. Я. Дарчинова*
Редакторы: *Г. А. Тарасова, Е. А. Маннапова*
Технический редакторы: *О. А. Аймурзаева, С. Р. Каримова*
Дизайн обложки: *Г. И. Загретдинова*

ISBN 978-5-8399-0819-2

Подписано в печать 30.11.2023. Формат 60×84/16.
Гарнитура PT Astra Serif, 9. Усл. печ. л. 27,68. Уч.-изд. л. 27,08.
Тираж 500 экз. (1-й завод – 50 экз.) Заказ № 101.

Издательство «Познание» Казанского инновационного университета им. В. Г. Тимирясова
420111, г. Казань, ул. Московская, 42; тел. (843) 231-92-90; e-mail: zaharova@ieml.ru

Отпечатано с готового оригинал-макета в типографии ООО «ТЦО «Таглимат»
420108, г. Казань, ул. Зайцева, 17