Как цитировать: Цифровые технологии и право: сборник научных трудов III Международной научно-практической конференции (г. Казань, 20 сентября 2024 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 6. – Казань: Изд-во «Познание» Казанского инновационного университета, 2024. EDN: EIVHER. http://dx.doi.org/10.21202/978-5-8399-0846-8_6 – 1 CD-ROM. – Загл. с титул. экрана. – Текст: электронный.

For citation: Digital Technologies and Law: collection of scientific papers of the III International Scientific and Practical Conference (Kazan, 2024, September 20) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 6. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2024. EDN: EIVHER. http://dx.doi.org/978-5-8399-0846-8_6 – 1 CD-ROM. – Title from the title screen. – Text: electronic.

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
III Международной научно-практической конференции

20 сентября 2024 г.

г. Казань

В шести томах
Том 6

Казань ▪ КИУ ИЗДАТЕЛЬСТВО «ПОЗНАНИЕ» ▪ 2024

DIGITAL TECHNOLOGIES AND LAW

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

2023, September 22

Kazan

In 6 volumes

Volume 6

Казань ▪ KIU "POZNANIYE" PUBLISHERS ▪ 2024

УДК 004:34(063)
ББК 67с51я43
Ц75

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

Рецензенты:

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

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

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

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

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

Ц75 **Цифровые технологии и право: сборник научных трудов III Международной научно-практической конференции** (г. Казань, 20 сентября 2024 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 6. – Казань: Изд-во «Познание» Казанского инновационного университета, 2024. EDN: EIVHER. http://dx.doi.org/10.21202/978-5-8399-0846-8_6 – 1 CD-ROM. – Загл. С титул. экрана. – Текст: электронный.

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

ISBN 978-5-8399-0859-8
ISBN 978-5-8399-0846-8 (Vol. 6)

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

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

Научные труды представленного тома охватывают широкий спектр тем, связанных с цифровыми технологиями и их правовым регулированием. В нем приведены труды по праву квантовых технологий, трудовым и семейным правоотношениям, здравоохранению и интеллектуальным транспортным системам, правовым аспектам цифровых платформ, цифровым продуктам и сервисам, а также интеллектуальным правам и технологиям в расследовании преступлений.

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

УДК 004:34(063)
ББК 67с51я43

© Авторы статей, 2024
© Казанский инновационный университет имени В. Г. Тимирясова, 2024

ISBN 978-5-8399-0859-8
ISBN 978-5-8399-0846-8 (Vol. 6)

Научное издание

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов II Международной научно-практической конференции

20 сентября 2024 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

Электронное издание

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

Дата подписания к использованию: 13.12.2024. Объем издания 5,9 Мб. Тираж 11 экз. Заказ № 13/2024.
ISBN 978-5-8399-0846-8

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

UDC 004:34(063)
LBC 67с51я43

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

Reviewers:

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

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

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

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

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

Digital Technologies and Law: collection of scientific papers of the III International Scientific and Practical Conference (Kazan, 2024, September 20) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 6. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2024. EDN: UBBTJU. http://dx.doi.org/10.21202/978-5-8399-0846-8_6 – 1 CD-ROM. – Title from the title screen. – Text: electronic.
ISBN 978-5-8399-0859-8
ISBN 978-5-8399-0846-8 (Vol. 6)

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

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

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

The scientific works of this volume cover a wide range of topics related to digital technologies and their legal regulation. The volume contains works on the law of quantum technologies, labor and family legal relations, healthcare and intelligent transport systems, legal aspects of digital platforms, digital products and services, as well as intellectual property rights and technologies in crime investigation.

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

UDC 004:34(063)
LBC 67с51я43

© Authors of articles, 2024
© Kazan Innovative University
named after V. G. Timiryasov, 2024

ISBN 978-5-8399-0859-8
ISBN 978-5-8399-0846-8 (Vol. 6)

Scientific publication

DIGITAL TECHNOLOGIES AND LAW

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

2024 September 20
Kazan

In 6 volumes

Volume 6

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

Electronic publication

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

Date of signing for usage: 13.12.2024. Volume of the publication 5.9 Mb. Number of copies: 11. Order No. 13/2024.
ISBN 978-5-8399-0846-8

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

Редакторы:

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

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

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

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

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

Editors:

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

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

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

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

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

СОДЕРЖАНИЕ

ПРАВО КВАНТОВЫХ ТЕХНОЛОГИЙ

Добробаба М. Б. ПРАВОВОЕ РЕГУЛИРОВАНИЕ КВАНТОВЫХ КОММУНИКАЦИЙ: ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 11

Евсиков К. С. ПРАВОВОЙ РЕЖИМ БЕСПРОВОДНЫХ ОПТИЧЕСКИХ КАНАЛОВ СВЯЗИ В СФЕРЕ КВАНТОВЫХ КОММУНИКАЦИЙ 16

Ефремов А. А. ЭКСПЕРИМЕНТАЛЬНЫЕ ПРАВОВЫЕ РЕЖИМЫ КАК МЕТОД РЕГУЛИРОВАНИЯ РАЗВИТИЯ КВАНТОВЫХ ТЕХНОЛОГИЙ 24

Минбалеев А. В., Петровская О. В. ОСНОВНЫЕ НАПРАВЛЕНИЯ РЕГУЛИРОВАНИЯ КВАНТОВЫХ ТЕХНОЛОГИЙ 27

Никольская К. Ю. КИБЕРБЕЗОПАСНОСТЬ И КВАНТОВЫЕ ТЕХНОЛОГИИ: РИСКИ И УГРОЗЫ 30

Пашнина Т. В. ВЛИЯНИЕ КВАНТОВЫХ КОММУНИКАЦИЙ НА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ 34

Химченко А. И. ОТДЕЛЬНЫЕ АСПЕКТЫ РАЗВИТИЯ КВАНТОВЫХ КОММУНИКАЦИЙ: ДОВЕРЕННЫЙ ПОДХОД 39

Холодная Е. В. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ В ЕС ПЕРИОДОВ ДОСТИЖЕНИЙ КВАНТОВОЙ ЭПОХИ 45

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ТРУДОВЫХ И СВЯЗАННЫХ С НИМИ ПРАВООТНОШЕНИЙ

Батусова Е. С. РАБОТНИКИ ЦИФРОВЫХ ПЛАТФОРМ КАК СПЕЦИАЛЬНЫЕ СУБЪЕКТЫ ТРУДОВОГО ПРАВА (НА ПРИМЕРЕ ЗАКОНОДАТЕЛЬСТВА РЕСПУБЛИКИ ЧИЛИ) 50

Иванова Т. Б. СОВЕРШЕНСТВОВАНИЕ СОЦИАЛЬНОЙ ЗАЩИТЫ ГРАЖДАН ПРИ ПОВЫШЕНИИ ВАРИАТИВНОСТИ ФОРМ ЗАНЯТОСТИ С УЧЕТОМ ЦИФРОВЫХ ТЕХНОЛОГИЙ 56

Сапфирова А. А. ИСПОЛЬЗОВАНИЕ РАБОТОДАТЕЛЯМИ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ТРУДОВЫХ ОТНОШЕНИЯХ: ПЕРСПЕКТИВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ 65

Томашевский К. Л. ОПЫТ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ ТРУДОВЫХ ОТНОШЕНИЙ (НА ПРИМЕРЕ БРАЗИЛИИ И ЕВРОПЕЙСКОГО СОЮЗА) 71

Шишкина Ю. О. ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА РАБОТУ РУКОВОДИТЕЛЯ ОРГАНИЗАЦИИ 75

Шуралева С. В. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ ТРЕХМЕРНОГО АВАТАРА РАБОТНИКА: ПОСТАНОВКА ПРОБЛЕМЫ 81

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ЗДРАВООХРАНЕНИИ

Финкина А. П., Бакуров А. В. ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В МЕДИЦИНЕ 85

Борисенко Д. Ю., Бурсов М. А. CRISPR: ПАТЕНТНЫЕ СПОРЫ И ПРОБЛЕМЫ ЛИЦЕНЗИРОВАНИЯ 90

Егоров К. В. ОТДЕЛЬНЫЕ ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ СИСТЕМ С ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ В МЕДИЦИНЕ 92

Ерахтина О. С. К ВОПРОСУ О РАСПРЕДЕЛЕНИИ ОТВЕТСТВЕННОСТИ ЗА ВРЕД ЗДОРОВЬЮ ПАЦИЕНТА, НАСТУПИВШИЙ В РЕЗУЛЬТАТЕ ПРИМЕНЕНИЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ ВРАЧЕБНЫХ РЕШЕНИЙ 99

Поздеев А. Р. РОЛЬ ПОДГОТОВКИ КВАЛИФИЦИРОВАННЫХ МЕДИЦИНСКИХ КАДРОВ В ПЕРИОД ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЗДРАВООХРАНЕНИЯ..... 103

Тимофеева Т. Ф., Тимофеев В. В. ЕДИНЫЙ ЦИФРОВОЙ КОНТУР ЗДРАВООХРАНЕНИЯ И ЕГО РОЛЬ В СБЕРЕЖЕНИИ НАРОДОНАСЕЛЕНИЯ..... 107

Шэй И. Ю. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ЗДРАВООХРАНЕНИИ.....113

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМ

Абрамова Е. Н. АРЕНДА БЕСПИЛОТНОГО ТРАНСПОРТНОГО СРЕДСТВА..... 120

Хотько О. А. ЦИФРОВАЯ ТРАНСФОРМАЦИЯ В СФЕРЕ ОКАЗАНИЯ ТРАНСПОРТНЫХ УСЛУГ НА СОВРЕМЕННОМ ЭТАПЕ: ПРАВОВЫЕ ОСНОВАНИЯ И ЗАКОНОДАТЕЛЬНЫЕ ПОДХОДЫ 126

Чеботарев В. Е. БЕЗОПАСНОСТЬ БЕСПИЛОТНЫХ ТАКСИ – ТЕХНОЛОГИИ И ПРАВО.... 134

DIGITAL FAMILY LAW: ЦИФРОВЫЕ ТЕХНОЛОГИИ В СЕМЕЙНЫХ ПРАВООТНОШЕНИЯХ

Селезнева Е. А. ЦИФРОВАЯ ТРАНСФОРМАЦИЯ СЕМЕЙНЫХ ПРАВООТНОШЕНИЙ: ПРАВОВЫЕ АСПЕКТЫ И ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... 138

Тарасова А. Е. SMART-РОДИТЕЛЬСТВО: ВЛИЯНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА СЕМЬЮ КАК МЕГАТЕНДЕНЦИЯ 30-ЛЕТИЯ МЕЖДУНАРОДНОГО ГОДА СЕМЬИ 152

ПРАВО ЦИФРОВЫХ ПЛАТФОРМ

Бурова А. Ю. К ВОПРОСУ ОБ ОТВЕТСТВЕННОСТИ ОПЕРАТОРОВ ФИНАНСОВЫХ ПЛАТФОРМ ЗА НЕНАДЛЕЖАЩЕЕ ИСПОЛНЕНИЕ ФИНАНСОВЫХ СДЕЛОК, СОВЕРШЕННЫХ НА ФИНАНСОВОЙ ПЛАТФОРМЕ 162

Мелешкина А. И. НЕОБХОДИМОСТЬ РЕГЛАМЕНТАЦИИ ПОРЯДКА ОЦЕНКИ СЕТЕВЫХ ЭФФЕКТОВ НА РЫНКАХ С ПЛАТФОРМАМИ..... 168

Семцива С. И. ЦИФРОВЫЕ ПЛАТФОРМЫ КАК НОВЫЙ ЭТАП РАЗВИТИЯ ТРАНСНАЦИОНАЛЬНЫХ КОРПОРАЦИЙ 172

Цветков В. В. ИНИЦИАТИВА ЕС ПО ПРАВОВОМУ РЕГУЛИРОВАНИЮ ТРУДА РАБОТНИКОВ ЦИФРОВЫХ ПЛАТФОРМ 176

Чугунов Д. К., Шабронова С. Е. ПОЛЬЗОВАТЕЛЬСКОЕ СОГЛАШЕНИЕ: МОЖЕТ ЛИ ПОЛЬЗОВАТЕЛЬ ЕГО ОСПОРИТЬ? 182

ЦИФРОВЫЕ ПРОДУКТЫ И СЕРВИСЫ: ПРАВОВЫЕ АСПЕКТЫ

Минуллина Т. И., Хусяиншин Р. Р., Епифанцева М. Г. ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РАБОТЕ СПЕЦИАЛИЗИРОВАННЫХ ОРГАНИЗАЦИЙ ПО РАБОТЕ С ИНВЕСТОРАМИ В РОССИИ 186

Зубрик Д. А. ИСПОЛЬЗОВАНИЕ ЧИТ-КОДОВ КАК НАРУШЕНИЕ ПРАВ ПОЛЬЗОВАТЕЛЕЙ ОНЛАЙН-ИГР 194

Осипов М. Ю. К ВОПРОСУ ОБ ОСОБЕННОСТЯХ ПРОЕКТИРОВАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ДЛЯ ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ 200

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ИНТЕЛЛЕКТУАЛЬНЫЕ ПРАВА

Айрапетов Н. А. ОТДЕЛЬНЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ И ЗНАЧЕНИЯ ПРИНЦИПА ДОБРОСОВЕСТНОСТИ ПРИ РАСПОРЯЖЕНИИ ИСКЛЮЧИТЕЛЬНЫМ ПРАВОМ..... 207

Борулёва Е. Д. ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ «ДИПФЕЙК» ВО ВЗАИМОСВЯЗИ С ПРАВОМ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ: РОССИЙСКАЯ И ЗАРУБЕЖНАЯ ПРАКТИКА 213

Губаева Е. А. ОТВЕТСТВЕННОСТЬ ОПЕРАТОРА ЦИФРОВОЙ ПЛАТФОРМЫ ПРИ НАРУШЕНИИ НА ПЛАТФОРМЕ ИСКЛЮЧИТЕЛЬНЫХ ПРАВ НА ТОВАРНЫЕ ЗНАКИ 221

Косьяненко Е. М. АКТУАЛЬНЫЕ ПРАВОВЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ПРОИЗВЕДЕНИЙ АРХИТЕКТУРЫ И ДИЗАЙНА В СЕТИ ИНТЕРНЕТ 228

Останина Е. А. ИМЯ ФИЗИЧЕСКОГО ЛИЦА И ПСЕВДОНИМ КАК СРЕДСТВА ИНДИВИДУАЛИЗАЦИИ 235

Чирагов М. Н., Алиев У. А. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК УГРОЗА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ 239

Чурилов А. Ю. ДЕПОНИРОВАНИЕ ОБЪЕКТОВ АВТОРСКОГО ПРАВА: ТЕОРИЯ И ПРАКТИКА 247

ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Гильманов Э. М., Бабаева А. М. ИСПОЛЬЗОВАНИЕ КРИМИНАЛИСТИЧЕСКИХ МЕТОДИК ДЛЯ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ В ЦИФРОВОЙ СФЕРЕ 251

Зиновьева Е. С. ДОВЕРИТЕЛЬНЫЙ АСПЕКТ ИНСТИТУТА ПОРУЧИТЕЛЬСТВА..... 253

Латыпова Э. Ю., Бадрутдинов Р. Р. ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ В СФЕРЕ КОМПЬЮТЕРНЫХ ИГР И ИХ ОСНОВНЫЕ ХАРАКТЕРИСТИКИ 256

Мотолько А. Ф. БЕЛОРУССКИЙ ОПЫТ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННОЙ СИСТЕМЫ «СЛЕД» 263

Муратов К. Д., Плачинта Н. Э. ЦИФРОВЫЕ ДОКАЗАТЕЛЬСТВА В СИСТЕМЕ МЕЖОТРАСЛЕВЫХ ВЕЩЕСТВЕННЫХ ДОКАЗАТЕЛЬСТВ 267

Хомяков Э. Г. АКТУАЛЬНЫЕ ВОПРОСЫ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ 274

Цветкова А. Д. ПОВЕДЕНЧЕСКАЯ БИОМЕТРИЯ В КРИМИНАЛИСТИКЕ 279

Шевелева К. В. О КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ ПРИ РАССЛЕДОВАНИИ НЕЗАКОННЫХ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ АЗАРТНЫХ ИГР, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ» 282

Шубина К. С. ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ OSINT ДЛЯ СБОРА КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ 287

ПРАВО КВАНТОВЫХ ТЕХНОЛОГИЙ

М. Б. Добробаба,
доктор юридических наук, доцент,
Московский государственный юридический
университет имени О.Е. Кутафина (МГЮА)

ПРАВОВОЕ РЕГУЛИРОВАНИЕ КВАНТОВЫХ КОММУНИКАЦИЙ: ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Данная статья посвящена анализу состояния и определения перспектив правового регулирования квантовых коммуникаций в целях обеспечения информационной безопасности. Показано значение нормативно-технического регулирования отрасли квантовых коммуникаций. Обоснована необходимость разработки национальных стандартов для обеспечения совместимости устройств, производимых разными производителями.

Ключевые слова: цифровые технологии, квантовые технологии, квантовые коммуникации, информационная безопасность, стандарты информационной безопасности, сертификация, критическая информационная инфраструктура, информационная угроза, квантовая угроза, цифровая экономика, защита информации

Исследование выполнено за счет гранта Российского научного фонда (проект № 24-18-00950 «Проблемы и перспективы регулирования квантовых коммуникаций в условиях экономики данных»).

LEGAL REGULATION OF QUANTUM COMMUNICATIONS: INFORMATION SECURITY ISSUES

Abstract. This article is devoted to the analysis of the state and determination of prospects for the legal regulation of quantum communications in order to ensure information security. The importance of regulatory and technical regulation of the quantum communications industry is shown. The necessity of developing national standards to ensure the compatibility of devices manufactured by different manufacturers is justified.

Keywords: digital technologies, quantum technologies, quantum communications, information security, information security standards, certification, critical information infrastructure, information threat, quantum threat, digital economy, information protection.

The research was carried out at the expense of a grant from the Russian Science Foundation (project No. 24-18-00950 "Problems and prospects of regulating quantum communications in a data economy").

Введение. Понятие информационной безопасности как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз…» и необходимость её обеспечения провозглашены в Доктрине

информационной безопасности Российской Федерации [3]. Одним из элементов системы защиты информации является защита её целостности при передаче, что способствует обеспечению информационной безопасности личности, общества и государства.

В условиях активного развития квантовых технологий квантовая угроза признана многими странами и Россией также, что обуславливает необходимость разработки новых методов защиты информации. Учитывая необходимость обеспечения безопасности информации, была принята «Дорожная карта развития "сквозной" цифровой технологии «Квантовые технологии» [8], направленная на обеспечение информационной безопасности России.

Квантовые коммуникации являются видом квантовых технологий, использование которых обеспечивает криптографическую защиту информации, посредством квантовых частиц. Являясь высокотехнологичным направлением, квантовые коммуникации способствуют защите инфраструктуры цифровой экономики, что в условиях возрастающих угроз информационной безопасности требует выявления проблем, связанных с их разработкой и использованием.

Как и любые цифровые технологии, квантовые коммуникации развиваются быстрее, чем осуществляется развитие правового регулирования данной сферы [15. С. 64]. Учитывая значимость квантовых коммуникаций для устранения угроз информационной безопасности со стороны квантовых компьютеров, представляется необходимым определить уровень правового обеспечения разработки и применения квантовых коммуникаций и определить направления развития правового регулирования данного вида цифровых технологий.

Основная часть. Внедрение квантовых коммуникаций является проектом, реализуемым компанией «Российские железные дороги», предполагающим развёртывание оптико-волоконной сети с квантовым шифрованием, протяжённостью несколько тысяч километров. При реализации проекта РЖД осуществляет сотрудничество с производственными и научными центрами. Создаваемый продукт будет востребован в разных отраслях экономики, как в сфере государственного управления, так и в частном секторе. Одновременно потребуются специалисты в отрасли квантовых коммуникаций, что обуславливает необходимость совершенствования системы подготовки и увеличения количества специалистов в данной сфере.

Важное значение имеет принятие Правительством РФ Концепции регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года [6] (далее – Концепция регулирования отрасли квантовых коммуникаций). В данном концептуальном документе поставлена задача осуществления гармонизации регуляторной среды, при условии соблюдения баланса интересов человека, общества и государства. Кроме того, при внедрении в сети связи и ИС должен быть обеспечен должный уровень информационной безопасности.

Нормативно-техническое регулирование. Паспорт национального проекта «Национальная программа "Цифровая экономика Российской Федерации" включает федеральный проект «Информационная безопасность» [7], реализация мероприятий которого направлена на развитие квантовых коммуникаций. К таким мероприятиям относятся:

1. разработка и принятие стандартов информационной безопасности в системах, реализующих квантовые технологии;

2. создание испытательных лабораторий с использованием квантовых криптографических технологий.

Важное значение стандартизации в сфере квантовых коммуникаций заключается в установлении системы требований к сетям, оборудованию, программному обеспечению, а также использованию сетей связи. Соблюдение данных требований позволяет обеспечить совместимость устройств, производимых разными компаниями.

В 2023 году приказами Росстандарта по результатам проведённых научных исследований, а также с учётом приобретённого практического опыта применения технологий квантовых коммуникаций, утверждены предварительные национальные стандарты:

1. ПНСТ 829-2023 «Квантовые коммуникации. Общие положения» [9];

2. ПНСТ 832-2023 «Квантовые коммуникации. Термины и определения» [10].

Данные стандарты разработаны Сколковским институтом науки и технологий (Сколтех) и Университетом ИТМО в целях накопления опыта в процессе применения и утверждены на три года. По результатам их апробации планируется разработка и утверждение национальных стандартов.

Можно констатировать значение нормативно-технического регулирования отрасли квантовых коммуникаций.

Относительно вышеобозначенных испытательных лабораторий с использованием квантовых криптографических технологий, следует отметить, что уже осуществляется их создание и функционирование. В частности, открыта лаборатория ООО «СФБ Лаб», находящаяся в системе аккредитации Федеральной службы безопасности Российской Федерации. В Национальном исследовательском университете МЭИ открылась Лаборатория по криптографической защите объектов энергетики (МЭИ. Лаборатория).

Развитие правового регулирования. Как справедливо отмечает Е. В. Холодная, несмотря на значимость для государства и бизнеса квантовых коммуникаций, они до сих пор не являются объектом правового регулирования [13. С. 38–45]. Кроме того, до сих пор отсутствует единая терминология, связанная с данной цифровой технологией. Данные проблемы, несомненно, требуют своего решения.

Если рассматривать отраслевую составляющую развития отрасли квантовых коммуникаций, речь идет о функционировании *отрасли связи.* Таким образом, требуется интеграция квантовых коммуникаций в сети связи.

Одновременно развитие квантовых коммуникаций должно осуществляться в системе *информационной безопасности.* Обозначенное позволяет утверждать, что квантовые коммуникации должны развиваться в рамках комплексной модели правового регулирования, что предполагает правовое регулирование квантовой связи и одновременно квантовой информационной безопасности [12. С. 112–120]. Подобная правовая модель будет способствовать решению задачи нейтрализации возможной угрозы безопасности для инфраструктуры связи [11. С. 25–37].

Речь идёт о таких отраслях, как транспорт, промышленность, космическая деятельность. Особое значение имеют квантовые коммуникации в публичном управлении.

Экспериментальные правовые режимы. Оптимальным способом выявить правовые меры, направленные на обеспечение информационной безопасности в сфере квантовых коммуникаций, должно стать применение экспериментальных правовых режимов. Согласно Федеральному закону «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (п. 1 ст. 2), экспериментальный правовой режим в сфере цифровых инноваций – «применение в отношении участников экспериментального правового режима в течение определенного периода времени специального регулирования по направлениям разработки, апробации и внедрения цифровых инноваций» [2].

Следует иметь в виду, что экспериментальные правовые режимы в сфере цифровых инноваций могут применяться не во всех отраслях, а только в нормативно установленных. Так, одним из направлений, где осуществляется разработка, апробация и внедрение цифровых инноваций, является «связь» [4].

При этом устанавливать экспериментальные правовые режимы целесообразно в тех сферах, где требуется повышение уровня информационной безопасности. Такой сферой является, например, сфера беспилотного транспорта, где важно обеспечить безопасную передачу данных. Это может быть обеспечено с помощью технологий квантовых коммуникаций. Так, сервис «Яндекс.Такси» проводит эксперимент с беспилотными такси на дорогах общего пользования.

Сертификация и методы защиты информации. Согласно Концепции регулирования отрасли квантовых коммуникаций, должны быть соблюдены требования Федерального закона «Об информации, информационных технологиях и о защите информации [1].

Важное значение имеют обязательные требования к линиям связи, установление которых требуется до проектирования и ввода в эксплуатацию квантовых коммуникаций. В случае несоответствия оборудования действующим требованиям, в целях информационной безопасности применяются различные методы защиты информации.

Развитие правовой культуры информационной безопасности. С этой целью принята Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации [5], реализация мероприятий которой позволит достичь данной цели. К числу таких мероприятий, в частности, относится повышение информационной грамотности как взрослого населения посредством разработки специальных курсов, так и обучающихся образовательных учреждений, в том числе посредством социальной рекламы, включения соответствующих блоков в образовательную программу и т. д. Отдельное направление представляют мероприятия по повышению информационной грамотности государственных и муниципальных служащих, лиц, замещающих государственные и муниципальные должности.

Перспективы квантового сотрудничества России и Китая. Важно изучать опыт правового регулирования квантовых коммуникаций в зарубежных странах. Не менее важное значение имеет международное сотрудничество в данном направлении.

Одним из лидеров в области квантовой коммуникации является *Китай* – первая и единственная страна со спутниковой квантовой защищенной связью. В 2023 г. Китай стал страной, получившей полный цикл собственного производства квантового процессора, наряду с США и Канадой. Межгосударственное сотрудничество России с Китаем видится наиболее перспективным, учитывая территориальную близость, особый доверительный уровень отношений двух стран. Кроме того, КНР и Россию объединяет общая повестка противостояния Западу, что на этом этапе может стать основой для сотрудничества и в научно-технологической сфере. Китай

В стратегических документах КНР тематика квантовых технологий впервые нашла закрепление в 2006 году. Спустя 10 лет была принята *Национальная программе ключевых исследований и разработок, в содержание которой* была включена стратегия развития квантовой науки Китая. Следует отметить, что квантовая наука в Китае получила поддержку науки после реорганизации финансирования научных исследований, приоритетом которого стало инновационное развитие, увеличение инвестиций и развитие системы грантов, создание совместных научных центров [14]. В настоящее время квантовые коммуникации в КНР включены в список мегапроектов, реализуемых до 2030 г.

Заключение. Подводя итог, можно констатировать, что развитие квантовых коммуникаций осуществляется в рамках отрасли связи, одновременно квантовые коммуникации являются элементом системы обеспечения информационной безопасности.

Список литературы

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.), ст. 34484.

2. Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации: Федеральный закон от 31.07.2020 № 258-ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ. – 2020. – № 31 (часть I), ст. 5017.

3. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства РФ. – 2016. – № 50, ст. 7074.

4. Об установлении направлений разработки, апробации и внедрения цифровых инноваций, по которым может устанавливаться экспериментальный правовой режим в сфере цифровых инноваций: Постановление Правительства РФ от 18.12.2020 № 2149 (ред. от 21.02.2023) // Собрание законодательства РФ. – 2020. – № 52 (ч. 1), ст. 8832.

5. Об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации: Распоряжение Правительства РФ от 22.12.2022 № 4088-р // Собрание законодательства РФ. – 2022. – № 52, ст. 9726.

6. Об утверждении Концепции регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года: Распоряжение Правительства РФ от 11.07.2023 № 1856-р // Собрание законодательства РФ. – 2023. – № 30, ст. 5712.

7. Проект «Информационная безопасность» Паспорта национального проекта «Национальная программа "Цифровая экономика Российской Федерации"», утв. Президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, Протокол от 04.06.2019 № 7.

8. Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии». Доступ из справ.-прав. системы «КонсультантПлюс».

9. ПНСТ 829-2023. Предварительный национальный стандарт Российской Федерации. Квантовые коммуникации. Общие положения (утв. и введен в действие Приказом Росстандарта от 11.07.2023 № 22-пнст). – М.: ФГБУ «Институт стандартизации», 2023.

10. ПНСТ 832-2023. Предварительный национальный стандарт Российской Федерации. Квантовый интернет вещей. Термины и определения (утв. и введен в действие Приказом Росстандарта от 11.07.2023 № 25-пнст). – М.: ФГБУ «Институт стандартизации», 2023.

11. Добробаба М. Б., Чаннов С. Е., Минбалеев С. Е. Квантовые коммуникации: перспективы правового регулирования // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2022. – № 4(92). – С. 25–37.

12. Минбалеев А. В., Ефремов А. А., Добробаба М. Б., Чубукова С. Г. Методы и подходы к регулированию формирующейся отрасли квантовых коммуникаций в условиях современного информационного общества // Информационное общество. – 2024. – № (4). – С. 112–120.

13. Холодная Е. В. Квантовые технологии как объект права // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2022. – № 4. – С. 38–45.

14. Китайский путь к «квантовому превосходству» [Электронный ресурс]. URL: https://docs.yandex.ru/docs/view?tm=1725705915&tld=ru&lang=ru&name=943632099.pdf&text=правовое%20регулирование%20квантовых%20коммуникаций%20в%20китае&url=https%3A%2F%2Fissek.hse.ru%2Fmirror%2Fpubs%2Fshare%2F943632099.pdf&lr=213&mime=pdf&l10n=ru&sign= (дата обращения: 07.09.2024).

К. С. Евсиков,
кандидат юридических наук, доцент,
Тульский государственный университет,
доцент,
Московский государственный юридический университет
имени О. Е. Кутафина (МГЮА)

ПРАВОВОЙ РЕЖИМ БЕСПРОВОДНЫХ ОПТИЧЕСКИХ КАНАЛОВ СВЯЗИ В СФЕРЕ КВАНТОВЫХ КОММУНИКАЦИЙ

Аннотация. В 2023 году Правительство Российской Федерации утвердило Концепцию регулирования отрасли квантовых коммуникаций в РФ до 2030 года. Ее проект создан группой экспертов Московского государственного юридического университета им. О. Е. Кутафина (МГЮА). Данный документ не имеет аналогов

за рубежом и является частью построения в нашей стране экономики данных. Во исполнение данного документа уже внесены изменения в Общероссийский классификатор видов экономической деятельности и Общероссийский классификатор продукции по видам экономической деятельности. Это позволило выделить среди других видов информационных технологий оборудование квантовых коммуникаций, которое было разделено по предложению автора статьи на оборудование квантовой криптографии и оборудование квантовой связи. Однако в процессе установления правового режима для оборудования квантовой связи возникли, связанные с задействованием для передачи квантового сигнала атмосферных оптических линий связи, которые в отечественном законодательстве не урегулированы. В статье проанализированы ключевые правовые конфликты, возникающие в процессе использования данного вида связи, а также предложены способы их преодоления.

Ключевые слова: атмосферная оптическая связь; квантовая коммуникация; квантовая связь; квантовая криптография; квантовые технологии; лазерная связь; правовая защита линий связи

Исследование выполнено за счет гранта Российского научного фонда (проект № 24-18-00950 «Проблемы и перспективы регулирования квантовых коммуникаций в условиях экономики данных»).

THE LEGAL REGIME OF WIRELESS OPTICAL COMMUNICATION CHANNELS IN THE FIELD OF QUANTUM COMMUNICATIONS

Abstract. In 2023, the Government of the Russian Federation approved the Concept of Regulating the quantum Communications industry in the Russian Federation until 2030. Her project was created by a group of experts from the O. E. Kutafin Moscow State Law University (MGUA). This document has no analogues abroad and is part of building a data economy in our country. In pursuance of this document, changes have already been made to the All-Russian Classifier of types of Economic Activity and the All-Russian Classifier of products by type of economic activity. This made it possible to distinguish among other types of information technologies quantum communication equipment, which was divided at the suggestion of the author of the article into quantum cryptography equipment and quantum communication equipment. However, in the process of establishing a legal regime for quantum communication equipment, problems arose related to the use of atmospheric optical communication lines for transmitting a quantum signal, which are not regulated in domestic legislation. The article analyzes the key legal conflicts arising in the process of using this type of communication, as well as suggests ways to overcome them.

Keywords: atmospheric optical communication; quantum communication; quantum communication; quantum cryptography; quantum technologies; laser communication; legal protection of communication lines.

The research was carried out at the expense of a grant from the Russian Science Foundation (project No. 24-18-00950 "Problems and prospects of regulating quantum communications in a data economy").

Введение. Правительством Российской Федерации технологии квантовой коммуникации отнесены к сквозным технологиям (технологическим направлениям), под которыми понимаются перспективные технологии межотраслевого назначения, обеспечивающие создание инновационных продуктов и сервисов и оказывающие существенное влияние на развитие экономики, радикально меняя существующие рынки и (или) способствуя формированию новых рынков [1]. Сквозные технологии определяют перспективный облик экономики и отдельных отраслей в течение ближайших 10–15 лет [2]. В связи с этим перед органами государственной власти ставится задача поддержать развитие квантовой коммуникации [2, 3].

Во исполнение данного документа внесены изменения в Общероссийский классификатор видов экономической деятельности. ОК 029-2014 (КДЕС Ред. 2), куда с 27.11.2023 вошли следующие коды:

26.30.7. Производство оборудования квантовых коммуникаций;

26.30.71. Производство оборудования квантовой криптографии;

26.30.72. Производство оборудования квантовой связи.

Данная классификация основана на модели правового регулирования технологий квантовой коммуникации, предложенной ранее. Как показали исследования, первым легальным термином, относящимся к квантовым коммуникациям, стал концепт квантовое распределение ключей, который был закреплен в Указе Президента РФ от 06.03.2008 № 326 «О внесении изменений в Указе Президента Российской Федерации от 5 мая 2004 г. № 580 [3] (документ утратил силу), где технология была отнесена к товарам, ограниченным в обороте. В примечании к данному документу появилась ссылка «Квантовая криптография также известна как квантовое распределение ключей (КРК)».

В действующем сегодня Постановлении Правительства РФ от 19.07.2022 № 1299 под квантовой криптографией предложено понимать совокупность технических приемов по созданию совместно используемого ключа для защиты информации путем измерения квантово-механических свойств физической системы (включая те физические свойства, которые ясно определены квантовой оптикой, квантовой теорией поля или квантовой электродинамикой [1]. Этим же документом определены такие термины, как постквантовый, квантово-безопасный или квантово-устойчивый алгоритм защиты информации. К таковым документ отнес:

– выявление аномалий с самым коротким или самым близким одномерным массивом данных, состоящим из однотипных элементов, связанных с алгебраическими решетками CRYSTALS;

– поиск изогений между суперсингулярными эллиптическими кривыми (например, суперсингулярная изогения обмена ключами);

– дешифрование случайных кодов (например, алгоритмы McEliece, Niederreiter).

Главное преимущество квантовых распределенных ключей – защищенность информации, гарантированная законами физики. Таким образом, квантовое распределение ключей определено как одна из разновидностей квантовых коммуникаций, что дало возможность более комплексного правового регулирования общественных отношений, а также привело к появлению в официальных документах концепции квантовой связи.

Однако в силу отсутствия понимания у органов публичной власти в правовом регулировании возникла терминологическая путаница, когда бессистемно использовались дефиниции: квантовая связь, квантовая криптография, квантовое распределение ключей, постквантовый алгоритм защиты информации (квантово-безопасный, квантово-устойчивый) и т. д. Поскольку устоявшееся определение данных терминов отсутствовало, то они могли необоснованно использоваться как синонимы, а также как части или элементы категории квантовые технологии. Например, квантовая криптография длительный период времени в нормативных актах была синонимом термина квантовое распределение ключей, хотя в ходе рабочих групп, проводимых в рамках настоящего исследования, все эксперты согласились, что подобное ограничительное понимание технологий квантовой криптографии необоснованно.

Данная идея была одобрена и соответствующие изменения внесены в Общероссийский классификатор продукции по видам экономической деятельности. ОК 029-2014 (КДЕС Ред. 2), куда с 27.11.2023 вошли следующие коды:

26.3023.310. Оборудование квантовых коммуникаций;

26.30.23.311. Оборудование квантовой криптографии;

26.30.23.312. Оборудование квантовой связи;

26.30.23.319. Оборудование квантовых коммуникаций прочее, не включенное в другие группировки.

Это позволяет говорить, что в Российской Федерации возникли общественные отношения, подпадающие под термин квантовая связь, а значит, регулируемые законодательством о связи [4]. Для понимания направлений воздействия данного законодательства на квантовую коммуникацию предлагаем провести анализ, разделив правоотношения по предмету правового регулирования. В силу ограниченности объема данной статьи нами будет рассмотрен лишь один элемент этого правового механизма: атмосферные оптические линии квантовой связи.

Организации приняли и другие стандарты, например, для атмосферных оптических линий квантовой связи особый интерес могут иметь рекомендации ITU-R Recommendation P.1817-1 Propagation data required for the design of terrestrial free-space optical links. Этот документ регламентирует проектирование наземных оптических линий связи в свободном пространстве.

Проведенный анализ показывает, что регулирование данного вида связи в большинстве стран носит общий характер, что объясняется не значительным объемом рынка FSO.

Однако исследования последних лет показывают наличие высокого коммерческого потенциала у такого вида коммуникации. Например, в 2020 году продемонстрирована совместная многопользовательская коммуникация по схеме «многоточка – множество точек» (Multipoint-to-Multipoint Cooperative Multiuser SIM Free-Space Optical) [5]. В 2022 году произведена демонстрация когерентной оптической связи в свободном пространстве со скоростью 100 Гбит/с на скоростях отслеживания [4]. Эксперимент проведен с развертыванием оптического терминала, расположенного на крыше здания физики в кампусе Университета Западной Австралии в Кроули, примерно на высоте 34 м над уровнем моря. Связь осуществ-

лялась по схеме «земля – воздух» с использованием дрона. Также высокий потенциал имеют технологии Li-Fi (Light Fidelity), основанные на использовании инфракрасного и видимого спектра света в качестве канала связи для высокоскоростной передачи данных.

Эти технологии могут работать в рамках квантовой связи, что делает их правовое регулирование важным элементом развития отрасли квантовых коммуникаций. Данный вывод подтверждается и зарубежными авторами. Например, немецкий проект QuINSiDa, объединил QKD и LiFi [4]. Важно отметить, что развитию этой технологии будет способствовать существующее в ряде стран законодательное ограничение на воздействие электромагнитных волн на человека (Закон Абей, Пчелиный закон и т. д.). Хотя в настоящее время нет достоверных данных, что источники радиочастотных волн способствуют развитию патологий, но Всемирная организация здравоохранения отнесла электромагнитные радиочастоты к категории «возможно канцерогенных для человека». В связи с этим можно прогнозировать постепенное замещение систем Wi-Fi, на технологии Li-Fi.

Австралийская компания QinetiQ считает, что оптическая связь в свободном пространстве (FSOC) является уникальной инновацией, которая существенно изменит военный потенциал государств (рис. 1).

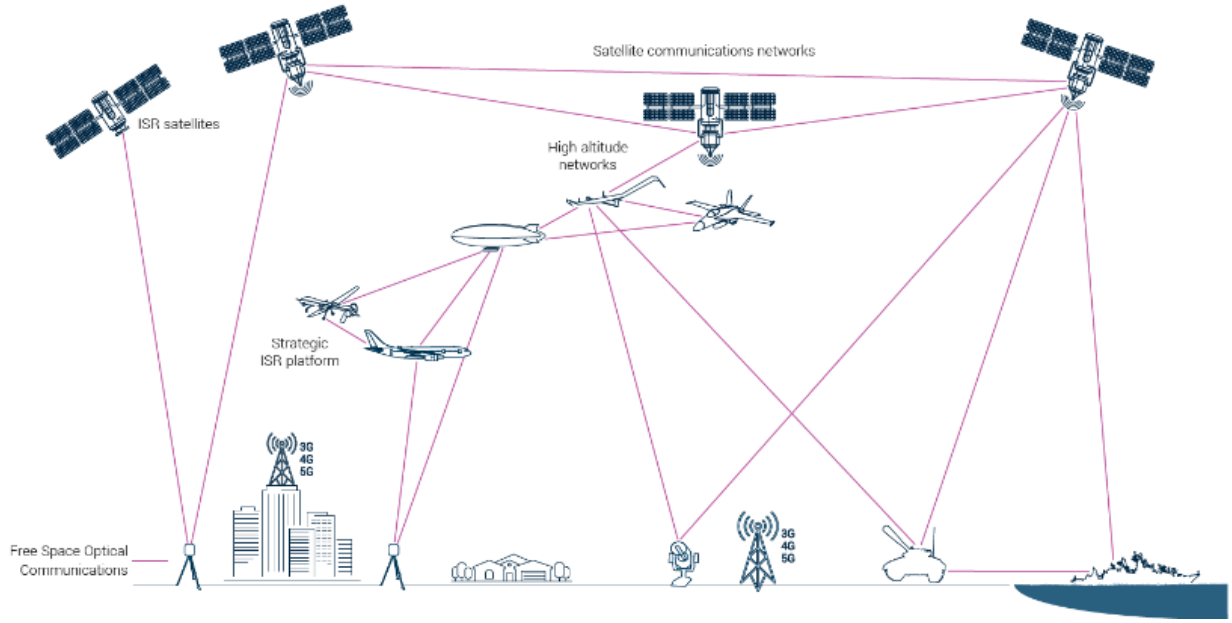

Рис. 1. Схема применения FSOC в военной сфере [1]

Как отмечают исследователи [5], оптическая связь в свободном космосе стремительно развивается благодаря спутниковому сектору. Первой исследовательской группой, сообщившей о лазерной спутниковой связи на гигабитных скоростях, была Европейская система ретрансляции данных (EDRS) (создана по соглашению о коммерческом партнерстве между Airbus и Европейским космическим агентством (ESA). EDRS использует низкоорбитальные (LEO) каналы связи с геостационарными спутниками для передачи больших наборов данных на

Землю. Поскольку группировки, такие как EDRS, передают данные через фиксированный геостационарный спутник, который поддерживает постоянную прямую видимость с наземными станциями, долгое ожидание подходящего соединения больше не требуется.

По мере роста спроса на большое количество группировок на низкой околоземной орбите, будет расти и спрос на большое количество спутников. Это, в свою очередь, приведет к дальнейшей оптимизации и коммерциализации необходимой технологии. Сегодня реализуются планы по запуску нескольких низкоорбитальных группировок, которые позволят многократно увеличить количество FSO-терминалов на орбите. Среди организаций и инициатив, движущих эту тенденцию, можно назвать Telesat Lightspeed LEO Network (188 спутников), Rivada Space Networks (600 спутников), Project Kuiper (3236 спутников), Starlink компании SpaceX, насчитывающий 12 000 спутников.

Признавая потенциал в разных сферах коммуникации в большинстве стран, осуществляется прямое или опосредованное правовое регулирование FSO. Этому способствуют исследования правоведов, которые проводятся около 10 лет. Это подтверждается публикациями по данной тематике, которые характеризуют национальное законодательство о связи и особенности его использования для регулирования нового вида коммуникации. Например, в 2014 году эксперты провели анализ правовой базы Австрии, связанной с системой FSO, ими установлено, что первостепенное значение для регламентации подобных каналов связи имеют правоотношения:

– обеспечивающие здоровье граждан, где в первую очередь выделены вопросы безопасности глаз;

– связанные с пересечением линиями FSO частной собственности [5].

Данные общественные отношения и сегодня остаются первоочередными для правового регулирования квантовой связи. Однако технологическое развитие позволяет добавить к ним вопрос правового регулирования использования спутниковой оптической связи, что, помимо защиты прав участников коммуникации, должно обеспечить безопасность государства.

Проведенное исследование позволяет говорить, что эталонного правового регулирования FSO за рубежом нет. Однако нормативные акты в данной сфере принимаются органами публичной власти разных странах. Например, регулятор ОАЭ принял уже вторую версию требований к созданию и использованию оптических каналов связи (TRA Regulations – Free Space Optics (FSO) [5]. Издание постановления о свободной космической оптике в Индонезии означает, что теперь страна представляет собой открытый рынок для устройств FSO. Как отмечают органы публичной власти для производителей, дистрибьюторов или импортеров, желающих расширить свой бизнес FSO работать в Индонезии стало легальным. Однако до начала импорта или использования устройства FSO, необходимо пройти процедуру оценки соответствия (сертификация SDPI) национальному законодательству, а точнее FSO: «KEPUTUSAN MENTERI KOMUNIKASI DAN INFORMASI REPUBLIK INDONESIA NOMOR 59 TAHUN 2022».

Анализ зарубежной правоприменительной практики и научных исследований позволяет говорить, что FSO является каналом связи, который можно использовать для квантовых методов передачи данных [5]. Каналы FSO не имеют ограничений по расстоянию передачи одиночного фотона, который существует в оптоволоконных сетях. FSO может использовать традиционные методы мультиплексирования с разделением по длине волны для отправки зашифрованных данных с более высокой скоростью. Зарубежный бизнес отмечает высокий интерес во всех сферах к каналам связи, которые невозможно обнаружить, прослушать или взломать обычными методами. Квантовое шифрование через FSO развилось настолько, что некоторые военно-морские силы НАТО тестируют эту технологию для связи между кораблями. На основании изложенного можно сделать вывод о важности стимулирования создания каналов FSO в Российской Федерации.

Для решения данной задачи органы публичной власти могут использовать два основных метода:

– прямое финансирование проектов в данной сфере;

– создание условий для развития технологий в частном секторе.

В рамках данного исследования первый вариант поддержки FSO не рассматривается, а предлагается стимулировать развитие технологии, созданием комфортного правового поля. Важно отметить, что на первоочередном этапе развития информационной технологии отсутствие правового поля является предпочтительным элементом поддержки. Например, сегодня, создание и использование АОЛП нормативными актами практически не регулируется. Это значит, что применение технологии не требует каких-либо проектных, согласовательных, лицензионных издержек, платы за использование радиочастотного спектра, так как используются частоты, на которые не требуется разрешение.

Список товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники, и в отношении которых осуществляется экспортный контроль, утвержденный Постановлением Правительства РФ от 19.07.2022 № 1299. Данным документом к ограниченным в обороте отнесены технологии разработки или применения техники лазерной связи со способностью автоматического захвата и удержания сигнала и поддержания связи через внеатмосферную или подземную (подводную) передающую среду (пункт 5.5.1.2.2).

Иных нормативных правовых актов, содержащих нормы, регламентирующие создание и использование атмосферных оптических линий передачи данных, в нашей стране нет. Правила регламентируют техническое состояние оборудования, но не включают нормы, определяющие права и обязанности лиц в процессе эксплуатации линий лазерной связи. Хотя подробные нормы регламентируют создание и использование ВОСП. Например, защита волоконно-оптических линий связи от повреждения при строительстве урегулировано несколькими нормативными правовыми актами.

Акты стратегического планирования, в которых особое место отводится линиям атмосферной оптической связи. Среди таковых можно выделить Стратегию развития беспилотной авиации Российской Федерации на период до 2030 года и на перспективу до 2035 года и план мероприятий по ее реализации, утвержденную Распоряжением Правительства РФ от 21.06.2023 № 1630-р.

Кроме того, можно отметить, что ряд технологий, используемых для передачи квантовой информации в свободном пространстве, не имеют правового статуса в Российской Федерации. К их числу можно отнести системы передачи данных по принципу Li-Fi. Правовой пробел в данной сфере существует и на нормативном, и на техническом уровне, что значительно снижает возможности защиты прав участников взаимодействия в рамках данных линий связи. Например, ГОСТ Р 59162-2020 «Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей» регулирует защиту данных в сетях Bluetooth и Wi-Fi. Технология Li-Fi при этом в стандарте не упоминается, что может мотивировать создателей данных сетей к «экономии» на информационной безопасности, вызванной отсутствием к ним жестких требований со стороны государства. В связи с этим представляется необходимым начать разработку документов технического характера в данной сфере, что позволит законодателю урегулировать общественные отношения, возникающие в связи с созданием и использованием данного способа коммуникации. Важно отметить, что в мире уже существуют стандарты для данного вида связи, которые могут быть взяты за основу в нашей стране, например, в 2023 IEEE сертифицировал первый стандарт Li-Fi, который регламентирует высокоскоростную цифровую связь в инфракрасном (ИК), визуальном и ультрафиолетовом (УФ) спектрах (IEEE 802.11bb Global Light Communications Standard).

На основании изложенного, можно сделать следующие выводы. В настоящее время идет развитие различных способов передачи квантовой информации. Согласно существующей в отечественном праве классификации, выделяют:

– волоконно-оптические линии передачи;

– атмосферные оптические линии передачи.

В Российской Федерации сети атмосферной оптической передачи данных не получили широкое распространение, а их правовая регламентация минимальна. В условиях становления новой информационной технологии подобный подход можно признать оптимальным. Например, к числу преимуществ данного вида связи и в Российской Федерации, и за рубежом относят безлицензионную передачу данных на большие расстояния, что дает технологии конкурентные преимущества перед радиосвязью. Особенно важна данная технология при обеспечении информационной безопасности технологического оборудования, базирующегося в труднодоступных местах или работающего в агрессивной среде [1]. Однако развитие квантовой сети связи требует совершенствования правового режима этого способа передачи информации. Этот вывод подтверждается и анализом зарубежного опыта, где коммерциализацию получили линии квантовой связи с использованием космического сегмента, а также комбинированные системы связи, соединяющие FOS или Li-Fi и QKD.

Список литературы

1. Об утверждении приоритетных направлений научно-технологического развития и перечня важнейших наукоемких технологий: Указ Президента РФ от 18.06.2024 № 529 // Собрание законодательства РФ. 2024. № 26, ст. 3640.

2. Об утверждении Концепции технологического развития на период до 2030 года: распоряжение Правительства РФ от 20.05.2023№N 1315-р // Собрание законодательства РФ. 2023. № 22, ст. 3964.

3. Минбалеев А. В., Берестнев М. А., Евсиков К. С. Наилучшие доступные технологии и их использование для технологического развития // Известия Тульского государственного университета. Науки о Земле. 2024. № 1. С. 144–161.

4. Евсиков К. С. Правовое регулирование поддержки отечественных производителей квантовых коммуникаций // Право и цифровая экономика. 2023. № 3. С. 11–19.

5. Евсиков К. С. Метавселенные как новый объект регулирования для информационного права // Труды по интеллектуальной собственности (Works on Intellectual Property). 2023. Т. 44, № 1. С. 47–57.

А. А. Ефремов,
доктор юридических наук, профессор,
Московский государственный юридический университет
имени О. Е. Кутафина (МГЮА)

ЭКСПЕРИМЕНТАЛЬНЫЕ ПРАВОВЫЕ РЕЖИМЫ КАК МЕТОД РЕГУЛИРОВАНИЯ РАЗВИТИЯ КВАНТОВЫХ ТЕХНОЛОГИЙ

Аннотация. В статье проведен анализ перспектив применения экспериментальных правовых режимов как метода развития квантовых технологий. Обосновано значение развития указанных технологий для обеспечения технологического суверенитета Российской Федерации, а также проанализированы существующие проблемы разработки и реализации экспериментальных правовых режимов. Разработан комплекс предложений по совершенствованию действующего и разрабатываемого (проекты федеральных законов и постановлений Правительства Российской Федерации) правового регулирования экспериментальных правовых режимов, направленный на обеспечение эффективного их применения как метода регулирования развития квантовых технологий.

Ключевые слова: квантовые вычисления, квантовые коммуникации, квантовые технологии, метод регулирования, право, цифровые технологии, экспериментальные правовые режимы

Исследование выполнено за счет гранта Российского научного фонда (проект № 24-18-00950 «Проблемы и перспективы регулирования квантовых коммуникаций в условиях экономики данных»).

EXPERIMENTAL LEGAL REGIMES AS A METHOD OF REGULATION OF THE DEVELOPMENT OF QUANTUM TECHNOLOGIES

Abstract. The article analyzes the prospects for the application of experimental legal regimes as a method for the development of quantum technologies. The importance of developing these technologies to ensure the technological sovereignty of the Russian Federation is substantiated, and the existing problems of developing and implementing experimental legal regimes are analyzed. A set

of proposals for improving the current and developing (draft federal laws and decrees of the Government of the Russian Federation) legal regulation of the experimental legal regimes is developed, aimed at ensuring their effective application as a method for regulating the development of quantum technologies.

Keywords: quantum computing, quantum communications, quantum technologies, regulatory method, law, digital technologies, experimental legal regimes.

The research was carried out at the expense of a grant from the Russian Science Foundation (project No. 24-18-00950 "Problems and prospects of regulating quantum communications in a data economy").

Обеспечение (или достижение) технологического суверенитета является одной из целей технологического развития нашей страны в соответствии с Концепцией технологического развития на период до 2030 года, утв. распоряжением Правительства РФ от 20.05.2023 № 1315-р [2]. В соответствии с постановлением Правительства РФ от 15.04.2023 № 603 оборудование для квантовых технологий отнесено к приоритетным направлениям технологического суверенитета. При этом необходимо учитывать, что реализация отдельных мер стимулирования развития квантовых технологий должна быть соотнесена с оценкой их результативности и эффективности [3].

Одним из ключевых условий для обеспечения развития квантовых технологий, в том числе прорывного, опережающего развития в современных геополитических и геоэкономических условиях является формирование комфортной регуляторной среды.

Вопросы регулирования квантовых технологий начинают активно рассматриваться в российской и зарубежной научной литературе, при этом внимание уделяется таким аспектам, как фронтирность регулирования квантовых вычислений [9] и определение их «ландшафта» [10], формирование права квантовых технологий [13, 14], определение юрисдикции в отношении транснациональных квантовых сетей [8], определение законодательных основ для регулирования квантовых вычислений [11], перспективы регулирования квантовых коммуникаций [17], регулирование квантовых вычислений как инновационных технологий [12], соотношение квантовых вычислений и права интеллектуальной собственности [16], методы регулирования квантовых коммуникаций [6], в том числе этико-правовое регулирование [15].

Создание нового нормативного правового регулирования для развития технологий, включая квантовые, предполагает разработку совершенно новых моделей регулирования [1], а также адаптацию существующих правовых механизмов.

В настоящее время квантовые технологии в соответствии с постановлением Правительства Российской Федерации от 28.10.2020 № 1750 отнесены к технологиям, которые применяются в рамках экспериментальных правовых режимов в сфере цифровых инноваций. Однако прогнозируемое их бурное развитие и возможности применения в различных сферах делают необходимым расширение сферы возможного установления экспериментальных правовых режимов.

Следует отметить, что в мае 2024 г. Правительством РФ внесен в Государственную Думу Федерального собрания РФ, а 18.06.2024 принят в первом чтении

законопроект № 632206-8 «О технологической политике в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» [5], который предусматривает изменения в законодательства об экспериментальных правовых режимах в части его расширения на сферу технологических инноваций.

Реализация предложенных положений [6] позволит повысить эффективность применения экспериментальных правовых режимов как метода регулирования развития квантовых технологий.

Список литературы

1. Громова Е. А. Модели экспериментальных правовых режимов в сфере цифровых инноваций и технологий. Москва, 2023. 96 с.

2. Ефремов А. А. Информационно-правовое обеспечение технологического суверенитета // Информационное право. 2022. № 4. С. 14–17.

3. Ефремов А. А. Оценка результативности и эффективности стимулирования развития отрасли информационных технологий в России: состояние и перспективы // Вопросы государственного и муниципального управления. 2023. №4. С. 71–99.

4. Ефремов, А. А., Южаков, В. Н. Оценка результативности и эффективности экспериментального регулирования в сфере цифровых инноваций // Информационное общество. 2021. № 3. С. 41–50.

5. Законопроект № 632206-8 «О технологической политике в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации». – URL: https://sozd.duma.gov.ru/bill/632206-8 (дата обращения: 08.09.2024)

6. Минбалеев А. В., Ефремов А. А., Добробаба М. Б., Чубукова С. Г. Методы и подходы к регулированию формирующейся отрасли квантовых коммуникаций в условиях современного информационного общества // Информационное общество. 2024. № 4. С. 112–120.

7. Проект Постановления Правительства РФ «Об утверждении Положения о подготовке, распространении, в том числе опубликовании, ежегодного государственного доклада о деятельности, осуществляемой в рамках реализации экспериментальных правовых режимов в сфере цифровых инноваций». – URL: https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=149604 (дата обращения: 08.09.2024)

8. Abdikhakimov I. Jurisdiction over Transnational Quantum Networks // International Journal of Law and Policy. – 2023. – Т. 1, №. 8.

9. Babikian J. The Legal Frontier: Understanding Regulations for AI, Quantum Computing, and Blockchain //International Journal of Advanced Engineering Technologies and Innovations. – 2020. – Т. 1, №. 1. – С. 137–156.

10. Babikian J. Navigating the Legal Landscape: Regulations for Artificial Intelligence, Quantum Computing, and Blockchain //International Journal of Advanced Engineering Technologies and Innovations. – 2017. – Т. 1, №. 1. – С. 1–16.

11. DeRose K. Establishing the legal framework to regulate quantum computing technology // Cath. UJL & Tech. – 2022. – Т. 31. – С. 145.

12. Girasa R., Scalabrini G. J. Regulation of innovative technologies: blockchain, artificial intelligence and quantum computing. – Springer Nature, 2022.

13. Gromova E. A., Petrenko S. A. Quantum law: the beginning // Journal of Digital Technologies and Law. – 2023. – Т. 1, №. 1.

14. Gulyamov S. Quantum law: navigating the legal challenges and opportunities in the age of quantum technologies //Uzbek Journal of Law and Digital Policy. – 2023. – Т. 1, №. 1.

15. Kop M. Establishing a legal-ethical framework for quantum technology // Yale Law School, Yale Journal of Law & Technology (YJoLT), The Record. 2021.

16. Kop M. Quantum computing and intellectual property law // BTLJ Comment. – 2022. – С. 101.

17. Minbaleev A., Zenin S., Evsikov K. Prospects for Legal Regulation of Quantum Communication //BRICS Law Journal. – 2024. – Т. 11, №. 2. – С. 11–54.

А. В. Минбалеев,
доктор юридических наук, профессор,
Московский государственный юридический
университет имени О. Е. Кутафина (МГЮА)
О. В. Петровская,
кандидат юридических наук, старший преподаватель,
Московский государственный юридический
университет имени О. Е. Кутафина (МГЮА),
научный сотрудник,
Институт государства и права
Российской академии наук

ОСНОВНЫЕ НАПРАВЛЕНИЯ РЕГУЛИРОВАНИЯ КВАНТОВЫХ ТЕХНОЛОГИЙ

Аннотация. В статье авторами анализируются основные направления регулирования квантовых технологий в России и в мире. Целью исследования является выявление уровня современного состояние нормативного правового регулирования квантовых технологий в России и выработка основных подходов к их регулированию в краткосрочной и среднесрочной перспективе.

Ключевые слова: квантовая экосистема, квантовые измерения, квантовые коммуникации, квантовый компьютер, квантовые технологии, право, цифровые технологии

Исследование выполнено за счет гранта Российского научного фонда (проект № 24–18-00950 «Проблемы и перспективы регулирования квантовых коммуникаций в условиях экономики данных»).

THE MAIN DIRECTIONS OF REGULATION OF QUANTUM TECHNOLOGIES

Abstract. In the article, the authors analyze the main directions of regulation of quantum technologies in Russia and in the world. The purpose of the study is to identify the current state of the regulatory legal regulation of quantum technologies in Russia and to develop basic approaches to their regulation in the short and medium term.

Keywords: quantum ecosystem, quantum measurements, quantum communications, quantum computer, quantum technologies, law, digital technologies

В части формирования правовых основ отрасли квантовых коммуникаций постоянно проводятся сбор и обработка предложений органов публичной власти и коммерческих организаций о целесообразности принятия конкретного проекта нормативного правового акта, а также об изменении очередности их разработки. Например, в апреле 2024 года участниками рынка поставлен вопрос о необходимости изменения документации Евразийской экономической комиссии, в том числе Решения Совета Евразийской экономической комиссии от 23.11.2020 № 105 «Об утверждении Правил определения страны происхождения отдельных видов товаров для целей государственных (муниципальных) закупок» [1], Решения Совета Евразийской экономической комиссии от 14.09.2021 № 80 «Об утверждении единой Товарной номенклатуры внешнеэкономической деятельности Евразийского экономического союза и Единого таможенного тарифа Евразийского экономического союза, а также об изменении и признании утратившими силу некоторых решений Совета Евразийской экономической комиссии» [2] и др.

Активно осуществляется мониторинг передовых актов, принимаемых в Европейском союзе и ведущих экономически развитых государствах мира. Так, в Европейском союзе принята «Рекомендация по скоординированной дорожной карте реализации перехода к постквантовой криптографии», которая призывает «государства-члены разработать всеобъемлющую стратегию внедрения постквантовой криптографии, чтобы обеспечить скоординированный и синхронизированный переход между различными государствами-членами и их государственными секторами. Стратегия должна определять четкие цели, этапы и сроки, в результате чего будет определена совместная дорожная карта внедрения постквантовой криптографии. Это должно привести к развертыванию технологий постквантовой криптографии в существующих системах государственного управления и критически важных инфраструктурах с помощью гибридных схем, которые могут сочетать постквантовую криптографию с существующими криптографическими подходами или с квантовым распределением ключей» [3]. В связи с этим сегодня ставится вопрос о разработке проектов нормативных правовых актов, посвященных развитию постквантовой криптографии, и в Российской Федерации.

В «Принципах корпоративного управления» выделяются некоторые из вероятных правовых и нормативных вопросов, которые компаниям необходимо будет иметь в виду при планировании, разработке и продвижении продуктов, связанных с квантовыми вычислениями. Это вопросы, на которых сосредоточены

наши юристы в технологическом секторе: прогнозирование правовых и нормативных проблем для всех форм передовых технологий (включая искусственный интеллект, криптовалюты, NFT и технологии, связанные с метавселенной). Особое место занимают вопросы правового обеспечения кибербезопасности. Расширенные возможности квантовых вычислений по взлому современных стандартов шифрования означают, что кибербезопасность сетей и информационных систем будет иметь ключевое значение. Квантово-устойчивая криптография может становиться все более необходимой, и компаниям необходимо будет оценить, в какой степени их развивающиеся сети (системы) соответствуют применимым нормам кибербезопасности, особенно тем, которые работают в критически важных секторах, на которые распространяются определенные стандарты кибербезопасности (например, оборона и сфера финансовых услуг)» [4].

Заключение. Наблюдается недостаток регулирования в области квантовых технологий, в этой сфере пока нет ни стратегической базы, ни конкретных подходов к правовому регулированию, что необходимо проработать.

Список литературы

1. Решение Совета Евразийской экономической комиссии от 23.11.2020 № 105 (ред. от 14.05.2024) «Об утверждении Правил определения страны происхождения отдельных видов товаров для целей государственных (муниципальных) закупок» [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_369802 (дата обращения: 16.08.2024).

2. Решение Совета Евразийской экономической комиссии от 14.09.2021 № 80 «Об утверждении единой Товарной номенклатуры внешнеэкономической деятельности Евразийского экономического союза и Единого таможенного тарифа Евразийского экономического союза, а также об изменении и признании утратившими силу некоторых решений Совета Евразийской экономической комиссии» [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_397176 (дата обращения: 16.08.2024).

3. Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography [Электронный ресурс]. – URL: https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography (available at: 05.08.2024).

4. A quantum-enabled future: legal and regulatory aspects of quantum technology [Электронный ресурс]. – URL: https://techinsights.linklaters.com/post/102hryr/a-quantum-enabled-future-legal-and-regulatory-aspects-of-quantum-technology (available at: 05.08.2024).

К. Ю. Никольская,
научный сотрудник,
Научно-образовательный центр
правового регулирования в сфере высоких технологий,
Московский государственный юридический университет
имени О. Е. Кутафина

КИБЕРБЕЗОПАСНОСТЬ И КВАНТОВЫЕ ТЕХНОЛОГИИ: РИСКИ И УГРОЗЫ

Аннотация. В статье приведены риски и угрозы кибербезопасности, которые могут возникнуть при использовании квантовых технологий. Рассмотрены такие аспекты, как лицензирование деятельности компаний по производству квантового оборудования, а также регулирование квантовых облачных сервисов. Рассмотрены проблемы постквантовой криптографии и необходимость ее внедрения в существующие инфраструктуры. Дано определение и описание такого явления, как «Q-Day», а также причины его возникновения. Описан подход «собрать сейчас, расшифровать позже» и почему он важен для квантового права как основа для правового регулирования.

Ключевые слова: кибербезопасность, квантовые компьютеры, квантовое право, квантовые технологии, информационная безопасность, информационное право, принципы правового регулирования

Исследование выполнено за счет гранта Российского научного фонда (проект № 24-18-00950 «Проблемы и перспективы регулирования квантовых коммуникаций в условиях экономики данных»).

CYBERSECURITY AND QUANTUM TECHNOLOGIES: RISKS AND THREATS

Abstract. The article presents the risks and threats to cybersecurity that may arise when using quantum technologies. It considers such aspects as licensing the activities of companies producing quantum equipment, as well as the regulation of quantum cloud services. It considers the problems of post-quantum cryptography and the need to implement it in existing infrastructures. It defines and describes such a phenomenon as «Q-Day», as well as the reasons for its occurrence. It describes the «Collect now, decrypt later» approach and why it is important for quantum law as a basis for legal regulation.

Keywords: cybersecurity, quantum computers, quantum law, quantum technologies, information security, information law, principles of legal regulation

The research was carried out at the expense of a grant from the Russian Science Foundation (project No. 24-18-00950 "Problems and prospects of regulating quantum communications in a data economy").

Из-за стремительного развития квантовых компьютеров общество сталкивается с переломным моментом в кибербезопасности. Несмотря на все преимущества, которые принесет использование квантовых компьютеров, такие как ожида-

емые «квантовые скачки» в разработке лекарств, необходимо также проанализировать риски и потенциальную угрозу их реализации. Квантовые вычисления могут использоваться для проведения кибератак. Традиционные вычисления работают с битами – двоичными фрагментами информации, которые выражаются либо как 0, либо как 1. Квантовые вычисления используют кубиты (квантовые биты). В отличие от традиционных битов, кубиты могут находиться в нескольких позициях одновременно (эта способность называется суперпозицией), что означает, что они могут существовать как 0, так и как 1 одновременно. Суперпозиция кубитов позволяет им выполнять множество вычислений одновременно. Именно это делает квантовые вычисления и квантовый взлом таким мощным оружием – потенциально достаточно мощными, чтобы взломать традиционные алгоритмы шифрования, которые используются в настоящее время [3].

Для того чтобы разработать методы регулирования квантовых технологий, необходимо понимать ландшафт квантовых рисков и угроз. Рассмотрим основные из них ниже.

Первым риском можно назвать наступление так называемого «Q-Day». «Q-Day» – день, когда развитие квантовых вычислений сможет нарушить существующие стандарты безопасности. Различные исследователи предполагают, что этот день возникнет в ближайшие 5–10 лет. Основная опасность заключается в том, что квантовые вычисления смогут взломать алгоритмы шифрования, которые используются сейчас как эталонные в банковской сфере, кибербезопасности и других критически важных отраслях [8].

В 2022 году Агентство национальной безопасности США выпустило призыв перейти к 2035 году на квантово-безопасное шифрование. В 2023 году Агентство по кибербезопасности и безопасности инфраструктуры, агентство национальной безопасности и Национальный институт стандартов и технологий опубликовали документ, в котором опубликованы рекомендации по переходу на постквантовую криптографию [5].

Еще одним важным фактором для регулирования и обеспечения безопасности являются облачные квантовые вычисления. На данный момент уже существуют компании, которые предоставляют подобный доступ (IBM, Microsoft, Google, Amazon и др.). Некоторые исследователи считают, что предоставление подобного доступа несет в себе огромные риски для кибербезопасности. Однако далеко не все квантовые компьютере несут в себе подобные риски. На данный момент развития технологии не существует квантового компьютера, а тем более облачного доступа к нему, который смог бы угрожать традиционному шифрованию и способен был взломать современные алгоритмы, такие как ГОСТ Р 34.12-2015, RSA, ECC и др. Это связано с тем, что в современных квантовых компьютерах используются от сотни до тысячи «шумных» кубитов, что позволяет получить только небольшое количество «стабильных» кубитов без ошибок. Для взлома современных алгоритмов шифрования необходимо использование порядка миллиона «шумных» кубитов [9].

Проблема регулирования создания и продажи квантовых компьютеров, а также предоставление доступа к облачным сервисам – это второй важный риск.

Свободный доступ к облачным ресурсам может привести к тому, что злоумышленники, маскируясь под научные организации, смогут получить доступ к подобным ресурсам и использовать их в своих противоправных действиях. Создание и продажа квантовых компьютеров в будущем, которые смогут угрожать целостности защиты кибербезопасности организаций и компаний, нуждается в регулировании уже сейчас [1].

Еще одним риском можно назвать атаки с использованием подхода «собрать сейчас, расшифровать позже». Его суть заключается в следующем: злоумышленники крадут зашифрованные файлы и хранят их до тех пор, пока не появятся квантовые компьютеры, которые смогут взломать современные алгоритмы шифрования. Таким образом, данные с длительной ценностью, такие как данные о здоровье, финансовые записи и другие, будут представлять непосредственный интерес для киберпреступников. Стоит отметить, что сегодняшние постквантовые решения могут создать ложное чувство безопасности, поскольку неизвестно, останутся ли квантовые алгоритмы, которые сегодня считаются устойчивыми, такими по мере того, как квантовые компьютеры станут производительнее и эффективнее. На данный момент существует постквантовый алгоритм CRYSTALS-Kyber [11], который выбран основой для стандарта будущих криптографических систем США, в котором в 2022 году исследователями из Королевского института KTH в Швеции был найден ряд критических уязвимостей [7].

Еще одним риском можно считать интеграцию искусственного интеллекта и квантовых вычислений. Это позволит значительно увеличить сложность и масштаб киберугроз [2]. Атаки с использованием искусственного интеллекта будут использовать алгоритмы машинного обучения для обхода традиционных мер безопасности и выполнять целевые вторжения значительно более эффективно [13]. Например, с помощью искусственного интеллекта можно анализировать большие наборы данных для выявления уязвимостей в системах, а после разрабатывать индивидуальные атаки, которые будет трудно обнаружить и защититься [10].

Что касается угроз, то главной можно назвать модернизацию существующей инфраструктуры как частных, так и государственных организаций, которые используют в своей работе алгоритмы шифрования данных. Согласно исследованию [6], более половины руководителей ИТ-подразделений считают, что их компании не будут готовы к кибератакам, в которых будут использоваться квантовые технологии. Уже сейчас компании могут начать внедрение постквантовых алгоритмов, чтобы сократить расходы в будущем. Например, iMessage и Signal стали пока что единственными приложениями для обмена сообщениями, которые предлагают постквантовое шифрование [14].

Еще одной угрозой можно назвать взлом существующих постквантовых алгоритмов шифрования, которые считаются устойчивыми к квантовым атакам [12]. На данный момент нет информации, что хотя бы одно приложение было взломано с помощью методов квантового взлома, но внедрение подобных технологий в будущем позволит обезопасить пользователей и их личные данные. Несмотря на внедрение современного постквантового шифрования, в апреле 2024 Илей Чен разработал способ, которым квантовые компьютеры могут атаковать алгоритмы, которые основаны на математике решеток, которые считаются одними из самых

сложных для взлома [4]. Подобные методы лежат в том числе в основе системы безопасности iMessage.

Список литературы

1. Добробаба М. Б., Чаннов С. Е., Минбалеев А. В. Квантовые коммуникации: перспективы правового регулирования // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2022. – № 4. – С. 25–37.

2. Ayoade O., Rivas P., Orduz J. Artificial Intelligence Computing at the Quantum Level // Data, Volume 7(3), 2022.

3. Balamurugan K. S., Sivakami A., Mathankumar M., Yalla Jnan Devi Satya prasad, Irfan A. Quantum computing basics, applications and future perspectives // Journal of Molecular Structure, Volume 1308, 2024.

4. Chen Y. Quantum Algorithms for Lattice Problems // Cryptology ePrint Archive [Электронный ресурс]. – URL: https://eprint.iacr.org/2024/555 (дата обращения: 06.09.2024).

5. CISA, NSA and NIST Publish New Resource for Migrating to Post-Quantum Cryptography // CISA [Электронный ресурс]. – URL: https://www.cisa.gov/news-events/news/cisa-nsa-and-nist-publish-new-resource-migrating-post-quantum-cryptography (дата обращения: 07.09.2024).

6. DigiCert Global Study: Preparing for a Safe Post-Quantum Computing Future // Digicert [Электронный ресурс]. – URL: https://www.digicert.com/news/digicert-global-study-preparing-for-a-safe-post-quantum-computing-future (дата обращения: 07.09.2024).

7. Dubrova E., Ngo K., Gärtner J. Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste // Cryptology ePrint Archive [Электронный ресурс]. – URL: https://eprint.iacr.org/2022/1713.pdf (дата обращения: 057.09.2024).

8. Fazal R. The Future of Cybersecurity in the Age of Quantum Computers // Future Internet, Volume 14, 2022.

9. Fazal R. The Q-Day Dilemma and the Quantum Supremacy // Advantage Conjecture. Research square, 2022.

10. Gupta R. Quantum Computing and AI // IJFMR, Volume 6, Issue 3, 2024.

11. Ji Y., Wang R., Ngo K., Dubrova E., Backlund L. A Side-Channel Attack on a Hardware Implementation of CRYSTALS-Kyber // IEEE European Test Symposium (ETS), Venezia, Italy, 2023, pp. 1-5.

12. Kumar M. Post-quantum cryptography Algorithm's standardization and performance analysis // Array, Volume 15, 2022.

13. Shuford, J. Quantum Computing and Artificial Intelligence: Synergies and Challenges // Journal of Artificial Intelligence General Science (JAIGS), Volume 1(1).

14. Will Your Online Conversations Be Safe in the Quantum Hacking Era? // The fast mode [Электронный ресурс]. – URL: https://www.thefastmode.com/expert-opinion/35430-will-your-online-conversations-be-safe-in-the-quantum-hacking-era (дата обращения: 07.09.2024).

Т. В. Пашнина,
кандидат юридических наук,
Российского государственного университета правосудия,
Уральский филиал

ВЛИЯНИЕ КВАНТОВЫХ КОММУНИКАЦИЙ НА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ

Аннотация. Цель работы состоит в исследовании проблем и перспектив обеспечения безопасности передачи информации посредством квантовых коммуникаций. На основе анализа научных работ ведущих специалистов информационного права изучено понятие, виды и особенности квантовых технологий в контексте информационных и сквозных цифровых технологий. Отмечено двойственное влияние квантовых коммуникаций на информационную безопасность – в качестве «квантовой угрозы», с одной стороны, и технологии, способной обеспечить качественно превосходящий уровень безопасности передачи информации за счет постквантовой криптографии, с другой. На основе зарубежных публикаций проанализирована сущность распределения квантовых ключей и постквантовых криптографических алгоритмов; рассмотрены преимущества и риски применения квантовых технологий для обеспечения безопасности передачи информации. Сделан вывод о необходимости создания эффективной системы нормативного регулирования квантовых коммуникаций, включающей правовой, технический и этический компоненты. Обоснована целесообразность разработки в перспективе концепции информационной безопасности личности в киберпространстве с включением в нее положений о защите от «квантовой угрозы» и практических шагов, направленных на формирование «квантовой грамотности» у возможно большего числа граждан Российской Федерации.

Ключевые слова: цифровая трансформация, информационная безопасность, кибербезопасность, квантовые технологии, квантовые коммуникации, квантовая угроза, квантовая криптография

THE INFLUENCE OF QUANTUM COMMUNICATIONS TO ENSURE THE SECURITY OF INFORMATION TRANSMISSION

Abstract. The purpose of this work is to explore the challenges and opportunities in ensuring the security of information transmission through quantum communication. Based on an analysis of scientific publications by leading experts in the field of information law, we analyze the concept and types of quantum technologies within the context of end-to-end digital technology. We note the dual impact of quantum technologies on information security: as a «quantum threat» on the one hand and as a means of achieving a qualitatively higher level of information transmission using quantum and post-quantum cryptography on the other. Based on foreign publications, the essence of the distribution of quantum keys and post-quantum cryptographic algorithms is analyzed. The advantages and risks of using quantum technologies to ensure the security of information transmission are considered. It is concluded that the need to master quantum technologies and create an effective system of their regulatory regulation, including legal, technical and ethical components, is an objective

need, without which it is impossible to ensure technological sovereignty and information security of the state. The expediency of developing the concept of personal information security in cyberspace in the future with the inclusion of provisions on protection from the «quantum threat» and practical steps aimed at the formation of «quantum literacy» among a possible larger number of citizens of the Russian Federation is substantiated.

Keywords: digital transformation, information security, cybersecurity, quantum technology, quantum communication, quantum threat, quantum cryptography

Введение. Начало XXI века ознаменовало собой тектонические сдвиги в научно-техническом развитии человечества, в числе прочего связанные с информационной сферой. Особый интерес в этом контексте представляют сквозные цифровые технологии – искусственного интеллекта, больших данных, распределенного реестра хранения данных (блокчейна), облачных вычислений и др., входящих в число так называемых «прорывных технологий», оказывающих существенное влияние на все сферы жизнедеятельности технически развитых государств мира. Именно от уровня владения передовыми технологиями сегодня во многом зависит эффективность обеспечения национальной безопасности государств, в том числе безопасность в сфере передачи и распространения информации.

Несмотря на то, что, как правило, наиболее перспективными из всех «сквозных» технологий исследователи и практики называют технологии искусственного интеллекта, не меньший потенциал для прогрессивного развития всех сфер жизнедеятельности несут в себе квантовые технологии, способные обрабатывать гораздо большие объемы данных в максимально короткое время, по сравнению с другими технологиями.

Е. В. Холодная пишет о том, что с позиций действующего информационного законодательства «квантовые технологии можно рассматривать в качестве разновидности информационных технологий», представляющих собой «совокупность процессов, средств, методов сбора, обработки и передачи данных с использованием квантовых явлений (квантовых эффектов). <…> Основное отличие квантовых технологий от иных информационных технологий, разработанных на основе математических платформ и алгоритмов, – в их физической (природной) сущности, основанной на законах и явлениях квантовой механики (квантовых эффектах). <... > В настоящий момент квантовые технологии подразделяются на виды: квантовые вычисления; квантовые сенсоры; квантовые коммуникации» [5. С. 40–41]. С положительной стороны можно оценить то, что авторами впервые в юридической науке проведен комплексный анализ существующего национального регулирования квантовых технологий [6].

Квантовые коммуникации способны произвести настоящую революцию в области криптографии и обеспечения безопасности передачи информации, в свете чего особенно важными становятся правовые рамки и стратегические ориентиры их применения.

В принятой в 2023 г. Концепции регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года, утвержденной распоряжением Правительства Российской Федерации от 11 июля 2023 г. № 1856-р, закреплены

значение и базовые принципы применения квантовых технологий в нашей стране, среди которых: обеспечение прав человека; приоритет безопасности государства; право на защиту информации.

В свете последнего ведущие специалисты в области информационного права справедливо отмечают, что «использование квантовых коммуникаций позволяет обеспечивать практически абсолютную гарантию безопасности передаваемой информации, по крайней мере их уровень информационной безопасности на современном этапе развития технологий является принципиально более высоким, нежели традиционных технологических решений… В России и в мире наиболее распространено регулирование квантовых коммуникаций с позиции рассмотрения их как информационной (цифровой технологии), обеспечивающей защиту передаваемой информации, т. е. как новой технологии защиты информации» [2. С. 105–106].

Так, А. М. Минбалеев, М. Б. Добробаба и С. Е. Чаннов утверждают: «Квантовые коммуникации включают разработку систем квантовой криптографии и квантовой связи. Главное преимущество квантовых коммуникаций – это защищенность информации, гарантированная законами физики, применение которых обеспечит более высокий и ранее недоступный уровень информационной безопасности и построение квантовых защищенных и вычислительных сетей» [3. С. 8; 1. С. 27].

При всех своих достоинствах, распространение квантовых технологий имеет и «оборотную сторону медали», способную породить принципиально новые вызовы, с которыми система информационной безопасности не имела дела прежде.

Дуализм квантовых коммуникаций эксперты, с одной стороны, видят в том, что они несут в себе потенциал новой мощной угрозы информационной безопасности («квантовая угроза»), связанной с «разрушением систем защиты данных, вызванных появлением квантового компьютера» [5. С. 57]; с другой – квантовые технологии являются технологиями, способными перевести информационную безопасность передачи информации на качественно иной уровень за счет применения квантовой криптографии, значительно превосходящей возможности современных средств криптографической защиты информации.

Основная часть. Говоря об обеспечении безопасности при передаче информации в век «прорывных» технологий, необходимо разобраться, прежде всего, с понятием технологий квантовых коммуникаций, представляющих собой «системную совокупность технологических решений (направлений), использующих квантовые явления (квантовые эффекты) для информационного обмена», одной из разновидностей которых является «квантовое распределение ключей (квантовая криптография)» [4. С. 42].

Исследователи утверждают, что большинство стран мира осознали наличие квантовой угрозы и начали исследования в области квантово-безопасной криптографии. Выделяют новые методы защиты информации, которые включают в себя: постквантовые криптографические алгоритмы; распределение квантовых ключей [6. С. 15].

Авторы научной работы «Квантовая защищенная коммуникация: Всеобъемлющий литературный анализ с глубоким осмыслением» («Quantum Secure Communication: A Comprehensive Literary Analysis with In-Depth Insights», 2023) относительно технологии распределения квантовых ключей (QKD) отмечают следующее: «…история QKD уходит корнями в 1970-е годы, когда Стивен Визнер выдвинул идею квантовой криптологии. Позже Чарльз Х. Беннетт изобрел протокол bb84, который стал краеугольным камнем квантовой криптологии, основанной на непараллельных состояниях. В 1990 году Артур Экерт внес значительный вклад в QKD, исследовав квантовую запутанность как основу безопасной коммуникации. На сегодняшний день QKD рассматриваются как перспективные методы установления защищенных каналов связи» [8. С. 172].

На основе комплексного анализа научных публикаций по квантовым коммуникациям индийские исследователи обосновывают сущность распределения квантовых ключей и постквантовых криптографических алгоритмов: «Защищенность передачи информации достигается путем обмена ключами в зашифрованном формате, между отправителем и получателем. Этот метод использует принципы квантовой физики, которые могут помочь принять меры безопасности, способные противостоять угрозам, исходящим от квантовых вычислений. QKD обеспечивает безопасную передачу данных, посылая пакеты квантовых частиц, обычно известных как фотоны, по оптоволоконным кабелям. Каждый фотон несет случайный квантовый сигнал, состояние или кубит, представляющий двоичную цифру 0 или 1. Эти кубиты измеряются на стороне получателя, образуя набор битов или последовательностей. Эта последовательность битов затем становится ключом для шифрования и расшифровки сообщений. Любые попытки внешних источников вмешаться в передачу или отслеживать ее могут быть обнаружены благодаря внутренним свойствам, определяемым квантовой механикой. Протоколы QKD делятся на две основные категории: протоколы, основанные на подготовке и измерении, и протоколы, основанные на запутывании. Первый включает в себя измерение состояния частицы. В то же время, последнее зависит от исключительного явления квантовой запутанности, при котором измерительные действия, выполняемые с одной частицей, оказывают существенное влияние на поведение другой частицы. Эти протоколы обеспечивают предотвращение попыток несанкционированного доступа, тем самым эффективно защищая коммуникации» [8. С. 172].

Зарубежные специалисты по вопросам кибербезопасности делают акцент и на том обстоятельстве, что квантовая обработка информации и коммуникация превосходят классическую коммуникацию благодаря своим возможностям. Авторы научной работы «A Review of Quantum Cybersecurity: Threats, Risks and Opportunities» (2022) отмечают, что «во-первых, неопределенность не позволяет определить положение частицы в микромире из-за ее существования в разных местах. Квантовое клонирование также позволяет восстановить любую информацию, удаленную из квантовой системы злоумышленником. Квантовая телепортация, кроме того, позволяет передавать данные, которые не были извлечены при измерении отправителем и передаются получателю посредством измерения. Квантовая информация также обладает скрытыми свойствами, которыми не обладает

классическая информация. Запутанность информации в квантовой криптографии делает невозможным получение данных с помощью локальной операции измерения; только совместное измерение может выявить их. Одной из желательных особенностей квантовой криптографии является ее безусловная безопасность, поскольку, в отличие от классических вычислений, где данные защищены с помощью шифрования, которое может быть перехвачено злоумышленниками, в квантовой коммуникации обнаружение подслушивающего устройства обеспечивается благодаря квантовой теории отсутствия клонирования. Таким образом, квантовая криптография является более выгодной, чем классическая криптография, благодаря своей безусловной защите и возможностям обнаружения перехватов» [9. С. 8].

Однако, как и любая иная сквозная цифровая технология, применение квантовых технологий порождает целый ряд доселе неизвестных науке и практике *проблем*. Анализ зарубежных публикаций позволяет обозначить среди таковой проблемы прозрачности и масштабируемости в квантовой защищенной связи, проявляющиеся в нескольких аспектах:

а) *сложность квантовой технологии* для неспециалистов;

б) *ограниченная осведомленность общественности,* порождающая скептицизм среди пользователей;

в) *непрозрачность квантового ключа и протоколов распространения,* способные подорвать у пользователя доверие к безопасности сети [8. С. 176].

Выводы. В заключение еще раз подчеркнем, что квантовые коммуникации благодаря особенностям физической природы, бесспорно, являются перспективной сквозной цифровой технологией, способной обеспечить качественно более высокий уровень безопасности передачи информации.

С другой стороны, именно квантовые технологии в сочетании с иными сквозными технологиями, например нейросетями, способны создать наиболее серьезные риски для кибербезопасности, поскольку существующие средства криптографической защиты информации не способны им противостоять.

Поэтому поддерживаем мнение ведущих специалистов информационного права (А. В. Минбалеева, Т. В. Поляковой, М. Б. Добробабы, К. С. Евсикова и др.) о том, что овладение квантовыми технологиями и создание эффективной системы их нормативного регулирования, включающей правовой, технический и этический компоненты, является объективной потребностью, без которой невозможно обеспечение технологического суверенитета и информационной безопасности государства.

Заключение. Кроме того, учитывая тот факт, что в недалеком будущем квантовые технологии будут способны оказать существенное влияние не только на информационную безопасность государств, но и на отдельно взятых граждан, чьи персональные данные и иная информация, содержащая личную, семейную, банковскую и иные виды тайн, может быть скомпрометирована вследствие применения квантовых коммуникаций, считаем целесообразной в ближайшей перспективе разработку концепции информационной безопасности личности в киберпространстве с включением положений о защите от «квантовой угрозы» и практических шагов, направленных на формирование «квантовой грамотности» у возможного большего числа граждан Российской Федерации.

Список литературы

1. Добробаба М. Б., Чаннов С. Е., Минбалеев А. В. Квантовые коммуникации: перспективы правового регулирования // Вестник Университета имени О. Е. Кутафина. – 2022. – № 4 (92). – С. 25–37.
2. Евсиков К. С. Информационная безопасность цифрового государства в квантовую эпоху // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2022. – № 4(92). – С. 46–58.
3. Козубов А. В., Гайдаш А. А., Кынев С. М., Егоров В. И., Иванова А. Е., Глейм А. В., Мирошниченко Г. П. Основы квантовой коммуникации: часть 1. – СПб.: Университет ИТМО, 2019. – 85 с.
4. Полякова Т. А., Минбалеев А. В., Наумов В. Б. Правовое регулирование квантовых коммуникаций в России и в мире // Государство и право. – 2022. – № 5. – С. 104–114.
5. Холодная Е. В. Квантовые технологии как объект права // Вестник Университета имени О. Е. Кутафина. – 2022. – № 4(92). – С. 38–45.
6. Gromova E.A., Petrenko S.A. Quantum Law: The Beginning. Journal of Digital Technologies and Law. 2023. Т. 1, № 1. Pp. 62–88. https://doi.org/10.21202/jdtl.2023.3. EDN: FKAWRT
7. Minbaleev A., Zenin S., Evsikov K. Prospects for Legal Regulation of Quantum Communication // BRICS Law Journal. – 2024. – Vol. 11, No. 2. – Pp. 11–54.
8. Vavilla Rupesh, Cheemalamarri Venkata Naga Rugvidh, Thatiparthi Subramanya, Prem Rajiv Kumar, S. Kiran, A. Ashok Kumar, Chinnem Rama Mohan. Quantum Secure Communication: A Comprehensive Literary Analysis with In-Depth Insights // Bioscience Biotechnology Research Communications. – 2023. – Vol. 16, No. 3 (July-Aug-Sep). – Pp. 171–177. – URL: https://www.researchgate.net/publication/376378341_Quantum_Secure_Communication_A_Comprehensive_Literary_Analysis_with_In-Depth_Insights (дата обращения: 02.09.2024).
9. Md Jobair Hossain Faruk, Sharaban Tahora, Masrura Tasnim, Hossain Shahriar, Nazmus Sakib. A Review of Quantum Cybersecurity: Threats, Risks and Opportunities // 1-st International Conference on AI in Cybersecurity (ICAIC). At: Victoria, USA. – 2022, May. – Pp. 1–9. – URL: https://www.researchgate.net/publication/360626265_A_Review_of_Quantum_Cybersecurity_Threats_Risks_and_Opportunities (дата обращения: 02.09.2024).

А. И. Химченко,
кандидат юридических наук, доцент,
Московский государственный юридический университет
имени О. Е. Кутафина (МГЮА)

ОТДЕЛЬНЫЕ АСПЕКТЫ РАЗВИТИЯ КВАНТОВЫХ КОММУНИКАЦИЙ: ДОВЕРЕННЫЙ ПОДХОД

Аннотация. В условиях стремительного технологического развития активно создаются инновационные решения и продукты, формируются качественно

новые механизмы и принципы взаимодействия. Целью настоящего исследования стал поиск концептуального подхода к развитию и доверенному функционированию отрасли квантовых коммуникаций, являющейся характерным примером практической реализации таких решений. Предпринята попытка систематизировать взаимосвязь развития отрасли квантовых коммуникаций и повышения безопасности цифровой среды. По результатам исследования выделяются отдельные факторы доверия, формируемые потенциалом технологий квантовых коммуникаций, предложения по совершенствованию отраслевой сертификации.

Ключевые слова: квантовые технологии, доверие, коммуникации, цифровая среда, стандартизация

SELECTED ASPECTS OF QUANTUM COMMUNICATIONS DEVELOPMENT: TRUSTED APPROACH

Abstract. In the context of rapid technological development, innovative solutions and products are being actively created, qualitatively new mechanisms and principles of interaction are being formed. The purpose of this study was to find a conceptual approach to the development and trusted functioning of the quantum communications industry, which is a typical example of the practical implementation of such solutions. An attempt has been made to systematize the relationship between the development of the quantum communications industry and improving the security of the digital environment. According to the results of the study, individual factors of trust are identified, formed by the potential of quantum communication technologies, and proposals for improving industry certification.

Keywords: quantum technologies, trust, communications, digital environment, standardization

Введение. В условиях цифровой трансформации происходит экспоненциальный рост количества информационных массивов и наборов данных, развитие прикладных решений по их аналитике и анализу, создание новых способов взаимодействия и передачи данных. Такое развитие расширяет спектр возможностей в деловом обороте и повседневной жизни, при этом неизбежно увеличивается и потенциал рисков и угроз цифровой среды.

В указанных условиях среди новых технологических направлений и субтехнологических отраслевых решений выделяется отрасль квантовых коммуникаций, которая ввиду своей высокой научной и уже реализованной коммерческой составляющей [1. С. 35], может стать как источником роста стратегических направлений развития секторов экономики, так и драйвером создания новых продуктов и решений в сфере кибербезопасности, повышения защищенности и доверия в цифровой среде.

Потенциал развития и роль в функционировании цифровой среды. В настоящее время квантовые технологии являются одним из ключевых технологических направлений, способных существенно влиять на цифровую среду и особенности ее функционирования. Неслучайно вопросам их развития уделяется внимание в ключевых отраслевых и стратегических документах. Рассматрива-

ются вопросы применения в государственном (муниципальном) управлении, системах высоко- и полностью автоматизированного транспорта, системах управления в машиностроении, металлургии, горной добыче, нефтегазовом секторе, химической промышленности и других отраслях. При этом наиболее емкий потенциал прикладного применения в обеспечении безопасности информационно-телекоммуникационных сетей, вычислительных комплексов и информационной инфраструктуры, создании новых коммуникационных решений и линий квантовой связи.

Так, в соответствии с Указом Президента РФ от 18.06.2024 № 529 технологии защищенных квантовых систем передачи данных входят в перечень важнейших наукоемких технологий. Стратегия развития отрасли информационных технологий определяет квантовые технологии в качестве приоритетной технологии развития отрасли, а решения на основе квантовых технологий признаются в качестве ожидаемых результатов перспективных направлений научных исследований. Концепцией технологического развития квантовые коммуникации и вычисления, а также технологии доверенного взаимодействия отнесены к соответствующим технологическим направлениям. Помимо этого, активное использование решений на основе квантовых технологий предусматривается и стратегическими документами отраслевыми развития.

Доверенный подход. Одним из фундаментальных условий повышения качества цифровой среды является выработка механизмов ее доверенного функционирования, несмотря на то что достижение доверия в цифровой среде в целом является комплексной задачей, предполагающей широкий спектр мер, ключевое значение среди которых имеет безопасность взаимодействия в цифровой среде [2. С. 83].

Значительное увеличение числа дистанционных сервисов и услуг, массовое удаленное трудоустройство и взаимодействие в цифровой среде способствуют увеличению значимости безопасности информации непосредственно в цифровой среде, а также безопасности самих цифровых технологий в числе ключевых факторов, обеспечивающих доверие к ним [3. С. 19].

В указанных условиях высокий технологический потенциал в части реализации защищенного взаимодействия может стать значительным фактором формирования доверенной цифровой среды – использование технологий квантовой коммуникации рассматривается как важный элемент обеспечения информационной безопасности [4. С. 14], в том числе для критической информационной инфраструктуры и защиты отдельных видов информации. При этом Стратегией национальной безопасности обеспечение информационной безопасности на основе квантовых вычислений признается одной из основных задач государственной политики в Российской Федерации

Стоит отметить, что в основе логики реализации технологии квантовых коммуникаций лежит использование доверенных решений – согласно предусмотренному в «дорожной карте» развития «сквозной» цифровой технологии «Квантовые технологии» подходу построение квантовых сетей осуществляется на основе доверенных узлов.

Паспортом «дорожной карты» развития высокотехнологичной области «Квантовые коммуникации» технология доверенных промежуточных узлов в сетях квантового распределения ключей (КРК) отнесена к приоритетным при создании продуктов, тематические НИОКР предусматривают разработку технологии построения доверенных промежуточных узлов в сетях КРК, а мероприятия по созданию магистральных квантовых сетей предусматривает разработку оборудования для организации доверенных промежуточных узлов.

Указанный подход реализован в отечественной и мировой практике – в Российской Федерации создаются линии квантовых коммуникаций через промежуточные доверенные узлы на расстояния до 1000 км, при этом протяженность существующих линий передачи информации на основе квантового распределения ключа с использованием доверенных узлов достигает до 2000 км (Пекин – Шанхай, Китай) [5. С. 2].

Также в контексте доверия следует отметить реализуемый документом «Р 1323565.1.046-2023. Рекомендации по стандартизации. Информационная технология. Криптографическая защита информации. Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации» (утв. и введены в действие Приказом Росстандарта от 30.11.2023 № 1510-ст) доверенный подход – защищенный протокол взаимодействия узла системы выработки и распределения ключей предусматривает доверенный способ доставки двух симметричных ключей при организации ключевой системы.

Вопросы регулирования и стандартизации. Вместе с тем ключевым условием развития и продуктивного использования квантовых технологий, а также соответствующего своему технологическому потенциалу влияния на доверие в цифровой среде является наличие качественных правовых механизмов отраслевого регулирования. Т. А. Полякова еще в 2019 году обращала внимание на актуальность задачи по созданию механизмов правового регулирования отношений в области применения квантовых технологий [6. С. 2].

Не имея целью настоящего исследования рассмотрение особенностей развития отраслевого регулирования квантовых технологий, не являющихся полноценным объектом правового регулирования [7. С. 44] и относимых к terra incognita для отечественной юриспруденции [8. С. 114], отметим, что на сегодняшний день действующее законодательство не содержит профильных норм, а подходы к развитию системы нормативного регулирования в Российской Федерации отрасли квантовых коммуникаций находят отражение лишь на концептуальном уровне.

Вместе с тем отдельное значение приобретают образуемые технологическими особенностями квантовых коммуникаций техническое регулирование и стандартизация. В настоящее время роль реализации правовых механизмов стандартизации значительно повышается, являясь существенной тенденцией регуляторного подхода в цифровой среде.

Указанный подход отражен и в Концепции регулирования отрасли квантовых коммуникаций предусматривающей, что техническое регулирование отрасли квантовых коммуникаций должно основываться на национальных стандартах. При этом совершенствование законодательства о стандартизации отмечено среди

ключевых задач, на решение которых направлено регулирование отрасли квантовых коммуникаций.

В 2023 году был разработан набор предварительных национальных стандартов в сфере квантовых коммуникаций, утв. и введенных в действие Приказами Росстандарта от 11.07.2023 № 22-24-пнст:

«ПНСТ 829-2023. Квантовые коммуникации. Общие положения»;

«ПНСТ 830-2023. Квантовые коммуникации. Термины и определения»;

«ПНСТ 831-2023. Квантовый интернет вещей. Общие положения»;

«ПНСТ 832-2023. Квантовый интернет вещей. Термины и определения».

Вместе с тем полный комплекс отраслевых стандартов в части описания методов построения квантовых сетей, компонентов и сетевых интерфейсов, потенциальных угроз не реализован.

Заключение. Реализация технологии квантовых коммуникаций, имея высокий потенциал обеспечения безопасного взаимодействия, способствует повышению безопасности и доверия в цифровой среде. Кроме того, в условиях возможных квантовых угроз, перед которыми уязвима большая часть алгоритмов шифрования, развитие решений по противодействию становится критически важным вопросом.

Одновременно, для эффективной практической реализации одним из приоритетных вопросов является проведение стандартизации протоколов квантовой коммуникации, что в свою очередь находит отражение в положениях Концепции, фиксирующих необходимость утверждения национальных стандартов, включающих требования к сетям квантовых коммуникаций, оборудованию, программному обеспечению и совместному использованию линий квантовой связи с существующими линиями (сетями) связи.

В указанных условиях представляется целесообразным дополнение текущего перечня предварительных стандартов следующими проектами:

1. Разработка проекта ГОСТ Квантовые коммуникации. Методы построения квантовых сетей.

2. Разработка проекта ГОСТ Квантовые коммуникации. Компоненты и интерфейсы.

3. Разработка проекта ГОСТ Квантовые коммуникации. Модель угроз.

4. Разработка проекта ГОСТ Доверенная среда. Термины и определения.

Список литературы

1. Добробаба М. Б., Чаннов С. Е., Минбалеев А. В. Квантовые коммуникации: перспективы правового регулирования // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2022. – № 4. – С. 25–37. DOI: 10.17803/23115998.2022.92.4.025-037.

2. Химченко А. И. Актуальные информационно-правовые вопросы формирования цифровой среды доверия // Правовое государство: теория и практика. – 2023.– № 4. – С. 78–86.

3. Полякова Т. А., Минбалеев А. В. Понятие и правовая природа «цифровой зрелости» // Государство и право. – 2021. – № 9. – С. 115.

4. Евсиков К. С. Правовое регулирование поддержки отечественных производителей квантовых коммуникаций // Право и цифровая экономика. – 2023. – № 3. – С. 11–19.

5. Постановление Президиума РАН от 18.05.2021 № 79 «О состоянии и перспективах развития квантовых технологий в Российской Федерации».

6. Полякова Т. А. Актуальные проблемы развития системы правового обеспечения информационной безопасности в цифровую эпоху и юридическое образование // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2019. – № 12. – С. 43.

7. Холодная Е. В. Квантовые технологии как объект права // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2022. – № 4. – С. 38–45. DOI: 10.17803/2311-5998.2022.92.4.038-045.

8. Полякова Т., Минбалеев А., Наумов В. Правовое регулирование квантовых коммуникаций в России и мире // Государство и право. – 2022. – № 5. – С. 104–114.

9. Об утверждении приоритетных направлений научно-технологического развития и перечня важнейших наукоемких технологий: Указ Президента РФ от 18.06.2024 № 529 // СЗ РФ. – 2024. – № 26, ст. 3640.

10. Стратегия развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года» Утв. Распоряжением Правительства РФ от 01.11.2013 № 2036-р // СЗ РФ. 2013. № 46, ст. 5954.

11. Прогноз научно-технологического развития Российской Федерации на период до 2030 года (утв. Правительством РФ). URL: http://government.ru (дата обращения - 01.08.2024).

12. Об утверждении Концепции технологического развития на период до 2030 года: Распоряжение Правительства РФ от 20.05.2023 № 1315-р (вместе с «Концепцией технологического развития на период до 2030 года») // СЗ РФ. – 2023. – № 22, ст. 3964.

13. Об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года: Распоряжение Правительства РФ от 24.11.2023 № 3339-р // СЗ РФ. 2023. № 50, ст. 909.

14. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 2 июля 2021 г. № 400 // СЗ РФ. 2021. № 27 (ч. II), ст. 5351.

15. Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии». URL: https://digital.gov.ru/ (дата обращения: 01.08.2024).

16. Постановление Президиума РАН от 18.05.2021 № 79 «О состоянии и перспективах развития квантовых технологий в Российской Федерации».

17. Об утверждении Концепции регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года: Распоряжение Правительства РФ от 11.07.2023 № 1856-р // СЗ РФ. 2023. № 30, ст. 5712.

Е. В. Холодная,
кандидат юридических наук, доцент,
Московский государственный юридический университета
имени О. Е. Кутафина (МГЮА)

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ В ЕС ПЕРИОДОВ ДОСТИЖЕНИЙ КВАНТОВОЙ ЭПОХИ

Аннотация. В статье определены три периода развития достижений в сфере квантовых технологий. Каждый период имеет свое организационное и правовое сопровождение, создавая фундамент для стимулирования технологического прогресса в сфере квантовых технологий и возможностей применения достижений квантовой эпохи в повседневной практической деятельности. Первый период квантовой эпохи определяется выработкой концепций, доктрин и стратегий, создающих предпосылки для наращивания исследований в сфере квантовых технологий для их дальнейшего практического внедрения. В ЕС достигнут второй этап квантовой эпохи, предполагающий создание и внедрение информационной системы «квантовой паутины». Третий этап квантовой эпохи это наращивание квантовой индустрии путем коммерциализации достижений НИР и включения инновационных продуктов в массовый гражданский оборот.

Ключевые слова: информационные технологии; квантовые технологии; квантовая паутина; инфраструктура квантовых коммуникаций, информационный суверенитет

Исследование выполнено за счет гранта Российского научного фонда (проект № 24-18-00950 «Проблемы и перспективы регулирования квантовых коммуникаций в условиях экономики данных»).

LEGAL SUPPORT IN THE EU FOR PERIODS OF ACHIEVEMENT OF THE QUANTUM ERA

Abstract. The author defines three periods of development of achievements in the field of quantum technologies. Each period has its own organizational and legal support, creating a foundation for stimulating technological progress in the field of quantum technologies and the possibilities of applying the achievements of the quantum era in everyday practice. The first period of the quantum era is defined by the development of concepts, doctrines and strategies that create prerequisites for increasing research in the field of quantum technologies for their further practical implementation. The second stage of the quantum era has been reached in the EU, involving the creation and implementation of the "quantum web" information system. The third stage of the quantum era is the development of the quantum industry through the commercialization of research achievements and the inclusion of innovative products in mass civilian circulation.

Keywords: information technologies; quantum technologies; quantum web; infrastructure of quantum communications, information sovereignty.

The research was carried out at the expense of a grant from the Russian Science Foundation (project No. 24-18-00950 "Problems and prospects of regulating quantum communications in a data economy").

Введение. В начале XX века первая квантовая революция позволила понять и использовать основные квантовые эффекты в различных технических устройствах, например, таких как транзисторы и микропроцессоры. Вторая квантовая революция нацелена на использование квантовых эффектов для достижения крупных технологических достижений во многих областях, включая вычисления, сенсорику, метрологию, моделирование, криптографию и телекоммуникации [3. P. 02001], создав предпосылки для будущего квантовой эпохи. Коммерциализация научных достижений в сфере квантовых технологий включает сверхточные датчики для использования в медицине, квантовые коммуникации и квантовое распределение ключей для повышения безопасности цифровых данных [1. С. 25–37]. В перспективе – распознавание закономерностей и обучение систем искусственного интеллекта и др. [7]. Такие глобальные парадигмы технологических возможностей предполагают ориентацию на лучшие мировые практики в сфере развития квантовых технологий, среди которых можно выделить опыт ЕС как одного из флагманов по достижениям в сфере квантовых технологий при высокой организационной и правовой поддержке.

На наш взгляд, предлагаемый опыт может быть использован и РФ во взаимодействии со странами БРИКС и иными дружественными союзами для достижения лидерских позиций в сфере квантовых технологий.

Основная часть. Развитие технологических достижений в преддверии квантовой эпохи предполагает создание организационной поддержки и правового сопровождения данного инновационного направления [2. С. 38–45]. С 1998 года программа Комиссии по будущим и появляющимся технологиям (FET) выделила около 550 млн евро финансирования на квантовые исследования в Европе; через Европейский исследовательский совет (ERC) с 2007 г. профинансировано более 250 исследовательских проектов [8].

На первом этапе развития сферы квантовых технологий уже 2016 году в ЕС был принят Квантовый манифест для выработки единой европейской стратегии для достижения лидерских позиций в квантовую эпоху [10]. В 2018 году было принято Постановление Совета ЕС о создании Европейского объединения высокопроизводительных вычислений для создания экосистемы мирового класса в области суперкомпьютерных и квантовых вычислительных технологий и приложений на территории ЕС. В 2018 году была запущена инициатива «флагман квантовых технологий», объединяющая исследовательские институты, промышленность и государственный сектор, консолидируя и расширяя европейское научное лидерство и передовой опыт в этой области. Таким образом, на первом этапе развития сферы квантовых технологий в ЕС были созданы необходимые организационные и правовые предпосылки для создания инфраструктуры «квантовой паутины».

Второй этап квантовой эпохи предполагается в виде создания и внедрения информационной системы «квантовой паутины»: квантовые компьютеры, симуляторы и датчики связаны между собой с помощью сетей квантовой связи.

В ЕС сегодня поддержка развития и внедрения квантовых технологий осуществляется со стороны программ исследований и космических приложений Horizon Europe [4] и Digital Europe [5]. В 2022 г. объединенный университет

EuroHPC объявил об организации шести площадок по всему ЕС (Чехия, Германия, Испания, Франция, Италия и Польша) для развертывания инфраструктуры квантовых вычислений, доступной европейским ученым и бизнесу через облако на некоммерческой основе.

В 2019 году государства ЕС подписали Декларацию о сотрудничестве в области инфраструктуры связи, обеспечивающей квантовую безопасность (EuroQCI), объединившись при поддержке Европейской комиссии и Европейского космического агентства над развитием инфраструктуры квантовой связи на территории ЕС [12].

Инфраструктура квантовой связи будет интегрировать квантовые технологии и системы в обычные коммуникационные инфраструктуры и состоять из двух элементов:

– наземного компонента, использующего существующие оптоволоконные сети связи, связывающие стратегические объекты на национальном и трансграничном уровнях;

– космического компонента для покрытия больших расстояний по ЕС и другим континентам.

По оценкам специалистов, сейчас первоочередные задачи решаются в области квантового распределения ключей (QKD), т. е. формы шифрования, основанной на принципах квантовой механики для предоставления отправителю и получателю зашифрованного сообщения безопасным способом (методом случайного ключа), для выведения информационной системы из-под возможного контроля извне [14].

К основным предпринятым мерам по созданию инфраструктуры квантовой связи можно отнести:

– организацию двух отраслевых консорциумов для проведения исследований системного проектирования и определения архитектуры EuroQCI;

– с 2023 г. практическое внедрение EuroQC по направлениям реализации: промышленных проектов по разработке ключевых технологических строительных блоков; национальных проектов по основам наземного сегмента инфраструктуры квантовой связи, тестируя различные технологии и протоколы и адаптируя их к конкретным потребностям каждой страны; взаимного сотрудничества по координации и поддержке всех НИР, вопросам стандартизации и др.;

– создание фонда «Соединяя Европу» (CEF) для обеспечения финансирования проектов по развитию трансграничных связей между национальными сетями и взаимосвязей с космическим компонентом EuroQCI;

– в 2024 г. предполагается внедрение инфраструктуры тестирования для оценки и валидации технологий и сервисов квантовой связи;

– на 2026 г. запланировано внедрение космического компонента инфраструктуры квантовой связи, ведутся работы по спецификациям группировки спутников EuroQCI первого поколения [13].

Инфраструктура квантовой связи сможет обеспечивать безопасность финансовых транзакций, обеспечивать передачу, защиту и долгосрочное хранение конфиденциальных данных.

Особое значения для развития сферы квантовых технологий играет принятие в 2020 году Европейской декларации по квантовым технологиям [6], признавшей на наднациональном правовом уровне стратегическое значение квантовых технологий для научной и промышленной конкурентоспособности ЕС и суверенитета ЕС в целом. Основными направлениями деятельности по достижению мирового лидерства и созданию «квантовой долиной» мира на территории ЕС можно назвать: масштабную поддержку НИР, стимулирование квантовых инноваций как в малом бизнесе, так и в крупных промышленных предприятиях; координацию по ускорению перехода от «лаборатории» к «фабрике», в том числе путем устранения логистических пробелов в европейской цепочке поставок, содействие внедрению научных достижений в продукты гражданского и иного оборота; создание сетей кластеров квантовых компетенций для развития квантово-ориентированных, отраслевых исследований, принятие мер по развитию навыков и профессиональной подготовки кадров в сфере квантовых технологий и др.

В 2024 году также принята Рекомендация по скоординированной дорожной карте внедрения перехода к постквантовой криптографии для выработки единой стратегии ЕС, определения единых целей, задач, методов и временных рамок интеграции [11]. Фактически на квантовые технологии делается ставка для обеспечения суверенитета ЕС.

ЕС уже сегодня создает условия для приближения третьего этапа квантовой эпохи [9]. Третий этап квантовой эпохи это развитие квантовой индустрии путем коммерциализации достижений НИР и включения инновационных продуктов в массовый гражданский оборот.

Заключение. Масштабы проектов по квантовым технологиям не могут быть обеспечены исключительно мерами отдельного государства. Для глобального лидерства в области квантовых исследований, а также разработок и внедрения признанных стандартов в сфере квантовых технологий, необходимы усилия для привлечения значительных инвестиций, что возможно в рамках международного сотрудничества и партнерства, поэтому важное значение в данном направлении будут занимать научные исследования, в том числе направленные на поиск оптимального и эффективного нормативного регулирования квантовых технологий [15].

Список литературы

1. Добробаба М. Б., Минбалеев А. В., Чаннов С. Е. Квантовые коммуникации: перспективы правового регулирования // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2022. – № 4(92). – С. 25–37.

2. Холодная Е. В. Квантовые технологии как объект права // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2022. – № 4(92). – С. 38–45.

3. Minbaleev A., Evsikov K Regulation of atmospheric optical quantum communication links // E3S Web of Conferences. 2024. Vol. 541. P. 02001.

4. EU budget: Commission proposes most ambitious Research and Innovation programme yet. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4041 (дата обращения 03.09.2024)

5. EU budget: Commission proposes €9.2 billion investment in first ever digital programme. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4043 (дата обращения: 03.09.2024)

6. European Declaration on Quantum Technologies. URL: https://digital-strategy.ec.europa.eu/en/library/european-declaration-quantum-technologies (дата обращения: 02.09.2024)

7. High performance computing. URL: https://digital-strategy.ec.europa.eu/en/policies/high-performance-computing (дата обарщения: 02.09.2024).

8. Quantum Technologies Flagship kicks off with first 20 projects. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6205 (дата обращения: 03.09.2024).

9. Quantum Technologies Flagship. URL: https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship (дата обращения: 03.09.2024).

10. Quantum Manifesto for Quantum Technologies. URL: https://ec.europa.eu/futurium/en/content/quantum-manifesto-quantum-technologies.html (дата обращения: 03.09.2024).

11. Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. URL: https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography (дата обращения: 03.09.2024).

12. Signed Declaration of Cooperation on Quantum-secure Communication Infrastructure.

13. The European Quantum Communication Infrastructure (EuroQCI) Initiative. URL: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (дата обращения 03.09.2024).

14. The future is quantum: EU countries plan ultra-secure communication network. URL: https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network (дата обращения: 03.09.2024).

15. Громова Е. А., Петренко С. А. Квантовое право: начало // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 62–88. https://doi.org/10.21202/jdtl.2023.3. EDN: FKAWRT

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ТРУДОВЫХ И СВЯЗАННЫХ С НИМИ ПРАВООТНОШЕНИЙ

Е. С. Батусова,
кандидат юридических наук, доцент,
Национальный исследовательский университет
«Высшая школа экономики»

РАБОТНИКИ ЦИФРОВЫХ ПЛАТФОРМ КАК СПЕЦИАЛЬНЫЕ СУБЪЕКТЫ ТРУДОВОГО ПРАВА (НА ПРИМЕРЕ ЗАКОНОДАТЕЛЬСТВА РЕСПУБЛИКИ ЧИЛИ)

Аннотация. В статье анализируется подход законодателей Республики Чили к закреплению трудовых прав работников цифровых платформ, раскрывается содержание правового статуса данных специальных субъектов трудового права. Большое внимание в работе уделяется и характеристике влияния отдельных норм Трудового кодекса Республики Чили на регламентацию труда работников цифровых платформ с 2022 года по настоящее время.

Ключевые слова: трудовое право, работа на цифровых платформах, независимый работник цифровых платформ, зависимый работник цифровой платформы, Трудовой кодекс Чили, права работников цифровых платформ, обязанности работников цифровых платформ, гарантии работникам цифровых платформ

EMPLOYEES OF DIGITAL PLATFORMS AS SPECIAL SUBJECTS OF LABOR LAW (BASED ON THE EXAMPLE OF THE LEGISLATION OF THE REPUBLIC OF CHILE)

Abstract. In this article the approach of the legislators of the Republic of Chile to the consolidation of the labor rights of employees of digital platforms is analyzed, it reveals the content of the legal status of these special subjects of labor law. Much attention is also paid to the characterization of the impact of certain norms of the Labor Code of the Republic of Chile on the regulation of the work of employees of digital platforms from 2022 to the present.

Keywords: labor law, work on digital platforms, independent employees of digital platforms, dependent employee of a digital platform, the Labor Code of Chile, rights of employees of digital platforms, obligations of employees of digital platforms, guarantees of employees of digital platforms

Введение. Инновационным достижением трудового права Чили как отрасли и как науки является его вклад в разработку проблемы правового регулирования труда платформенных работников. В Чили в 2022 году впервые в мире в Трудовом кодексе был закреплен трудо-правовой статус работников цифровой платформы (Глава X Трудового кодекса Чили «Работа через цифровые сервисные платформы»). Это неслучайно, так как Чили имеет самый высокий доход на душу

населения в Латинской Америке и относится к категории стран с высоким уровнем дохода, по данным Всемирного банка [3]. Ранее в некоторых странах (например, Хорватии, Италии, Канаде (провинции Онтарио) предпринимались попытки по закреплению правового статуса работников цифровых платформ, однако в законодательстве этих стран отсутствовал комплексный подход. Например, регламентировалось право доставщиков еды и таксистов на ограничение рабочего времени, однако трудовые права платформенных работников не закреплялись полном объеме в кодифицированном акте. В Чили же трудо-правовой статус платформенного работника зафиксировали именно в Трудовом кодексе.

Основная часть. Принятие Главы X ТК Чили «Работа через цифровые сервисные платформы» было обусловлено необходимостью устранения ряда причин, которые приводили к ухудшению положения работников цифровых платформ, а именно: несоблюдение ограничения рабочего времени, низкой оплаты, отсутствия охраны труда; зависимость от администрации цифровых платформ и т. д. Обратим внимание и на то, что большую часть пользователей платформ составляли мигранты, так как труд в этой сфере рассматривался как низкоквалифицированный [7].

По нашему мнению, проблема статуса работников цифровых платформ в Чили имеет много общего с проблемами аналогичных работников в других странах мира. Ее сущность заключается в том, что, с одной стороны, экономике требуется гибкое регулирование сферы труда, которое достигается посредством функционирования подобных цифровых платформ, а с другой – необходима защита прав лиц, работающих с этими платформами посредством признания их работниками. Чилийские законодатели попытались решить эту проблему посредством принятия X главы Трудового кодекса.

В этой связи интересным представляется социологическое исследование, проведенное в 2024 году рядом ученых [4]. Они выявили закономерность, которую описали на основании балльной системы (от 1 до 5). Суть этой закономерности заключается в том, что в 2021 году до принятия главы X Трудового кодекса Чили условия труда работников в сфере функционирования цифровых платформ были несправедливыми. Это, например, относилось к такой знаменитой чилийской цифровой платформе, как Кабифи (Cabify), которая предоставляет услуги такси. В 2021 году были выявлены следующие нарушения: таксистам не гарантировалось получение минимальной заработной платы, не обеспечивалась охрана труда и свобода объединений для защиты своих прав [5].

После принятия изменений в Трудовой кодекс в 2022 году о цифровых платформах положение работников в Кабифи резко улучшилось. В 2024 году закреплено правило оплаты не ниже минимального размера оплаты труда, снизились риски при выполнении заказов, введен порядок разрешения конфликтных ситуаций между работниками и администрацией платформы, достигнут баланс в управлении персоналом и компанией [6].

По предложенной учеными балльной системе в 2021 году условия труда работников Кабифи оценивалось на 1 балл, а в 2024 году – на 5 баллов. Налицо положительная динамика.

Чилийские исследователи Родриго Паломо Велес, Пабло Контерас, Мария Солидад Жофре Бустос, Альфредо Сьера Херреро отмечают, что споры об условиях труда платформенных работников возникают в основном в больших городах. Этими спорами являются: споры о несправедливом увольнении, нарушении прав при увольнении, компенсации за ущерб при выполнении работы [8].

Проанализируем правовой статус работников цифровых платформ Чили, закреплённый в Трудовом кодексе Чили [2], с целью изучения возможности использования рекомендаций для российского законодателя.

Введенная Законом № 21.431а глава X Трудового кодекса Чили «Работа с использованием цифровых платформ» располагается в разделе о специальных договорах с отдельными категориями работников, например, в сфере воздушного транспорта, сельского хозяйства, спортсменов, надомных работников, дистанционных работников. Таким образом, раздел закрепляет как дифференциацию по отраслям экономики, так и по способу связи с работодателем.

В данной главе дается определение субъектов цифровых платформ с точки зрения трудового права. Работники разделяются на зависимых и независимых. Отдельно закреплено, что цифровая платформа должна быть зарегистрирована в качестве юридического лица. Данное требование делает незаконным функционирование платформ без образования юридического лица. Таким образом, предотвращается риск еще большей незащищённости работников платформ, при котором физическое лицо без регистрации занималось бы организацией платформенной занятости, например, в даркнете.

Специалисты МОТ отмечают, что Чили относится к странам, которые в законах, содержащих нормы о платформах, исключают отдельные виды экономической деятельности [1. С. 43]. Сделанное чилийским законодателем в данном случае исключение касается сайтов компаний рекламного характера, чьей целью не является собственно сопровождение платформенной занятости и контактирования в целях непосредственно организации обеспечения оказания услуг или работ посредством связи потенциального клиента и предоставляющего свои услуги, даже если посредством этого сайта или платформы стороны могут иметь возможность заключить договор.

При определении является ли лицо зависимым работником или независимым необходимо выявить, обладает ли оно признаками, закрепленными в статье 7 Трудового кодекса, а именно: наличием индивидуального трудового договора, в котором устанавливается право на получение оплаты труда за работу при подчинении работника правилам, установленным работодателем. Работник может предоставлять адресные услуги либо сам, либо от имени других, но обязательно в связи с запросом, полученным посредством использования программы на цифровой платформе. На таких работников распространяются общие как для зависимых, так и независимых работников права, закреплённые в главе X Трудового кодекса Чили.

В правовой статус зависимых работников цифровых платформ входят следующие права:

1. Информировать до принятия заказа о месте выполнения работы, оплате, клиенте, а при оказании транспортных услуг – дополнительно адресе начала оказания и окончания маршрута.

2. Право на информацию и охрану персональных данных работника и право получить в течение 15 рабочих дней ответ на запрос о доступе к результатам оценивания и критериям, которые влияют на выполнение работы, например, правильное отражение данных о квалификации. Формат полученных данных должен позволять работнику обрабатывать их. Дополнительным механизмом охраны трудовых прав работников является закрепления права проверок и надзора государственных органов, права на доступ к алгоритмам, которые используются при принятии решений, данных, которые используются для наладки и иные данные, требуемые для анализа соблюдения законности при функционировании платформы.

3. Запрещение дискриминации работников при применении программ выдачи заказов, алгоритмов расчета всех составляющих вознаграждения. Бездействие в отношении работников также рассматривается как дискриминация. Программа обеспечения устранения дискриминации должна доводиться до работников, и работодатель должен ее соблюдать и разъяснять механизмы ее действия.

4. Право на охрану труда должен обеспечить работодатель, что проявляется в обучении современным методам проведения работ, обеспечение сертифицированных средств индивидуальной защиты при работе в сфере транспорта и последующей их сдаче после оказания услуг. Страхование личного имущества, используемого при оказании услуг, с суммой покрытия, рассчитанной за годовой период. Данные гарантии распространяются как на зависимых работников, так и независимых занятых посредством платформы.

5. Компенсация при прекращении трудового договора рассчитывается исходя из среднегодового размера вознаграждения за последний год при исключении неотработанных месяцев из периода расчета.

6. Право на объединение в профессиональные союзы для защиты прав всех типов работников платформ и ведение коллективных переговоров, при возможности платформенных организаций объединиться для ведения переговоров о заключении договоров, если они согласны, или индивидуально вести их.

Также предусмотрено введение контроля за соблюдением прав платформенных работников, и применение санкций в виде штрафов, размер которых повышается вдвое при повторном нарушении закона платформой.

Обратимся к перечню прав независимых работников цифровых платформ, т. е. тех, кто не заключил индивидуальный трудовой договор, и обязанностей цифровой платформы. Ее администрация обязана только обеспечивать обмен информацией между клиентами и независимыми исполнителями-работниками посредством использования программ на платформе и при соблюдении установленных общих условий.

Платформа и независимый исполнитель обязаны заключить договор в письменной форме, в котором должны быть сведения о сторонах; составляющие постоянной и переменной части вознаграждения или ставки в местной валюте при описании критериев получения переменной части; описание механизма осуществления связи и дальнейшей коммуникации между клиентами, обращающимися к платформе, и независимым работником; конкретная территория оказания услуг или правил ее определения (отсутствие этого условия означает, что работник сам выбирает территорию); конфиденциальности в отношении персональных

данных работника; максимальный временной период непрерывного подключения к платформе и период отключения от платформы для отдыха; судебный орган для разрешения споров; официальный способ передачи независимым работником претензий платформе по вопросам платежей и оцениванию оказанных услуг, а также ответственное должностное лицо для связи или очного обращения по конкретному адресу платформы; основания расторжения договора платформой, сроки их применения; правила оказания услуг на платформе. Стороны также могут вносить в договор дополнительные условия после переговоров.

Независимый исполнитель вправе начать работать на платформе только после подписания договора. Таким образом, фактического допуска к программной оболочке будет недостаточно для вступления в отношения по оказанию услуг на платформе. Это позволит избежать споров о законности оказания услуг при фактическом допуске. Также работник получает свой экземпляр в бумажном или электронном виде, а работодатель должен разместить договор в базе договоров при обеспечении возможности допуска к этой базе независимого работника-исполнителя с целью как ознакомиться, так и сохранить себе копию договора. Платформа должна обеспечивать такое подключение круглосуточно и для разных по характеристикам устройств независимого исполнителя. Таким образом, должна отсутствовать дискриминация по признаку характеристик технических средств для подключения платформа, т. е. работник не должен быть зависим от работодателя в части обязанности приобретения у работодателя каких-то конкретных технических средств с определенными работодателем характеристиками. Это дает работнику возможность выбирать разные средства для связи с платформой.

Работник имеет право получать зарплату не реже чем раз в месяц, при этом работодатель обеспечивает работника программными средствами перевода платежей, с данной суммы подлежит удержанию подоходный налог, перечисление которого лежит на платформе. Также налоги будут удерживаться и с платформы. Платформа проверяет, выдает ли работник клиентам платежные документы о факте оказания услуг и их оплаты, если налоговые органы не внедрили бездокументную отчетность по налогам и оплате. Платформа должна устанавливать оплату каждого часа работы не ниже суммы минимального установленного законом размера оплаты труда в месяц, рассчитанного пропорционально от показателя минимального ежемесячного дохода, увеличенного на 20 процентов за время подготовки к работе. При этом в случае, если рассчитанная сумма заработанных средств оказывается ниже этого показателя, то платформа доплачивает работнику до этого минимума. Работник также, выплачивая страховые выплаты, имеет право на получение пенсии, медицинское страхование, страхование от несчастных случаев и профессиональных заболеваний, получения инвалидности. Это не обязательные платежи, независимым работником они выплачиваются по желанию.

Право на ограничение рабочего времени также выражается в 12 часах временного отключения от платформы без санкций за невыполнение заказов в это время, это отключение не может использоваться как санкция за отказ от получения и выполнения заказов независимым работником.

При расторжении договора с работником, продолжительность работы которого более 6 месяцев, платформа обязана его уведомлять не позднее, чем за месяц

до последнего дня работы. Это не относится к увольнению работника за серьезные нарушения условий, закрепленных в договорном порядке. Работник также имеет право требовать у платформы соблюдения условий договора.

Работники, чья продолжительность работы в неделю составляет в среднем не менее 30 часов в неделю на протяжении не менее 3 месяцев имеют право на защиту от дискриминации за членство в профсоюзе, участие в коллективных переговорах и профсоюзной деятельности и возмещения вреда, причиненного работнику платформой. При подсчете часов учитывается только время, потраченное на оказание услуг работником.

Таким образом, мы видим, что в Трудовом кодексе Чили закреплен правовой статус как зависимого работника платформы, который заключает трудовой договор, так и независимого работника, заключающего договор с платформой. Страхование возможно и в том, и в другом случае, но независимый работник сам решает платить ли ему страховые платежи.

Что касается охраны оплаты труда, то этот механизм функционирует и в том, и в другом случае и оплачивается не только время работы, но время подготовки к работе, т. е. ожидания, например, время проезда для оказания транспортных услуг.

Важной особенностью является обучение охране труда и одной и другой категории работников, при этом законодательно установлено, что предоставление, например, специальной одежды не означает, что независимый работник подпадает под хозяйскую власть работодателя и правовой статус независимого работника меняется на зависимого, и он действует в интересах и под контролем платформы – работодателя.

Наличие периода времени включения и отключения от платформы, т. е. рабочего времени и времени отдыха, не является также признаком переквалификации независимого работника в зависимого. Тем более первый свободен в принятии или непринятии заказов через платформу.

Таким образом, в Трудовом кодексе Чили закреплены два типа организации работы на платформах: посредством трудового договора и оформления статуса самозанятого независимого работника.

Мы видим постепенное сближение этих двух правовых статусов, т. е. гибкое регулирование, в котором заинтересована работодатель-платформа и жесткое регулирование, например в сфере охраны труда, в котором заинтересован не только работник, но и государство.

Одновременно в трудовом договоре в части оплаты труда закреплена только местная валюта, нет указания о возможности оплаты иной валютой, например, криптовалютой; таким образом, также государством охраняются права этих двух категорий работников платформ.

Заключение. Анализ чилийского законодательства о статусе работников цифровых платформ позволяет сделать вывод о появлении позитивной тенденции – закрепление трудовых прав работников цифровых платформ, что имеет большое значение не только для Чили, но и для других стран мира, законодатели которых пока окончательно не определились со статусом данных субъектов права. Полагаем, что положительный правовой опыт Чили в данной сфере может быть использован и для совершенствования российского трудового законодательства.

Список литературы

1. Обеспечение достойного труда в платформенной экономике. – Женева: Международное бюро труда, 2024. – 146 с.
2. Código del Trabajo. Edición preparada en formato electrónico por el Boletín Oficial. Actualizada hasta el 26 de agosto de 2024. – URL: https://www.dt.gob.cl/legislacion/1624/w3-article-95516.html (дата обращения: 06.08.2024).
3. Economía de Chile. Ministerio de Relaciones Exteriores. – URL: https://www.chile.gob.cl/iran/sobre-chile/economia-de-chile/economia-de-chile (дата обращения: 07.09.2024).
4. Graham M., Arriagada A., Bertolini A., Egaña P.. Fair Work Chile Ratings. – URL: https://fair.work/en/ratings/chile (дата обращения: 06.09.2024).
5. Graham M., Arriagada A., Bertolini A., Egaña P.. Fair Work Chile Ratings. 2021. – URL: https://fair.work/en/ratings/platforms/chile-cabify/?tabfor2021 (дата обращения: 06.09.2024).
6. Graham M., Arriagada A., Bertolini A., Egaña P.. Fair Work Chile Ratings. 2024. – URL: https://fair.work/en/ratings/platforms/chile-cabify/?tabfor2024 (дата обращения: 06.09.2024).
7. New regulation of platform work in Chile fails to tackle power imbalances between platforms and workers. – URL: https://fair.work/en/fw/blog/chile-regulation-missed-opportunity (дата обращения: 07.09.2024).
8. Rodrigo Palomo Vélez, Pablo Contreras, María Soledad Jofré Bustos, Alfredo Sierra Herrero. El debate sobre la laboralidad del trabajo vía plataformas digitales en Chile y algunos problemas conexos. Revista Latinoamericana de Derecho Social. August 2022. DOI: 10.22201/iij.24487899e.2022.35.17272. – URL: https://www.researchgate.net/publication/368378187_El_debate_sobre_la_laboralidad_del_trabajo_via_plataformas_digitales_en_Chile_y_algunos_problemas_conexos (дата обращения: 06.09.2024).

Т. Б. Иванова,
доктор экономических наук, профессор,
Волгоградский институт управления –
филиал Российской академии народного хозяйства
и государственной службы при Президенте Российской Федерации

СОВЕРШЕНСТВОВАНИЕ СОЦИАЛЬНОЙ ЗАЩИТЫ ГРАЖДАН ПРИ ПОВЫШЕНИИ ВАРИАТИВНОСТИ ФОРМ ЗАНЯТОСТИ С УЧЕТОМ ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Аннотация. Цель данного исследования – проанализировать вариативность отношений занятости с учетом применения цифровых технологий как основы принятия решений для совершенствования социальной защиты граждан. Гипотеза: вариативность форм занятости с учетом применения цифровых технологий возрастает, появляются их новые сочетания, что усложняет нормирование формирования социальных отчислений. Подтверждение данной гипотезы было

получено на основе анализ форм занятости, принятой Международной организацией труда. На основе этого были обоснованы предложения по изменению подходов определения страховых взносов. Основываться при их исчислении не на отчислениях от полученных доходов, а от обязанности для каждого лица сформировать определенную ежегодную величину взносов на социальные цели. Это создаст дополнительный инструмент сокращения теневой экономики и при использовании цифровых технологий является достижимым.

Ключевые слова: трудовое право, цифровые технологии, трудовые правоотношения, наемные работники, самозанятые, зависимые подрядчики, платформенные занятые, социальная защита граждан.

Работа выполнена при финансовой поддержке Российского научного фонда и Комитета экономической политики и развития Волгоградской области по гранту № 24-28-20066 https://rscf.ru/project/24-28-20066/

IMPROVING THE SOCIAL PROTECTION OF CITIZENS WHILE INCREASING THE VARIABILITY OF FORMS OF EMPLOYMENT, TAKING INTO ACCOUNT THE USE OF DIGITAL TECHNOLOGIES

Abstract. The purpose of this study is to analyze the variability of employment relations, taking into account the use of digital technologies as a basis for decision-making to improve social protection of citizens. Hypothesis: the variability of forms of employment, taking into account the use of digital technologies, is increasing, new combinations of them appear, which complicates the rationing of the formation of social contributions. Confirmation of this hypothesis was obtained on the basis of an analysis of the forms of employment adopted by the International Labour Organization. Based on this, proposals were substantiated to change the approaches to determining insurance premiums. When calculating them, they should not be based on deductions from income received, but on the obligation for each person to form a certain annual amount of contributions for social purposes. This will create an additional tool for reducing the shadow economy and is achievable when using digital technologies.

Keywords: labor law, digital technologies, labor relations, employees, self-employed, dependent contractors, platform employees, social protection of citizens**.**

The article was prepared with the financial support of the Russian Science Foundation and the Committee for Economic Policy and Development of the Volgograd Region under grant No. 24-28-20066 https://rscf.ru/project/24-28-20066/

Введение. Человека создал труд – это высказывание является аксиомой и показывает длительную историю существования трудовой деятельности. Ее современные контуры сформировались в процессе становления рыночных отношений, развитие которых шло на протяжении всего XX века. В статье [1] показано, что уже для этого периода характерно увеличение разнообразия форм правового оформления исполнителей, повышение социальной защищенности работников. Но в связи с появлением новых субъектов хозяйственной деятельности, возникает необходимость уточнения их специфики как основы неизбежности выполнения

связанных с ними обязательств. Прежде всего, к ним относится социальная защищенность граждан, которая в настоящее время должна в обязательном порядке обеспечиваться при формировании трудовых правоотношений.

В то же время социальные льготы, присущие трудовым отношениям как фактору повышения стоимости выполнения трудовых функций, всегда воспринимаются работодателями отрицательно. Чтобы сократить эти расходы и не иметь обязательств перед работниками в соответствии с нормативно-правовой базой трудовых отношений, еще в начале XX века анализировалась возможность личного участия в производственном процессе не только на основе договора найма, но и гражданско-правового [6]. До сих пор эти различия в подходах к оценке характера трудовой деятельности остаются остро дискуссионными. Смещение акцента в пользу заключения договоров гражданско-правового характера при использовании этих двух форм привлечения гражданина к работе широко распространено и в настоящее время, причем в различных странах. Если отношения не строятся по типу трудовых, то решение социальных проблем человека за счет отчислений от собственных ранее полученных доходов отсутствует, перекладывается на плечи государства как форма предоставления социальной поддержки за счет иных, не гражданином сформированных источников, вызывает необходимость повышения бюджетных расходов на его содержание. Поэтому вопрос о том, являются ли те или иные отношения трудовыми, по-прежнему остается значимым и дискуссионным.

В Трудовом кодексе РФ определено, что трудовые отношения связаны с выполнением работником за плату указанных работодателем функций, под контролем последнего и в созданной им инфраструктуре (условия труда, нормативно-правовые акты, коллективные договоры) [7. Ст. 15, 56]. Именно такой подход к взаимодействию между исполнителем и нанимателем ведет к наложению на последнего обязанности обеспечить защищенность работника. В тоже время появляются новые явления, требующие оценки характера отношений между работником и нанимателей. Так, Постановлением Пленума Верховного Суда РФ от 29.05.2018 № 15 [3] этот вопрос рассматривается для регулирования труда работников, работающих у работодателей – физических лиц и работодателей – субъектов малого предпринимательства, в том числе микропредприятий. В нем акцентировано внимание, что признаками трудовых отношений являются также личное выполнение работ, их постоянный характер, интегрированность работника в организационную структуру работодателя, получение заработка как единственного или основного. При наличии оснований для признания отношений трудовыми перед работодателем возникает обязанность выплаты социальных отчислений и исполнения иных обязательств, установленных нормативными актами (еженедельные выходные, ежегодные отпуска). В качестве примера анализа характера отношений при осуществлении хозяйственной деятельности в Постановлении Верховного Суда РФ приводится договор возмездного оказания услуг. Выявляется, сохраняет ли работник самостоятельность, работает ли на свой риск, исходя из лично установленного графика, является ли результатом работы оказание услуги, а не выполнение трудовых функций. Из всех параметров сохранение работником самостоятельности является важнейшим критерием для отсутствия признания его участником трудовых отношений.

Цель данного исследования – проанализировать вариативность отношений занятости с учетом применения цифровых технологий как основы принятия решений для совершенствования социальной защиты граждан. Гипотеза исследования: отношения между исполнителем работ и нанимателем становятся все более разнообразными, но пока не во всех из них присутствуют элементы социальной защиты. Это приводит к необоснованному увеличению расходов бюджета на социальные цели в виде поддержки слоев населения, которые не уплачивали отчисления на социальные нужды, но государство вынуждено оказывать им поддержку как малоимущим. Кроме бюджетных потерь, это стимулирует развитие теневой экономики, так как если действует модель получения, например, пенсии не ниже прожиточного минимума без соответствующих отчислений, то по отношению к текущим доходам стимулируется их укрытие. Тем более что дифференциация размера социальной пенсии и начисленной исходя из пенсионных отчислений в настоящее время незначительна. Задачи, решенные для реализации цели исследования: 1) выявление вариативности форм занятости с учетом цифровых технологий, 2) анализ моделей формирования отчислений на социальные нужды и их связь с оценкой взаимоотношений между исполнителем и нанимателем как трудовых правоотношений при различных формах занятости, 3) разработка предложений по совершенствованию социальной защиты граждан в условиях повышения вариативности трудовых правоотношений под влиянием применения цифровых технологий.

Основная часть. Результаты анализа. Выявление вариативности форм занятости с учетом цифровых технологий показало, что согласно рекомендациям Международной организации труда (МОТ), при обследовании рабочей силы (ОРС) [4] статус занятости в настоящее время классифицируют по типам властных полномочий (степени контроля работников над своей деятельностью) и экономических рисков (подверженность потере ресурсов при выполнении работы). В первом случае работники делятся на независимых (владеют экономической единицей, контролируют её деятельность) и зависимые (не имеют полной власти или контроля над экономической единицей, в которой они работают). Во втором – работают за прибыль или за заработную плату. Сопряженность классификаций работников по статусам занятости показана в табл. 1. Как видим, полной сопряженности классификаций работников по статусам занятости типа властных полномочий и экономических рисков совпадают друг с другом частично. Все наемные работники одновременно являются зависимыми, работающими за зарплату. На семейных предприятиях работодатели и самозанятые, ориентированные на рынок, без наемных работников имеют общий статус занятости – работающие за прибыль.

Помимо статуса, оценивается занятость населения в неформальном секторе, под которым понимаются хозяйственные единицы без государственной регистрации в качестве юридического лица. К ним относятся индивидуальные предприниматели (ИП); наемные работники, работающие у них или у физических лиц; члены семьи, помогающие при ведении собственного дела; занятые в собственном домашнем хозяйстве, направленного на обмен или продажу произведенных, выращенных, полученных на охоте активов; индивидуальные работники без образова-

ния ИП. Кроме того, занятость может быть основной и/или дополнительной; дистанционной с удаленной работой в течение всех дней недели или нескольких; платформенной.

Таблица 1

Сопряженность классификаций статусов занятости работников по типу властных полномочий и экономических рисков (составлено автором на основе [4])

Статус по типу властных полномочий	**Группы работников**	**Статус по экономическим рискам**
Зависимые работники	Наемные работники: постоянные, нанятые на ограниченный срок, случайные, по краткосрочным контрактам, оплачиваемые стажеры, ученики, интерны	Работающие за зарплату
Независимые работники	Работодатели в компании	
	Владельцы-управляющие компании без наемного труда	
	Работодатели на семейных предприятиях	Работающие за прибыль
	Самозанятые на семейных предприятиях без наемного труда	
Зависимые работники	Зависимые подрядчики	
	Помогающие на семейных предприятиях	

Анализ действующей в настоящее время методологии обследования рабочей силы, принятой в мире, показывает существенную вариативность форм занятости, которая за счет применения цифровых технологий усиливается. При этом сопряженность всех используемых классификаций, по аналогии приведенной в табл. 1, отсутствует. Из занятых в неформальной экономике к определенному статусу по типу властных полномочий и экономических рисков относятся помогающие на семейных предприятиях. Они являются работающими за прибыль зависимыми лицами.

В табл. 2 приведены результаты анализа сопряженности вариантов форм занятости по вышеприведенным классификациям, используемым при обследовании рабочей силы.

Аргументируем приведенные в таблице данные. Занятость в неформальном секторе отмечена как возможная во всех ситуациях, где деятельность может проводиться в качестве индивидуального предпринимательства. Указано на невозможность занятости как неформальной для работодателей в компании и владельцев-управляющих компаний без наемного труда, так как сам термин «компания» подразумевает существование юридического лица.

Таблица 2

Матрица сопряженности вариантов форм занятости [составлена автором]

Группы работников	Тип властных полномочий	Статус по экономическим рискам	Занятость в неформальном секторе	Основная работа	Дополнительная работа	Дистанционная работа	Платформенная занятость
Найм постоянный	З	ЗП	+/-	+/-	+/-	+/-	-
Найм на ограниченный срок	З	ЗП	+/-	+/-	+/-	+/-	-
Найм случайный	З	ЗП	+/-	-	+/-	+/-	-
Найм по короткому контракту	З	ЗП	+/-	+/-	+/-	+/-	-
Оплачиваемые стажеры, ученики, интерны	З	ЗП	+/-	+/-	+/-	+/-	-
Зависимые подрядчики	З	П	+/-	-	+/-	+/-	+/-
Помощники на семейных предприятиях	З	П	+/-	+/-	+/-	+/-	+/-
Работодатели на семейных предприятиях	НЗ	П	+/-	+/-	+/-	+/-	+/-
Самозанятые на семейных предприятиях без наемного труда	НЗ	П	+/-	+/-	+/-	+/-	+/-
Работодатели в компании	НЗ	ЗП	-	+	+	+	+/-
Владельцы-управляющие компании без наемного труда	НЗ	ЗП	-	+	+	+	+/-

Условные обозначения: работники: З – зависимые, НЗ – независимые, работающие: П – за прибыль, ЗП – за заработную плату, возможность существования данной характеристики занятости в неформальном секторе, в качестве основной и дополнительной работы, дистанционной, при платформенной занятости – «+» – возможна, «–» – невозможна.

Вид занятости как основной работы невозможен, если найм случайный, так как она в силу неожиданности своего характере не может давать постоянный источник средств существования. Все виды работ могут создавать условия для дополнительной подработки. Аналогично и дистанционно могут выполняться любые работы, если для этого существуют необходимые удаленные технологии. Оценка платформенной занятости проведена, исходя из её специфики, сложившейся в настоящее время в России. Наличие наемных работников на платформах признание не получило, а стажировки не приняты, если только речь не идет о штатных работниках, обеспечивающих работу цифровой плат. Для регистрации на платформе надо быть самозанятым, индивидуальным предпринимателем, физическим или юридическим лицом. В остальных приведенных в таблице случаях зарегистрироваться и выполнять заказы на основе платформенной информации возможно в зависимости от формы, в которой будет выступать занятый. Зависимыми подрядчиками, работодателями на семейных предприятиях, работодателями в компаниях, владельцами-управляющими компаниями без наемного труда могут быть юридические лица, помощниками на семейных предприятиях – физические.

Таким образом, сложившаяся в мировой практике система учета форм занятости не позволяет однозначно отнести те или иные из них к трудовым. Предполагается, что необходимо использование дополнительных критериев для обоснования возникновения трудовых правоотношений в каждом конкретном случае. Это вызывает дополнительные сложности в реализации прав и обязанностей граждан, вызывая необходимость в отдельных случаях в индивидуальном порядке отстаивать свое право на получение отчислений на социальные нужды от работодателей или появление когнитивного диссонанса, при появлении необходимости самому принимать решения об их перечислении, при естественном стремлении отказаться от этих платежей для повышения своих текущих доходов.

Анализ моделей формирования отчислений на социальные нужды и их связь с оценкой взаимоотношений между исполнителем и нанимателем как трудовых правоотношений при различных формах занятости был проведен по материалам Налогового кодекса Российской Федерации (НК РФ). В разделе XI НК РФ [2] регламентируется перечень плательщиков страховых взносов, объекты налогообложения, базы исчисления, установлена предельная величина базы для исчисления страховых взносов на обязательное социальное страхование. Сопоставление приведенного в статье 34 НК РФ перечня плательщиков с формами занятости, согласно классификации МОТ, показывает, что обязательность платежей существует по всем из них, за исключением платформенных занятых. При этом «если плательщик относится одновременно к нескольким категориям, … он исчисляет и уплачивает страховые взносы отдельно по каждому основанию» [2. Ст. 34]. Идет расширение объектов налогообложения страховыми взносами. Так, 31.07.2023 года в их перечень были введены гражданско-правовые договоры на выполнение работ и оказание услуг.

В настоящее время в этот перечень не попадают самозанятые, численность которых на 31.07.2024 составила 10 984 938 человек, в том числе физических лиц – 10 447 351, остальные – индивидуальные предприниматели [5]. Индивидуальные предприниматели должны осуществлять социальные отчисления в обязательном порядке, к самозанятым – физическим лицам такое требование в настоящее время не предъявляется. До 2028 года изменений их режима налогообложения не планируется. Однако активно ведется работа по расширению числа лиц, добровольно уплачивающих взносы на социальное страхование. В настоящее время доля отчисляющих средства на пенсионное обеспечение составляет около 3% общей численности самозанятых. В московском регионе такие взносы добровольно делают 5,6 тыс. человек. Минимальный размер отчислений составляет 50 798,88 руб., максимальный – 406 391,04 рубля.

Увеличение числа лиц, имеющих право на социальную защиту – важное направление деятельности по отношению к самозанятым во всем мире. Международная организация труда уделяет существенное внимание выравниванию условий существования для граждан, работающих в различных формах занятости, особое внимание уделяя в последние годы платформенным работникам [8, 9].

В настоящее время принято, что отчисления на социальные нужды определяются конкретным видом деятельности, которым занимается гражданин. Исследование сопряженности вариантов форм занятости показывает, что они могут выполняться работником в самых различных сочетаниях. Сокращению теневой экономики будет способствовать введение обязанности гражданина уплачивать не менее определенной величины пенсионных отчислений. В этом случае бюджет СФР будет экономить средства в размере социальной пенсии по старости, которая в настоящее время, начисляется лицам, которые не заработали права на страховую пенсию по старости и поэтому получают социальную. Кроме того, принцип «социальные отчисления от человека, а не от вида формы его занятости» будет формировать ответственную модель поведения без расчета на патернализм государства. Это более уместно при появлении значительных миграционных потоков, которые формируются последние годы в связи с кризисными событиями в различных странах.

Заключение. Повышение вариативности форм занятости с учетом цифровых технологий, которые, с одной стороны, ведут к их разнообразию, с другой, создают возможности контроля за поведением каждого индивида, создают предпосылки для изменения формирования системы социальных отчислений граждан. Это позволит решить многовековой спор о необходимости делать социальные отчисления при наличии только трудовых правоотношений и определять их характер при разных формах занятости. Социальная защита должны быть присуща не конкретной форме занятости, а конкретному работнику, так как в течение жизни он может выступать в различных ролях и использовать разные виды занятости. Использование принципа «социальные отчисления от человека, а не от вида формы его занятости» позволят внедрять модель, при которой каждый будет понимать свою ответственность за получение различных социальных льгот. В условиях цифровизации формируется технологическая основа для проведения подобной работы. Ведение реестров ИНН, СНИЛС создают для этого высокотехнологичную основу.

Список литературы

1. Иванова Т. Б., Миронова С. М. Сравнительный анализ развития традиционных и платформенных отношений занятости // Вестник Московского университета. Серия 6. Экономика. – 2024. – № 59(4). – С. 135–159. https://doi.org/10.55959/MSU0130-0105-6

2. Налоговый кодекс Российской Федерации (с изм. и доп., вступ. в силу с 08.09.2024) // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_28165 (дата обращения: 05.09.2024).

3. О применении судами законодательства, регулирующего труд работников, работающих у работодателей – физических лиц и у работодателей - субъектов малого предпринимательства, которые отнесены к микропредприятиям. Постановлением Пленума Верховного Суда РФ от 29.05.2018 № 15 [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_299109 (дата обращения: 05.09.2024).

4. Об утверждении основных методологических и организационных положений по проведению выборочного обследования рабочей силы (с изм. на 22 марта 2024 года. Приказ Росстата от 29.12.2-24 № 707 [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_467194 (дата обращения: 05.09.2024).

5. Сведения о количестве самозанятых граждан, зафиксировавших свой статус и применяющих специальный налоговый режим «Налог на профессиональный доход» [Электронный ресурс] // Официальный сайт ФНС. – URL: https://rmsp.nalog.ru/statistics2.html?ysclid=m0tnv8eiyq267285026 (дата обращения: 05.09.2024).

6. Таль Л. С. Трудовой договор: цивилистическое исследование. Ч. 1. Общие учения. Тип. Яросл. губ. правления. – 1913. – 422 с.

7. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ в ред. от 08.08.2024 [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_34683 (дата обращения: 05.09.2024).

8. Realizing decent work in the platform economy Fifth item on the agenda International Labour Office. – Geneva. 2024. – 124 p. [Electronic resource]. – URL: https://www.ilo.org/esource/conference-paper/ilc/113/realizing-decent-work-platform-economy (date of application 05.09.2024).

9. Social security for self-employed workers. International Labour Office. Geneva. January 2023 [Electronic resource]. – URL: https://www.ilo.org/resource/article/social-security-self-employed-workers (date of application 05.09.2024).

А. А. Сапфирова,
доктор юридических наук, доцент,
Кубанский государственный аграрный университет имени И. Т. Трубилина

ИСПОЛЬЗОВАНИЕ РАБОТОДАТЕЛЯМИ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ТРУДОВЫХ ОТНОШЕНИЯХ: ПЕРСПЕКТИВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Аннотация. Исследуя вопросы правового регулирования использования цифровых технологий в трудовых отношениях, автор подчеркивает несовершенство норм трудового права в этом вопросе. В результате рассматривается использование цифровых технологий при ведении работодателем электронного кадрового документооборота, обработка им персональных данных работников в электронной форме, а также при коллизии норм о трудовом и гражданско-правовом регулировании возникших отношений. Автор предлагает установить обязательность для работодателей ведение электронного кадрового документооборота; считать работодателя добросовестным до тех пор, пока он не будет включен в реестр работодателей с нелегальной занятостью или реестр работодателей с просроченной заработной платой или не достигнет индикатора риска; закрепить в Трудовом кодексе РФ четкую обязанность работодателя о наличии согласия работника на обработку его биометрических данных при использовании цифровых технологий для контроля за процессом реализации работником трудовой функции.

Ключевые слова: цифровые технологии, работники, трудовые отношения, электронный кадровый документооборот, персональные данные

Исследование выполнено за счет гранта Российского научного фонда № 24-28-20205, https://rscf.ru/project/24-28-20205/ и Исследование выполнено при финансовой поддержке Кубанского научного фонда в рамках проекта № 24-28-20205

USE OF DIGITAL TECHNOLOGIES BY EMPLOYERS IN LABOR RELATIONS: PROSPECTS FOR LEGAL REGULATION

Abstract. Exploring the issues of legal regulation of the use of digital technologies in labor relations, the author emphasizes the imperfection of labor law norms in this matter. As a result, the use of digital technologies is considered when an employer maintains electronic personnel document management, processes personal data of employees in electronic form, as well as in the event of a conflict of norms on labor and civil law regulation of the relations that have arisen. The author proposes to establish the obligation for employers to maintain electronic personnel document management; to consider the employer in good faith until he is included in the register of employers with illegal employment or the register of employers with overdue wages or reaches the risk indicator; to enshrine in the Labor Code of the Russian Federation a clear obligation of the employer to have the employee's consent to the processing of his biometric data when using digital technologies to monitor the process of the employee's implementation of the labor function

Keywords: digital technologies, employees, labor relations, electronic personnel document management, personal data

The research is carried by a grant of the Russian Science Foundation № 24-28-20205, https://rscf.ru/project/24-28-20205/ and The research is carried out with financial support of the Kuban Science Foundation in the frame work of the scientific project Num. 24-2820205

Введение. Цифровые технологии стремительно включаются в современное правовое поле. Развивающаяся цифровизация не могла не затронуть и трудовые отношения. Появляются новые возможности для быстрого оформления кадровых документов и кадровых процессов. Однако определенная консервативность, присущая нормам трудового права, замедляет процесс внедрения «цифры». Возможно, в этом есть положительный момент, поскольку быстрая цифровизация трудовых отношений может негативно отразиться на занятости граждан, на выборе направлений их трудоустройства (не могут же все быть специалистами в IT-сфере). К тому же не все работодатели могут коренным образом перестроить свои взаимоотношения с работниками в столь короткие сроки, хотя те сроки, в которые внедряются цифровые технологии в трудовые отношения, нельзя назвать длительными.

Несомненно, наука не может не анализировать элементы взаимодействия и воздействия цифровых технологий на правоотношения. Появились монографии, научные статьи, посвященные влиянию цифровых технологий на трудовые отношения [1–5].

Основная часть. Анализ действующего законодательства, специальной литературы позволяет утверждать, что цифровые технологии в трудовых отношениях могут быть использованы работодателем в разных формах, а их правовое регулирование осуществляется не в полном объеме. Нам представляются перспективными такие направления использования цифровых технологий в трудовых отношениях, как ведение электронного кадрового документооборота и обработка персональных данных работников в электронной форме. Рассмотрим их по порядку.

1. Ведение кадрового электронного документооборота (КЭДО). При этом надо иметь в виду, что ряд документов (их совсем немного, и они перечислены в ст. 22.1 Трудового кодекса Российской Федерации (далее – ТК РФ): бумажная трудовая книжка, приказ о прекращении трудового договора, акт по форме Н-1, инструктажи по охране труда) оформляются в бумажном виде. Конечно, работодатель должен оформлять в электронном виде сведения о трудовой деятельности (на практике так называется «электронная» трудовая книжка), но бумажная трудовая книжка до сих пор ведется, если работник указал об этом в заявлении либо оказался «молчуном».

В настоящее время работодателями используются такие программы КЭДО, как HRlink, СБИС, Контур и т. д. Положительные и отрицательные стороны каждой из программ работодатели смогут узнать при их применении, но надо подчеркнуть, что ТК РФ пока не обязывает работодателей внедрять КЭДО. Согласно ст. 22.2 ТК РФ, это право работодателя. Аналогичное право есть и у работника отказаться от применения в трудовых отношениях с работодателем КЭДО. Правда, наличие этого права работника не позволяет работодателю эффективно управлять организацией, если один из всех работников не согласиться на КЭДО (на практике такие случаи имеют место быть). Нам представляется, что если ТК РФ закрепляет

право работодателя на использование КЭДО, то у работника должна быть обязанность согласиться с выбором работодателя. Это целесообразно и разумно с управленческой точки зрения. В противном случае введение КЭДО – это не право работодателя, а его законный интерес, не обеспеченный принудительной силой государства.

Для введения КЭДО работодатель должен разработать локальные нормативные акты, содержание которых определено в ст. 22.2 ТК РФ. Полагаем, что в ст.22.2 ТК РФ необходимо внести изменения и ввести обязательность КЭДО для каждого работодателя и работника, поскольку преимущества данной формы использования цифровых технологий очевидны. Для сторон трудовых отношений – это прозрачность трудовых отношений; возможность без труда доказать правомерность действий (бездействия) при потенциальных трудовых разногласиях и спорах. Есть еще одна немаловажная деталь для работодателя: введение КЭДО – это сокращение человеческих ошибок на подготовку и ведение кадровой документации как внутри работодателя, так и во внешних отношениях (например, при сдаче отчетности в органы занятости населения, в СФР и т. д.). Правда, технические ошибки все же могут иметь место. Так, работодатель через КЭДО отправил ЕФС-1 с неверным регистрационным номером страхователя. Организация представила уточняющий отчет, но Социальный фонд РФ не посчитал этот факт уважительной причиной непредоставления отчета в установленный срок. Работодателя привлекли к административной ответственности. Суд решил, что своевременное отправление отчета с технической ошибкой не может образовать состав административного правонарушения как не подача отчета.

В другом примере работодатель случайно по технической ошибке (определил суд в решении по иску ООО «АЭРОСТАР МСК» к Г.А.И.) перевел работнику заработную плату за декабрь 2022 года не 22 462,78 рублей, а 1 722 462,78 рублей, что на 1,7 млн рублей больше. Согласно ст. 137 ТК РФ, удержанию подлежит сумма, выплаченная в результате счетной, а не технической ошибки, отказал в иске работодателю.

Для государства преимущества ведения КЭДО, на наш взгляд, наиболее очевидны, нежели для работника и работодателя. КЭДО – это основа для внедрения системы государственного электронного надзора.

Заметим, что в ст. 214.2 ТК РФ предусмотрено право работодателя предоставлять Роструду дистанционный доступ к наблюдению за безопасным производством работ, а также к базам электронных документов работодателя в области охраны труда. Иными словами, в ст. 214.2 ТК РФ предусматривается правовая возможность осуществления государственного электронного надзора органом государства, но только при реализации работодателем права доступа. Однако с введением обязательного для работодателя КЭДО, думается, предоставление дистанционного доступа Роструду станет обязанностью работодателя.

2. Использование цифровых технологий в трудовых отношениях «помогает» взимать недоплаченные работодателями суммы в соответствующий бюджет. Так, обрабатывая информацию, полученную от работодателей в виде отчетов, федеральная налоговая служба (ФНС) получает сведения не только о нарушениях

трудовых прав, но и контролирует «работу» индикаторов риска. В частности, отслеживая деятельность индивидуальных предпринимателей (ИП) и самозанятых, ФНС может предполагать о наличии или отсутствии трудовых отношений между работодателем и, например, самозанятым. На основе сформированных теорией [6; 7; 8] и практикой признаках трудовых отношений ФНС выработала критерии цифрового разграничения трудовых и гражданско-правовых отношений и стала активно применять их на практике. Правда, возникает конкуренция компетенций ФНС, Роструда и суда в этом вопросе. В частности, в ст. 19.1 ТК РФ ФНС как субъект, правомочный и способный признать отношения трудовыми, отсутствует. Однако ФНС на данный факт не обращает внимания, видимо, считая его пробелом ст. 19.1 ТК РФ, ожидающим своего восполнения.

В случае признания ФНС возникших правоотношений трудовыми, она вправе доначислить страховые взносы и НДФЛ. Не согласный с этим работодатель может обратиться в Арбитражный суд, оспаривая действия ФНС, но, к сожалению, судебная практика складывается не в пользу работодателей. Одновременно указанную информацию ФНС направляет в Роструд, полномочный принимать меры по привлечению работодателей к ответственности, причем независимо от судебного спора с ФНС. Деятельность межведомственной комиссии по противодействию нелегальной занятости, созданной после 1 марта 2024 года в каждом субъекте РФ, логически продолжает показывать преимущества использования работодателями КЭДО. С 1 января 2025 года начнет действовать реестр работодателей с нелегальной занятостью, в который будут поступать первые сведения об этих работодателях. Подчеркнем, что и работодатели, допустившие просрочку выплаты заработной платы, подвергнутся аналогичным действиям со стороны государства: вызов на межведомственную комиссию субъекта РФ, включение в соответствующий реестр.

3. Обработка персональных данных работников в электронной форме – это третий пример использования цифровых технологий в трудовых отношениях. Надо сразу отметить, что в настоящее время обработка персональных данных работников, как правило, происходит без применения информационных систем. Тот документ, который специалист отдела кадров формирует в соответствующих программах на компьютере, а потом подписывает личной либо электронной подписью, не означает применение информационной системы работодателем, которая вообще не предполагает наличие бумажного документа. Возможно, с введением обязательного использования каждым работодателем КЭДО обработка персональных данных работников будет осуществляться исключительно в электронной форме с применением информационных систем.

Персональные данные работников разделяются на три вида: общие, специальные и биометрические. Электронная форма их обработки предполагает наличие ответа на вопрос: наличие (отсутствие) согласия на обработку. В современных условиях Роскомнадзор придает огромное значение наличию обязательного согласия на обработку персональных данных. В противном случае работодатель может быть привлечен к административной ответственности, предусмотренной ст. 13.11 КоАП РФ. Подчеркнем, что эти правоотношения регулируются ст. 6 Федерального

закона «О персональных данных», которая не во всех случаях диктует наличие обязательного согласия работника на обработку персональных данных.

Итак, в соответствии со ст. 214.2 ТК РФ работодатель вправе использовать в целях контроля за безопасностью производства работ приборы, устройства, оборудование и (или) комплексы (системы) приборов, устройств, оборудования, обеспечивающих дистанционную видео-, аудио- или иную фиксацию процессов производства работ, обеспечивать хранение полученной информации.

Согласно ст. 11 Федерального закона «О персональных данных», использование работодателем биометрии (физиологические и биологические данные о человеке) предполагает наличие письменного согласия работника, если целью является установление личности работника. К биометрическим данным относятся фото-, видеофиксация цветного изображения работника и звук его голоса.

При анализе приведенных выше положений возникает вопрос: необходимо ли работодателю получить письменное согласие работника в случае использования работодателем видеосъемки процесса на производстве? На первый взгляд, ответ очевиден: да, должен. Однако так ли это? Минтруд РФ свою позицию не определил, сославшись на конкретные ситуации, решаемые в судебном порядке.

С одной стороны, применение цифровых технологий в трудовых отношениях предоставляет право работодателю контролировать процесс производства, даже если придется с помощью фото- или видеофиксации идентифицировать работника, нарушающего, например, технологию производства или дисциплину труда, обязанность соблюдения которой указана в ст. 21 ТК РФ. В данном случае право работодателя не должно нарушать права работника на обработку его биометрии, соответственно требуется согласие работника на фото- или видеофиксацию процесса его труда. Эту позицию можно встретить и в судебных решениях.

С другой стороны, фото- или видеофиксация, установленная работодателем, и о которой уведомлен работник, может осуществляться с целью контроля за использованием рабочего времени работником в интересах работодателя, мониторинга эффективности трудозатрат, а не с целью идентифицировать работника с помощью биометрии. Поэтому и согласия работника на обработку его биометрии не требуется. И эту позицию можно встретить и в судебных решениях.

Во второй позиции, на наш взгляд, имеет место подмена целей. Зачем работодателю достижение цели контроля за использованием рабочего времени работниками? Если только для анализа трудозатрат, как указано в вышеприведенном примере, то, видимо, обработка биометрии будет отсутствовать. Однако, если конечная цель работодателя состоит все же в том, чтобы привлечь к дисциплинарной ответственности конкретного работника, используя данные фото- или видеофиксации, то очевидна цель – обработка биометрии, прикрытая другой целью – анализ трудозатрат. Заметим, что именно такая ситуация и имела место во втором случае. Полагаем, суд не обратил внимание на этот немаловажный факт, в связи с чем и решил, что отсутствие согласия на обработку биометрии правомерно.

Заключение. Резюмируя изложенное, считаем, что, во-первых, введение обязательного для работодателей КЭДО позволит полномочным органам государства более взвешенно, адресно и оперативно реализовывать контрольную функцию, а работодателям – быстрее и активнее осуществлять кадровые процессы. Во-

вторых, принцип добросовестности работодателя, закрепленный в ст. 8 Федерального закона «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации», приобретет цифровое подтверждение: если работодатель будет отсутствовать в реестре работодателей с нелегальной занятостью или с просроченной заработной платой, значит, предполагается его добросовестность в трудовых отношениях до тех пор, пока он не «перешагнет» индикатор риска. В-третьих, использование цифровых технологий для контроля за процессом реализации работником трудовой функции (не важно с какой первоначальной целью) во многих случаях имеет конечную цель – привлечение (или угрозу привлечения) к дисциплинарной ответственности работника, а значит, его идентификацию, что требует согласия работника на обработку его биометрии. Это положение целесообразно отразить в ТК РФ.

Список литературы

1. Беляева И. Я., Черняева Д. В. Особенности регулирования трудовых отношений в условиях цифровой экономики / под ред. проф. Ю. П. Орловского. – М., 2018. – 158 с.

2. Драчук М. А. Цифровизация отношений как вектор государственного управления в сфере труда // 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. 3. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. – С. 131–138.

3. Сапфирова А. А. Защита трудовых прав в условиях цифровой экономики: монография. – Краснодар, 2021. – 86 с.

4. Терелянский П. В., Титор С. Е., Косарин С. П., Стрельникова И. А., Милькина И. В. Цифровые технологии государственных услуг в области содействия занятости населения и исполнения контрольно-надзорных функций в сфере труда: монография. – Москва, 2020. – 372 с.

5. Филипова И. А. Влияние цифровых технологий на труд: ориентиры для трудового права: монография – Нижний Новгород: Нижегородский госуниверситет им. Н. И. Лобачевского, 2021. – 106 с.

6. Александров Н. Г. Трудовое правоотношение. Монография. – М.: Юридическое издательство министерства юстиции СССР, 1948. – 336 с.

7. Кузьменко А. В. Предмет трудового права России: опыт системно-юридического исследования. – СПб.: Юридический центр Пресс, 2005. – 274 с.

8. Таль Л. С. Трудовой договор. Цивилистическое исследование. Ч. 1. Общие учения. Ярославль: Тип. Губернского правления, 1913. – XII. – 422 с.

К. Л. Томашевский,
доктор юридических наук, профессор,
Казанский инновационный университет имени В. Г. Тимирясова

ОПЫТ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ ТРУДОВЫХ ОТНОШЕНИЙ (НА ПРИМЕРЕ БРАЗИЛИИ И ЕВРОПЕЙСКОГО СОЮЗА)

Аннотация. В статье анализируется недавний опыт законодательных инициатив по регулированию применения систем искусственного интеллекта в Бразилии и Европейском Союзе. Цель статьи – сопоставить опыт законотворческих разработок в сфере использования систем ИИ в аспекте трудовых отношений и сферы занятости в Бразилии и Европейском Союзе. Использован комплекс общенаучных и специальных методов исследования, в особенности сравнительно-правовой, конкретно исторический и формально-юридический. Зарубежный опыт правового регулирования трудовых отношений в данной сфере может представлять интерес в процессе разработки нормативных правовых актов, касающихся пределов использования систем ИИ, в России и других стран СНГ и ЕАЭС.

Ключевые слова: искусственный интеллект, система ИИ, законопроект, нейросети, рынок труда, занятость, трудовые отношения

EXPERIENCE OF LEGISLATIVE REGULATION OF THE APPLICATION OF AI SYSTEMS IN THE FIELD OF EMPLOYMENT RELATIONS (BASED ON THE EXAMPLE OF BRAZIL AND THE EU)

Abstract. The article analyzes the recent experience of legislative initiatives to regulate the use of artificial intelligence systems in Brazil and the European Union. The purpose of the article is to compare the experience of legislative developments in the field of using AI systems in the aspect of labor relations and employment in Brazil and the European Union. The article uses a complex of general scientific and special research methods, especially comparative legal, specifically historical and formal legal. Foreign experience in the legal regulation of employment relations in this area may be of interest in the process of developing regulatory legal acts regarding the limits of the use of AI systems in Russia and other CIS and EAEU countries.

Keywords: artificial intelligence, AI systems, bill, neural networks, labor market, employment, employment relations

Введение. Цифровые технологии и системы искусственного интеллекта (далее – ИИ) находят все боле широкое распространение в современном мире, включая трудовые отношения и сферу занятости. Повсеместное применение ИИ создает угрозу занятости людей, вытеснению представителей ряда профессий с рынка труда, вызывает потребность в правовом регулировании ограничения ее использования в определенных сферах общественных отношений.

Заметим, что анализ понятия ИИ, систем ИИ и технологии ИИ и их соотношение с роботами и нейросетями был всесторонне проанализирован в недавней статье И. А. Филиповой [3]. Последняя выделила два суперпризнака ИИ (интел-

лектуальная система и система неестественного происхождения), которые распадаются на ряд субпризнаков [3. С. 150–151]. В легальных определениях систем ИИ в новейшем законодательстве РФ и зарубежных стран эти признаки в том или иной виде находят свое закрепление.

В этой связи представляет научный интерес обращение к опыту законодательного регулирования и законопроектных инициатив в зарубежных странах, где данные вопросы в той или иной степени нашли свое урегулирование применительно к использованию систем ИИ, в том числе в сфере трудовых отношений и занятости. Для примера сравнительно-правового исследования в настоящей статье будут взяты Бразилия и Европейский Союз. Цель статьи – сопоставить опыт законотворческих разработок в сфере использования систем ИИ в аспекте трудовых отношений и сферы занятости в Бразилии и Европейском Союзе. В статье использован комплекс общенаучных и специальных методов исследования, в особенности сравнительно-правовой, конкретно исторический и формально-юридический.

Основная часть. В 2021 г. в Бразилии был принят законопроект 21/20 (разработчик – Эдуардо Бисмарк), который устанавливает основы и принципы разработки и применения ИИ в Бразилии, перечисляя руководящие принципы для продвижения и действий органов государственной власти по этому вопросу. Палата депутатов одобрила его 29.09.2021, а затем и Сенат. Государственные органы, согласно данному закону, должны действовать, чтобы стимулировать обучение и подготовку людей к реструктуризации рынка труда и поощрять инновационные педагогические практики с междисциплинарным видением, которое влияет на процесс подготовки учителей. Одна из разработчиков законопроекта Луиза Канциани подчеркнула, что «законопроект не следует европейской модели в отношении априорного запрета определенных видов ИИ или того, что представляет собой высокий риск, оставляя эти определения на более позднее отраслевое регулирование или саморегулирование» [4].

Технологию ИИ в Бразилии с 2023 г. стали внедрять даже в законодательный процесс. Так, в конце 2023 г. в Бразилии был принят первый в мире закон, полностью написанный с помощью нейросети ChatGPT. Этот закон бы принят на муниципальном уровне в столице бразильского штата Риу-Гранди-ду-Сул. По сообщениям СМИ, этот законопроект написан нейросетью по запросу члена городского совета Р. Росариу и позволяет муниципалитету не взимать с налогоплательщиков плату за замену счетчиков воды в случае их кражи. Документ был одобрен советом и подписан мэром С. Мелу. Любопытно, что о факте разработки законопроекта нейросетью все члены горсовета, а также мэр с горожанами узнали уже после принятия закона [1].

Запланированное на начало июля 2024 г. голосование по новому законопроекту (PL) № 2338/2023, регулирующему использование ИИ в Бразилии, было отложено в Сенате. Текст обсуждается специальным комитетом Палаты представителей, но сталкивается с оппозицией со стороны некоторых секторов, в том числе Национальной конфедерации промышленности (CNI) и цифровых платформ. Решение о новой отсрочке объявил президент коллегии Карлос Виана. Законопроек-

том, автором которого является президент Палаты представителей Родриго Пачеко, устанавливаются общие и национальные правила «разработки, внедрения и использования, ответственного за ИИ системы. Докладчиком по законопроекту является сенатор Эдуардо Гомес. Последний представил замену первоначальному тексту, предложенную председателем Сената Родриго Пачеко – автором первоначального законопроекта [4]. Предложение было основано на проекте, представленном комиссией юристов, которая изучала эту тему в 2022 году. Согласно последней поправке, из регулирования законом исключены системы ИИ, разработанные исключительно для целей национальной обороны, предназначенные для исследовательской деятельности и не представленные на рынке. Кроме того, системы ИИ, используемые физическими лицами только в личных, неэкономических целях, также не подлежат регулированию. Согласно тексту законопроекта, перед вводом в эксплуатацию система ИИ должна пройти предварительную оценку, которую проводят разработчики и поставщики. Целью является определение степени риска приложения. Если законопроект получит одобрение специального комитета, в котором он сейчас обсуждается, текст будет направлен на пленарное заседание [5].

Теперь обратимся к недавно принятому Регламенту ЕС 2024/1689 Европейского парламента и Совета ЕС от 13 июня 2024 г., устанавливающему гармонизированные правила в области искусственного интеллекта и вносящие поправки в Регламенты (ЕС) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) № 2018/858, (ЕС) № 2018/1139 и (ЕС) №2019/2144 и Директивы 2014/90/EU, (EU) 2016/797 и № 2020/1828 (далее – Акт ЕС об ИИ) [6, 8].

Вначале обратим внимание, что в зависимости от риска причинить вред пользователю Акт ЕС об ИИ классифицирует все системы ИИ на три категории: 1) запрещенные системы (с недопустимой степенью риска); 2) системы ИИ с высокой степенью риска; 3) остальные системы ИИ.

Согласно п. 2 ст. 2 того же Акта, для систем ИИ с высокой степенью риска в соответствии со статьей 6(1), относящихся к продуктам, на которые распространяется гармонизированное законодательство Союза, указанное в разделе B Приложения I, применяются только статья 6(1), статьи 102–109 и статья 112. Статья 57 Акта применяется только в той степени, в которой требования к системам ИИ высокого риска в соответствии с настоящим Регламентом были интегрированы в это гармонизированное законодательство Союза.

Согласно приложению III «Системы искусственного интеллекта высокого риска, упомянутые в статье 6(2)» Акта ЕС об ИИ, к данным системам отнесены «занятость, управление работниками и доступ к самозанятости», а именно:

(a) системы ИИ, предназначенные для использования для набора или отбора физических лиц, в частности, для размещения целевых объявлений о вакансиях, для анализа и фильтрации заявлений о приеме на работу, а также для оценки кандидатов;

(b) системы ИИ, предназначенные для принятия решений, влияющих на условия трудовых отношений, продвижения или прекращения трудовых договорных отношений, распределения задач на основе индивидуального поведения или

личных качеств или характеристик или для мониторинга и оценки производительности и поведение лиц в таких отношениях.

В сравнительно-правовом плане мы наблюдаем схожий подход к отнесению систем, предназначенных для использования для набора или отбора физических лиц, в частности, для размещения целевых объявлений о вакансиях, для анализа и фильтрации заявлений о приеме на работу, а также для оценки кандидатов, ранее апробированный в бразильском законопроекте № 2338/2023.

Как отмечает А. Ж. Степанян, «сферу применения Акта об ИИ можно охарактеризовать экстерриториальностью и вменением в связи с тем, что разработчик и поставщик системы не вполне могут ожидать и предвидеть даже не клиентов, а применение такими клиентами результатов деятельности систем» [2. С. 96]. Этот тезис можно распространить и на работодателей, являющихся резидентами различных стран ЕС, в том числе и по вопросам подбора, найма и увольнения работников из чиста трудящихся-мигрантов. При этом разработчики систем ИИ могут находиться, к примеру, в США, Индии или России.

К. Галлезе-Нобиле, проведя исследование регулирования умных роботов и искусственного интеллекта в Европейском Союзе по состоянию на 2023 г., сделал вывод том, что «выработка полного и согласованного законодательства по робототехнике в Европе еще далека от завершения, учитывая быстрое развитие ИИ и многообразие типов устройств, которые могут использоваться в самых разных сферах нашей жизни. Каждая такая сфера имеет свои особенности, поэтому желательно наряду с общими законами – об искусственном интеллекте и о киберустойчивости – задействовать множество других правовых инструментов, мер, инструкций, стандартов, относящихся к различным отраслям» [8. P. 52]. Данный подход следует поддержать, поскольку параллельно с разработкой и принятием общего законодательного акта об ИИ и умной робототехнике (как это уже было реализовано в ЕС) следует адаптировать к нему и нормы отраслевого законодательства, в том числе о труде (в особенности институт охраны труда), а также множество технических нормативных правовых актов, действующих в указанной сфере.

Заключение. Проведенный в статье краткий сравнительно-правовой анализ законодательных инициатив в Бразилии и Акта ЕС об ИИ показывает, что в целом при наличии определенных особенностей в обоих правопорядках за основу законодательного регулирования взята классификация систем ИИ в зависимости от риска причинить вред пользователю. При этом системы ИИ, предназначенные в целях использования для набора или отбора физических лиц, в частности, для размещения целевых объявлений о вакансиях, для анализа и фильтрации заявлений о приеме на работу, а также для оценки кандидатов; принятия решений, влияющих на условия трудовых отношений, продвижения или прекращения трудовых отношений, относятся к системам ИИ с высоким риском. Последнее должно отражаться на дополнительных требованиях к проверке и оценке таких систем ИИ на стадии их внедрениях в практическое использование. Важно также учитывать, что указанные системы ИИ распространяются не только на подбор и наем работников, но и на доступ к самозанятости, т. е. на большинство платформенных занятых.

Список источников

1. Бушев А. В Бразилии приняли первый в мире закон, разработанный нейросетью // Российская газета. 5.12.2023. – URL: https://rg.ru/2023/12/05/v-brazilii-priniali-pervyj-v-mire-zakon-razrabotannyj-nejrosetiu.html (дата обращения: 17.08.2024).
2. Степанян А. Ж. Регламент Европейского Союза об искусственном интеллекте (Artificial Intelligence Act): первый взгляд на проект // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2021. – №7. – С. 93–98.
3. Филипова И. И. Искусственный интеллект, робот и нейротехнологии: понятие, соотношение и пределы правового регулирования // Государство и право. – 2024. – №4. – С. 148–158.
4. Câmara aprova projeto que regulamenta uso da inteligência artificial Caberá à União legislar e editar normas sobre o tema Compartilhe Versão para impressão Comentários, 29/09/2021 [Electronic resource] // Agência Câmara de Notícias. – URL: https://www.camara.leg.br/noticias/811702-camara-aprova-projeto-que-regulamenta-uso-da-inteligencia-artificial (дата обращения: 17.08.2024).
5. Projeto de lei N° 2338, de 2023 Dispõe sobre o uso da Inteligência Artificial. Autoria: Senador Rodrigo Pacheco (PSD/MG) [Electronic resource] // URL: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1723640838762&disposition=inline (дата обращения: 17.08.2024).
6. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 [Electronic resource] // OJ L. – 2024/1689. – 12.7.2024. – URL: http://data.europa.eu/eli/reg/2024/1689/oj (дата обращения: 17.08.2024).
7. Sampaio Cr. PL que regulamenta Inteligência Artificial no Brasil tem votação novamente adiada no Senado; entenda disputa [Electronic resource] // Brasil de Fato | Brasília (DF). – 09 de julho de 2024. – URL: https://www.brasildefato.com.br/2024/07/09/pl-que-regulamenta-inteligencia-artificial-no-brasil-tem-votacao-novamente-adiada-no-senado-entenda-disputa (дата обращения: 17.08.2024).
8. Gallese Nobile C. Regulating Smart Robots and Artificial Intelligence in the European Union // Journal of Digital Technologies and Law. – 2023. – T. 1, № 1. – Pp. 33–61. https://doi.org/10.21202/jdtl.2023.2. EDN: UNSONV.

Ю. О. Шишкина,
ООО «Центр правовой поддержки»

ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА РАБОТУ РУКОВОДИТЕЛЯ ОРГАНИЗАЦИИ

Аннотация. В данной статье рассматриваются полномочия руководителя организации, а также различные сферы применения искусственного интеллекта в процессе его работы. Проанализированы трудности применения искусственного

интеллекта в работе организации президентом компании. Устанавливаются преимущества и недостатки для внедрения в работу искусственного интеллекта на предприятии – как для руководителей организации, так и для работников. Анализируются нормативные правовые акты, регулирующие вышеуказанные правоотношения. В заключение автор приходит к выводу, что применение искусственного интеллекта руководителем организации в настоящее время не урегулировано трудовым законодательством Российской Федерации. Возникает много вопросов и проблем при применении искусственного интеллекта директором фирмы применительно к трудовым отношениям.

Ключевые слова: руководитель организации, работник, искусственный интеллект, трудовые отношения

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE WORK OF THE HEAD OF THE ORGANIZATION

Abstract. This article discusses the powers of the head of the organization. There are also various fields of application of artificial intelligence by the head of the organization. The difficulties of using artificial intelligence in the work of the organization by the president of the company are analyzed. The advantages and disadvantages for the implementation of artificial intelligence in the enterprise, both for the heads of the organization and for employees, are established. The normative legal acts regulating the above-mentioned legal relations are analyzed. In conclusion, the author concludes that the use of artificial intelligence by the head of the organization is currently not regulated by the labor legislation of the Russian Federation. There are many questions and problems when using artificial intelligence by the director of a company in regulating labor relations.

Keywords: the head of the organization, the employee, artificial intelligence, labor relations

Введение. В настоящее время искусственный интеллект стремительно завоевывает все сферы влияния, не оказались в стороне и трудовые отношения. С появлением искусственного интеллекта и внедрением его в работу многих предприятий появились сложности нормативного правового регулирования данных отношений. На законодательном уровне до сих пор не урегулирована степень взаимоотношений искусственного интеллекта и руководителя организации, а также работников. Возникает много вопросов при определении степени ответственности и поиска виновных лиц при сбое в системе искусственного интеллекта. Также возникает много вопросов, что делать, если искусственный интеллект вытеснит много профессий и создаст массовую безработицу. В настоящее время требуется пересмотреть действующее трудовое законодательство, а также четко определить сферы внедрения технологии искусственного интеллекта в работу организации.

Основная часть. На сегодняшний день искусственный интеллект активно внедряется во все сферы человеческой жизни. Трудовое право также не стало исключением. В настоящий момент искусственный интеллект помогает руководителю организации в работе, а также способствует оптимизации процессов в организации.

Как отмечает С.Ю. Головина, «в условиях рыночной экономики с ее многообразными формами собственности на средства производства формируется рынок труда, для которого характерна конкуренция… Трудовые отношения, как неотъемлемая часть экономических отношений, отражают все трудности переходного периода от плановой экономики к рыночной…» [1. С. 20, 22].

Можно отметить, что искусственный интеллект в каких-то сферах труда и вытесняет работников, но директора компании в настоящий момент он заменить не может, он лишь помогает ему в работе.

Законодатель, пытаясь упорядочить данные отношения с помощью вновь издаваемых законов, создал на практике очень много проблем как для руководителей организации, так и для компаний в целом. При этом в процессе нормативного регулирования наблюдался определенный «крен» именно в сторону норм гражданского права, что вызывает вопросы.

В настоящий момент правовое регулирование искусственного интеллекта в сфере трудовых отношений составляет:

Постановление Правительства РФ от 18 апреля 2016 г. № 317 «О реализации Национальной технологической инициативы» [2], Указ Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [3] и иные нормативные правовые акты.

Так, в п. 9 Распоряжения Правительства РФ от 24 ноября 2023 г. № 3339-р «Об утверждении Стратегии развития отрасли связи РФ на период до 2035 г.» указано, что «решениями проблемы дефицита кадров в российской отрасли связи являются повышение качества образования и подготовки, актуализация образовательных программ с учетом возможностей современных технологий и требований работодателей, сокращение сроков разработки и внедрения новых программ, усиление взаимодействия организаций сферы образования с операторами связи, разработчиками телекоммуникационного оборудования и иностранными образовательными организациями, а также популяризация профессий отрасли связи» [4].

Существует несколько подходов к определению руководителя организацией, так, в соответствии со ст. 273 ТК РФ под руководителем организации понимается «физическое лицо, которое в соответствии с настоящим Кодексом, другими федеральными законами и иными нормативными правовыми актами Российской Федерации, законами и иными нормативными правовыми актами субъектов Российской Федерации, нормативными правовыми актами органов местного самоуправления, учредительными документами юридического лица (организации) и локальными нормативными актами осуществляет руководство этой организацией, в том числе выполняет функции ее единоличного исполнительного органа» [5].

В соответствии со ст. 2 Федерального закона «О несостоятельности (банкротстве)»: … руководитель …– единоличный исполнительный орган юридического лица или руководитель коллегиального исполнительного органа, а также иное лицо, осуществляющее в соответствии с федеральным законом деятельность от имени юридического лица без доверенности» [6].

Исходя из данных определений, можно сделать вывод о том, что законодатель закрепляет два основных критерия, характеризующих правовое положение руководителя организации.

По мнению авторов комментарий к ТК РФ под общ. ред. Ю.П. Орловского, «Во-первых, он определяет, что руководитель организации является работником, состоящим в трудовых отношениях, выполняющим в соответствии с заключенным с ним трудовым договором особую трудовую функцию. Во-вторых, законодатель характеризует и трудовую функцию руководителя организации, то есть она включает в себя реализацию компетенции юридического лица в гражданском обороте. Так, при исполнении своих трудовых обязанностей руководитель организации осуществляет деятельность, которая регулируется нормами не только трудового, но и гражданского права» [7. С. 915].

Данной точки зрения придерживаются, например, Ю. П. Орловский, О. Б. Зайцева [8. С. 15] и некоторые другие авторы. С. Ю. Головина добавляет, что руководитель организации «с одной стороны, … совместно с другими органами юридического лица реализует его правосубъектность в сфере гражданских правоотношений… С другой стороны, руководитель вместе с другими должностными лицами организации выступает в качестве представителя работодателя в трудовых правоотношениях с работниками, а также иных непосредственно связанных с трудовыми отношениями. … Наконец, сам руководитель состоит в трудовом правоотношении и в этом случае рассматривается как специальный субъект трудового права» [9. С. 93–94].

Рассмотрим подробнее применение искусственного интеллекта руководителем организации.

Процесс управления организацией – это сложный и многогранный процесс, требующий от директора компании много ресурсов. С помощью применения искусственного интеллекта президент фирмы может значительно увеличить производительность труда, сократить затраты на выплату заработной платы, улучшить качество производительности труда.

С помощью искусственного интеллекта руководитель организации может вести поиск и отбор работников на ту или иную вакансию, производить оценку эффективности труда конкретных работников в организации, производить оценку труда руководителей структурных подразделений их подчинёнными, выявлять конфликтных сотрудников, проверять знания работников, предотвращать выгорания сотрудников на работе, повышать мотивацию работников, помогать адаптироваться в другой организации новым сотрудникам.

Благодаря искусственному интеллекту вышеуказанные программы проверки работников исключают полностью человеческий фактор, что способствует всестороннему и абстрагированному анализу эффективности производительности труда работников.

Руководитель организации один из самых заинтересованных людей в получении большей прибыли от фирмы, поэтому, если программы и (или) роботы будут работать эффективнее работников и стоить дешевле, то предпочтение будет отдаваться искусственному интеллекту. Но здесь и другая проблема, в некоторых

отраслях существует недостаток работников из-за невостребованности определенных профессий, в связи с этим бизнесу приходится внедрять в эти сферы искусственный интеллект [12].

В перечисленных внедрениях искусственного интеллекта есть как положительные стороны, так и отрицательные.

Положительные стороны внедрения искусственного интеллекта в деятельность руководителя организации:

– отсутствует человеческий фактор при оценке деловых и личностных качеств работников;

– принимаются более рациональные решения, основанные на математических вычислениях;

– данные программы доступны;

– данные программы быстро подстраиваются под изменения, происходящие в организации;

– быстрый подбор материала;

– автоматическое заполнение документации.

Отрицательные стороны внедрения искусственного интеллекта в деятельность руководитель организации:

– риск безработицы из-за вытеснения искусственным интеллектом многих профессий;

– высокая стоимость программ;

– снижение и перенос ответственности за свои ошибки на работу искусственного интеллекта руководителем организации.

В своей статье «американский экономист Дарон Асемоглу в числе основных рисков выделяет: чрезмерную автоматизацию труда; рост социального неравенства; снижение заработной платы; неспособность повысить производительность труда» [10].

Так, «в 2019 г. компания Amazon была вынуждена отказаться от своего автоматического инструмента для найма работников после того, как алгоритм машинного обучения начал систематически отклонять кандидатов-женщин на инженерные должности. Алгоритм, используя технологию машинного обучения, научился отдавать предпочтение кандидатам-мужчинам, а не женщинам. Программа нашла выражения, используемые мужчинами в резюме (а именно слова «исполнять» и «заканчивать»), более убедительными. ИИ решил, что самопрезентация мужчинами своих трудовых достижений была более эффективной. Кроме того, система обучалась на резюме, представленных претендентами, получившими работу за десятилетний период, большая часть из которых поступила от мужчин. Отсюда можно определить очевидную проблему при найме работников с использованием алгоритмов ИИ: риск прямой и косвенной дискриминации» [11].

Заключение. Подводя итог вышеизложенному, следует сделать вывод, что искусственный интеллект в деятельности руководителя организации в настоящий момент будет эффективен на крупных предприятиях. Полностью и во всех сферах трудовой деятельности искусственный интеллект не заменит работника. Разные программы, используемые президентом компании, облегчают его труд

и труд его подчинённых, сводят к минимуму человеческий фактор. Но наряду с этим нужно понимать, что искусственные интеллект не совершенен, его внедрение достаточно сложный и многогранный процесс, который требует внимательности и контроля за ним.

При внедрении искусственного интеллекта важно не допустить дискриминации прав работников, определить сферы взаимодействия работника и робота.

В настоящее время не решен вопрос о том, как регулировать ответственность за невыполнение или выполнение работы не точно, с дефектами между работником, работодателем, руководителем организации и искусственным интеллектом.

В трудовом праве основополагающим признаком отношений между работником и работодателем является личный характер прав и обязанностей. Если искусственный интеллект наделить правами работника и закрепить регулирование труда робота в ТК РФ, то это будет противоречить сложившийся практики, которая обусловлена личным характером труда.

Список литературы

1. Головина С. Ю. Понятийный аппарат трудового права: монография. Екатеринбург, 1997. – 178 с.

2. Постановление Правительства РФ от 18 апреля 2016 г. № 317 «О реализации Национальной технологической инициативы» // Собрание законодательства РФ. – 2016. – № 17, ст. 2413.

3. Указ Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // Собрание законодательства РФ. – 2018. – № 20, ст. 2817.

4. Распоряжение Правительства РФ от 24 ноября 2023 г. № 3339-р «Об утверждении Стратегии развития отрасли связи РФ на период до 2035 г.» [Электронный ресурс] // СПС «ГАРАНТ». – URL: https://www.garant.ru/products/ipo/prime/doc/408020989 (дата обращения: 04.09.2024).

5. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ // Собрание законодательства РФ. – 2002. – № 1 (часть I), ст. 3.

6. Федеральный закон Российской Федерации «О несостоятельности (банкротстве)» от 26 октября 2002 г. № 127. // Собрание законодательства РФ. – 2002. – №43, ст. 4190.

7. Комментарий к Трудовому кодексу Российской Федерации. 5-е изд., испр., доп. и перераб. / под ред. Орловского Ю. П. – М.: ИНФРА-М, 2012. 1499 с.

8. Зайцева О. Б. Дифференциация правового регулирования труда руководителя в связи с принятием нового Трудового кодекса РФ // Трудовое право. – 2003. – № 3. – С. 15–19.

9. Правовое регулирование труда отдельных категорий работников: учеб.-практ. пособие / под ред. Головиной С. Ю. – М.: Дело, 2003. – 254 с.

10. Арзуманян А. Б. Влияние технологий искусственного интеллекта на права человека в сфере труда [Электронный ресурс] // Северо-Кавказский юридический вестник. – 2023. – № 4. – URL: http://vestnik.uriu.ranepa.ru/wp-content/uploads/2023/12/129-134.pdf (дата обращения: 04.09.2024).

11. Новиков Д. А. Трудовое право и искусственный интеллект: точки соприкосновения и расхождения // Ежегодник трудового права [Электронный ресурс]. – 2024. – Вып. 14. – URL: https://pureportal.spbu.ru/files/119700583/2024_.pdf (дата обращения: 04.09.2024).

12. Рицу С., Мелипатаки Г., Мате Д. А. Концепция труда: от традиционных социально-трудовых представлений к современным эффектам цифровой трансформации // Journal of Digital Technologies and Law. –2023. – Т. 1, № 1. – С. 175–190. https://doi.org/10.21202/jdtl.2023.7. EDN: ZENNZF

С. В. Шуралева,
кандидат юридических наук, доцент,
Пермский государственный национальный
исследовательский университет

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ ТРЕХМЕРНОГО АВАТАРА РАБОТНИКА: ПОСТАНОВКА ПРОБЛЕМЫ

Аннотация. С развитием технологий искусственного интеллекта и метавселенных становится реальной возможность создания и использования трехмерных аватаров работников для участия в совещаниях, выступления в корпоративных средствах массовой информации, общения с клиентами и иных целей. В порядке постановки проблемы исследуются возможные последствия и риски данных инновационных технологий с точки зрения трудового законодательства и законодательства о персональных данных.

Ключевые слова: трудовое правоотношение, трехмерный аватар работника, права работника, персональные данные, биометрические персональные данные, метавселенные, виртуальная реальность, дополненная реальность, цифровые технологии

EMPLOYEE'S DIGITAL AVATAR: NOT YET COMMONPLACE, BUT NO LONGER SCIENCE FICTION

Abstract. With the development of artificial intelligence and metaverse technologies, it becomes possible to create and use digital avatars of employees to participate in meetings, speak in corporate media, communicate with customers and other purposes. In order to pose the problem, the possible consequences and risks of these innovative technologies are investigated from the point of view of labor legislation and legislation on personal data.

Keywords: employment relations, avatar of an employee, personal data, metaverses, digital technologies

Введение. Влияние цифровизации на сферу занятости и развитие индивидуальных и коллективных трудовых отношений активно изучается в современной отечественной науке трудового права. В фокусе исследования – электронный документооборот, дистанционная (удаленная) работа, распространение прекарных нетипичных форм занятости; трудоправовой статус цифровых трудовых платформ

и платформенных трудящихся, проблемы защиты коллективных трудовых прав в условиях цифровизации, трудоправовые аспекты использования искусственного интеллекта, а с недавних пор и метавселенные [1– 5].

Дальнейшее развитие метавселенных, все всякого сомнения, отразится и на сфере труда и занятости. Одним из таких направлений, которое развивается уже сейчас, являются технологии, позволяющие создавать аватаров или цифровых двойников. Однако правовые последствия и риски применения этого еще предстоит оценить.

Основная часть. Дать единое и всеохватывающее определение метавселенной вряд ли возможно, ведь они находятся в процессе формирования, а с позиций сегодняшнего дня сложно предсказать с высокой точностью те перспективы, эффекты и структуры, которые будут метавселенными созданы. Поэтому вполне оправданы подходы, в соответствии с которым метавселенная рассматривается и определяется в зависимости от контекста – технологического, экономического, социально-культурного и т. д. [2. С. 36–37]. Так, описывая метавселенную как технологическую систему, С. В. Орехова и А. Е. Плахин в качестве одного из ключевых ее компонентов позиционируют аватары – цифровые двойники пользователей [2. С. 36].

Представляет интерес высказывания М. Болла, который рассматривает метавселенную как «квази-преемницу» мобильного интернета. Мобильный интернет не изменил способы получения доступа к Интернету, но побудил большинство пользователей приобрести персональный компьютер и доступ в Интернет. Метавселенная идет дальше и помещает всех внутрь виртуальной версии Интернета, внутрь миллиардов взаимосвязанных компьютеров рядом с другими пользователями в режиме реального времени. Люди будут находиться внутри на постоянной основе, а не иметь доступ время от времени. М. Болл утверждает, что неверно ассоциировать с метавселенными виртуальную реальность (это лишь способ ее ощутить) или видеоигру, которая всегда имеет цель, изолирована и конечна [6].

Несмотря на скептическое отношение к определениям метавселенной, М. Болл приводит свое, как он выразился, наиболее удачное определение: «Метавселенная – это масштабируемая (massively scaled) и функционально совместимая (interoperable) сеть трехмерных виртуальных миров и сред с визуализацией в реальном времени (real-time rendered 3D virtual worlds and environments), которые могут восприниматься (experienced) синхронно и постоянно неограниченным числом пользователей с индивидуальным ощущением присутствия (individual sense of presence) и непрерывностью данных, таких как личность, история, права, объекты, коммуникации и платежи» [6].

Отдельные технологии и явления, которые сейчас так или иначе связывают с метавселенными, уже стали частью повседневной жизни: массовые многопользовательские онлайн-игры, цифровые концерты и интервью (в том числе, в виртуальных мирах), видеозвонки с людьми со всего мира, цифровые платформы для общения, развлечения, приобретения товаров и услуг, технологии виртуальной и дополненной реальности, технологии, позволяющие создать реалистичный аватар.

Активное внедрение дистанционной (удаленной) работы в период пандемии COVID-19 выявило ряд проблем взаимодействия работников между собой, с работодателем и клиентами. Это было связано в том числе со сложностями при организации командной работы, участии в совещаниях. Обычный видеоформат не давал эффекта присутствия, люди ощущали разобщенность.

Примечательно, что еще конце 2021 года Билл Гейтс предсказывал, что в течение следующих двух – трех лет большинство виртуальных встреч перейдут от двухмерного изображения с камер к метавселенной, трехмерному пространству с цифровыми аватарами [8].

Пока этот прогноз не реализовался, но очевидно, что использование трехмерных аватаров при организации трудового процесса имеет ряд преимуществ. Общение между аватарами во время обучения, рабочих совещаний может проходить более вовлеченно, с эффектом присутствия. Трехмерный максимально реалистичный аватар может использоваться для трансляции сообщений, новостей, иной информации для работников или клиентов. Возможно использование аватара на определенных стадиях подбора персонала. Для генерации образа используются нейросети. Весьма вероятно, что сфера возможного применения трехмерного аватара будет расширяться, что потребует соответствующего правового регулирования.

И. А. Филипова справедливо отмечает, что трудовое законодательство как в России, так и в зарубежных странах не адаптировано к цифровой трансформации [5. С. 22].

Думается, этот ряд проблемных вопросов можно продолжить. С позиции работника особое значение приобретают гарантии реализации права на неприкосновенность частной жизни на рабочем месте. Установка работодателем видеокамер, программ, позволяющих контролировать активность работника на рабочем месте, его местонахождение, скорость выполнения операций и задач обеспечил возможность слежения за работником, а дистанционная работ способствовала распространению работодательского контроля за пределы офиса, в том числе и в частные помещения работников. Использование трехмерного аватара может еще больше усилить этот контроль.

Немаловажным видится вопрос о защите работников от дискриминации и домогательств в отношении аватара, поскольку он является отражением личности самого работника, а также защитой собственных персональных данных. «Цифровой след», оставляемый работником, все больше. Представим себе ситуацию, когда работник решил уволиться, и не желает, чтобы его «цифровой двойник» продолжал использоваться работодателем. Очевидно, что для такой ситуации в законодательстве и(или) в трудовом договоре должны быть зафиксированы соответствующие правила.

Для работодателя существенное значение могут приобрести вопросы ответственности за действия аватара при его взломе злоумышленниками или в ситуации кражи персональных данных, на основе которых сгенерирован аватар, а также защиты прав на созданные 3D-модели.

Заключение. Проблема использования трехмерных аватаров в настоящее время и тем более в связи погружением в метавселенную, помимо морально-эти-

ческих, экономических, технологических и психологических, имеет еще и правовые аспекты. И если массовое вхождение людей в метавселенные видится перспективой достаточно отдаленной, то использование трехмерных аватаров с применением искусственного интеллекта вовсе не является чем-то фантастическим. Решение юридических коллизий, связанных с использованием «цифровых двойников» в трудовом правоотношении, по-видимому, будет иметь межотраслевой характер.

Список литературы

1. Крылов И. В. Трудоправовые аспекты использования искусственного интеллекта: автореф. … дис. канд. юрид. наук. – М., 2024. – 23 с.

2. Орехова С. В., Плахин А. Е. Метавселенные: переход к новой бизнес-модели или образ будущего? // Управленец. – 2023. – Т. 14, № 2. – С. 35–46. DOI: 10.29141/2218-5003-2023-14-2-3.

3. Томашевский К. Л. Цифровизация и ее влияние на рынок труда и трудовые отношения (теоретический и сравнительно-правовой аспекты) // Вестник СПбГУ. Право. – 2020. – Т. 11, вып. 2. – С. 398–413.

4. Трудовое право: национальное и международное измерение: монография / под ред. С. Ю. Головиной, Н. Л. Лютова. Т. 2: Трансформация трудовых отношений и проблемы отдельных институтов трудового права. Нетипичная занятость. – М.: Норма, 2022. – 568 с.

5. Филиппова И. А. Создание метавселенной: последствия для экономики, социума, права // Journal of Digital Technologies and Law. – 2023. – Т 1, № 1. – С. 7–32. DOI: https://doi.org/10.21202/jdtl.2023.1

6. Ball M. Framework for the Metaverse [Electronic resource]. –URL: https://www.matthewball.co/all/forwardtothemetaverseprimer (дата обращения: 07.09.2024).

7. Bhatt S. What if metaverse becomes a part of HR technology [Electronic resource]. – URL: https://hr.economictimes.indiatimes.com/news/hrtech/what-if-metaverse-becomes-a-part-of-hr-technology/89008987 (дата обращения: 07.09.2024).

8. Gates B. Reasons for optimism after a difficult year 2021 was an incredibly hard year for many people, including me, but I’m hopeful that 2022 will be better [Electronic resource]. – URL: https://www.gatesnotes.com/Year-in-Review-2021 (дата обращения: 07.09.2024).

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ЗДРАВООХРАНЕНИИ

А. П. Финкина,
старший преподаватель,
Донецкий государственный университет
А. В. Бакуров,
магистрант,
Донецкий государственный университет

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В МЕДИЦИНЕ

Аннотация. Внедрение инновационных технологий в медицинскую практику неизбежно. При этом установлено отсутствие действующих законодательных норм, регулирующих эти инновационные виды деятельности. В стадии разработки находятся несколько этических кодексов, призванных стать базовыми для развития инновационного института правового регулирования цифровых технологий в здравоохранении. Процесс их разработки ещё не завершен, его необходимо осуществлять с привлечением экспертов из медицинского сообщества.

Ключевые слова: здравоохранение, медицина, цифровые технологии, правовое регулирование, искусственный интеллект, биопринтер, биопринтные органы

THE LEGAL REGULATION PROBLEMS OF THE DIGITAL TECHNOLOGIES USING IN THE MEDICINE

Abstract. The aim of the work was to study the peculiarities of civil law regulation of the application of digital technologies in medicine, because the introduction of innovative technologies into medical practice is inevitable. It was determined that the legislative norms regulating these innovative activities were absence. Several codes of ethics are being developed to serve as a basis for the development of a system of legal regulation of digital technologies in healthcare. The process of their development has not yet been finalized and should be carried out with the involvement of experts from the medical community.

Keywords: healthcare, medicine, artificial intelligence, legal regulation, digital technologies, 3D bioprinter, bioprinted organs

Введение. Наш век можно назвать веком цифровизации. Это позволяет создавать новые технологии и привносить их в различные сферы деятельности гражданского общества. Неизбежно внедрение цифровых инноваций и в систему здравоохранения. Так, ряд технических решений позволит сформировать целостное цифровое пространство системы здравоохранения, переведя его на новый уровень работы. При этом, учитывая особенности научно-технического прогресса, неизбежно внедрение в здравоохранение искусственного интеллекта (ИИ), цифровых технологий 3D-биопринтера, так называемых биопринтных тканевых (органных)

конструктов и биочернил [5]. Это качественно новые возможности, которые могут осуществить и, вероятно, осуществят «цифровую революцию» в медицине.

Основная часть. При этом до сих пор не выработано единое мнение относительно того, является ли биоматериал человека объектом вещного права, не нормирован правовой режим и его вовлеченность в гражданско-правовые общественные отношения [7. С. 81–95].

Отметим, что, определяя понятие «биологический материал» в статье 2 Федерального закона № 180-ФЗ от 23.06.2016 …, законодатель указывает на то, что прежде всего это компонент организма, или продукт его жизнедеятельности [8]. В настоящее время вступил в силу Федеральный закон от 04.08.2023 г. № 466-ФЗ «О внесении изменений в статью 4 Федерального закона "Об обращении лекарственных средств» и Федеральный закон «О биомедицинских клеточных продуктах», нормирующий понятие «биомедицинский клеточный продукт» [9]. Согласно ст. 2 данного ФЗ, «высокотехнологические лекарственные средства, включая генно-терапевтические лекарственные средства, подлежащие регистрации…» не относятся к биомедицинским клеточным продуктам.

Таким образом, перечисленные выше цифровые продукты (биочернила, биопринтные органы и т. д.) пока не имеют правового определения. Исследования этого направления актуальны, чрезвычайно важны, необходимо разрабатывать их законодательную базу.

Однако среди цивилистов нет единого мнения относительно того, является ли биоматериал организма человека объектом права. Имеется несколько противоположных точек зрения. Одними исследователями предлагается отнести его к вещам, ограниченным в обороте, в то время как другими отрицается такая возможность [7. С. 81–95]. Также очевидна особая регулирующая роль этического фактора. Согласно Федеральному закону от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», цифровизация в сфере здравоохранения неизбежна.

Рассмотрим, насколько «прорывным», а значит перспективным и востребованным может стать применение цифровых новаций и ИИ в сфере здравоохранения. В частности, так называемая 3D-печать (Three-Dimensional Printing Technology) позволяет разрабатывать инновационные технологии 3Dбиопринтинга. Можно думать, что это качественно новый уровень в сфере трансплантологии. Ведь на основе ДНК пациента вне его организма создаётся любой орган, а затем «подсаживается» или вживляется реципиенту. Таким образом, проблема гистосовместимости решена полностью, реакций отторжения нет, поскольку иммунная система «распознаёт» новый орган «своим». Причём диапазон возможностей воссоздания органов, тканей практически не ограничен. Так, в настоящее время уже разрабатывается технология 3D-биопринтинга костей и межпозвонковых дисков [11. С. 241–247]. Известно, что благодаря жанру фантастики в гражданский оборот вошли такие термины, как робот, компьютер, лазер. Благодаря технологии биопринтинга появился новый термин – бионический орган (пока не нормированный аналог протеза). Сама технология биопринтинга крайне востребована, следовательно, будет развиваться. Уже сейчас понятно, что её невозможно запретить.

Нельзя не согласиться с мнением А. А. Шутовой об имеющейся необходимости уже сейчас разрабатывать правовое регулирование 3D-биопринтинга [11. С. 241–247].

Отметим, что в настоящее время отечественное законодательство не содержит как легального определения 3D-биопринтинга, так и норм, регулирующих процесс создания бионических органов и их гражданский оборот.

Уточним, что биопринтер как таковой представляет собой роботизированное устройство, а это позволяет разработать его специализированный правовой режим. Такая работа уже ведётся. В частности, И. Р. Бегишевым разработан инициативный проект федерального закона «Об обороте роботов и их составных частей (модулей)» [2. С. 28]. В ст. 3 данного проекта трактуются такие понятия, как роботы, робототехника. В последующих статьях предложена классификация роботов, трактуются классы опасности роботов. Видится актуальным разработка вопросов, связанная с лицензированием деятельности субъектов, осуществляющих деятельность в этой сфере, создание государственного кадастра роботов и их моделей, проработка вопросов по созданию госреестра субъектов, осуществляющих деятельность в сфере оборота роботов, их составных частей.

Данный проект хорошо согласуется с Концепцией развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 г., утвержденной распоряжением Правительства Российской Федерации от 19 августа 2020 г. № 2129-р [10], отдельное внимание уделено такому направлению, как регулирование применения технологий искусственного интеллекта и робототехники в сфере охраны здоровья граждан. В указанном документе декларируется необходимость обязательной госрегистрации робототехники, относящейся к медицинским изделиям. Считаем это полностью оправданным, поскольку согласно европейскому опыту, эта техника относится к системам ИИ с высоким риском использования. Степень риска обусловлена потенциальной возможностью причинения вреда здоровью, либо нарушения деятельностью ИИ базовых прав и свобод человека [6. С. 389-391]. Отметим, что в ЕС внедряется так называемый «риск-ориентированный подход» при применении технологий ИИ, целью которого является снижение выявленных рисков [1. С. 325-331].

Рассмотрим, какие ещё в настоящее время предпринимаются шаги для решения задач правового регулирования новых сфер медицинской деятельности. Так, в настоящее время разработаны проекты нескольких типовых Этических кодексов, призванных стать основой для разработки новых нормативно-правовых актов (НПА), регулирующих применение в медицине описанных выше инновационных технологий. В частности, учёными Казанского университета им. В. Г. Тимирясова разработаны и предложены к рассмотрению три инновационных проекта этических кодексов. Так, один из них призван регламентировать субъектную деятельность в отношении медицинских изделий, создаваемых на основе технологий робототехники [3. С. 15]. Второй – на основе технологий ИИ [4. С. 16], а третий – на основе 3D-биопринтинга [5. С. 23].

Конечно, разработка и внедрение специализированных этических кодексов своевременна и актуальна. Считаем, что они могут послужить базисом, на основании которого может формироваться инновационный институт правового регулирования указанных технологий в здравоохранении.

Действительно, ряд провозглашаемых принципов созвучен с принципами биоэтики и перечисленными выше НПА. Это принцип государственного контроля и лицензирования медицинской деятельности по биопринтингу. Необходимость применения цифровых технологий в медицине с целью оказания медицинской помощи.

В то же время при ознакомлении с проектами кодексов возникают вопросы. Например, чем обусловлена необходимость создания цифровой модели пациента. При этом легального понятия «цифровой модели» не существует. Как за рамки юриспруденции, так и должностных обязанностей медицинских работников выходит вменяемая им новая обязанность пропагандировать целесообразность донорства по сдаче клеточного биоматериала. Тем более что в отечественном законодательстве отсутствуют нормы, регулирующие отношения по созданию банков клеток и их использованию. С одной стороны, провозглашается запрет на принуждение пациента к использованию изделий, произведенных ИИ, за исключением случаев «крайней необходимости». Тогда это всё же не исключает возможность принуждения, что противоречит основам биоэтики.

Авторы видят возможность спонсирования за счёт частных медицинских организаций, осуществляющих свою деятельность на коммерческой основе, научных исследований по развитию описываемых технологий с последующим внедрением их результатов в клинику. Это чревато преследованием, прежде всего, коммерческих целей, что само по себе несёт определенные риски. Думаем, что наши опасения не напрасны, поскольку все три проекта не исключают использования новых цифровых медицинских технологий в интересах бизнеса, хотя с оговоркой, что «медицинские изделия на основе технологий робототехники или технологии искусственного интеллекта не должны использоваться для придания человеку новых способностей, влекущих ограничение конкуренции».

Заключение. Таким образом, внедрение инновационных технологий в медицинскую практику нуждается в законодательном регулировании. В стадии разработки находятся несколько этических кодексов, которые призваны стать основой для развития системы правового регулирования использования цифровых технологий в здравоохранении. Однако при ознакомлении с ними выявлены определенные риски, следовательно, они должны быть доработаны.

Список литературы

1. Алексеев А. О., Алексеева И. Е., Ерахтина О. С. Об оценке риска применения технологий искусственного интеллекта// Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегишева и др. В 6 т. Т. 3. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. – 440 с.

2. Бегишев И. Р. Об обороте роботов, их составных частей (модулей) (инициативный проект федерального закона) // Препринты Казанского инновационного университета им. В. Г. Тимирясова. 2021. – № 1. – С. 28. URL: https://ieml.ru/podrazdeleniya-universiteta/izdatelstvo-poznanie/preprinty-kiu/ 18-03-2021 (дата обращения: 01.12.2023).

3. Инициативный проект этического кодекса субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на

основе технологий робототехники: препринт № 2, 2023 г. // А. А. Шутова, И. Р. Бегишев. Казань: Изд-во «Познание» КИУ. – 2023. – 15 с.

4. Инициативный проект Этического кодекса субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе технологий искусственного интеллекта: препринт № 1, 2023 г. // А. А. Шутова, И. Р. Бегишев. Казань: Изд-во «Познание» КИУ. – 2023. – 16 с.

5. 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, 2023 г. // А. А. Шутова, И. Р. Бегишев. Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – 23 с.

6. Крикунова В. В. Ответственность за деятельность искусственного интеллекта, осуществляемую с нарушением основных прав, свобод человека и гражданина // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегишева и др. В 6 т. Т. 3. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. – 440 с.

7. Крюкова Е. С., Поваров Ю. С. Вопросы включения биоматериала человека в гражданский оборот (Актуальные направления совершенствования законодательства // Власть закона. – 2021. – № 3(47). – С. 81 – 95.

8. О биомедицинских клеточных продуктах: Федеральный закон от 23 июня 2016 г. № 180-ФЗ // Собрание законодательства Российской Федерации. – 27.06.2016 г. – № 26 (часть I), ст. 3849.

9. О внесении изменений в статью 4 Федерального закона «Об обращении лекарственных средств» и Федеральный закон «О биомедицинских клеточных продуктах»: Федеральный закон от 4 августа 2023 г. № 466-ФЗ // Собрание законодательства Российской Федерации. – 07.08.2023. – № 32 (часть I), ст. 6198.

10. Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г.: распоряжение Правительства Российской Федерации от 19.08.2020 № 2129-р // Собрание законодательства Российской Федерации. – 2020. – № 35, ст. 5593. 11. Шутова А. А. Особенности и перспективы правового регулирования 3D-биопринтера // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегишева и др. В 6 т. Т. 3. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. – 440 с.

Д. Ю. Борисенко,
юрисконсульт,
АО «РАНБАКСИ» (SUN PHARMA)
М. А. Бурсов,
юрист,
АО «Фармстандарт»

CRISPR: ПАТЕНТНЫЕ СПОРЫ И ПРОБЛЕМЫ ЛИЦЕНЗИРОВАНИЯ

Аннотация. В ноябре 2018 года ученый из Южного университета науки и технологий в Шэньчжэне объявил о том, что впервые в мире имплантировал в матку зародыш, подвергнутый геномному редактированию. Беременность привела к рождению двух здоровых девочек-близнецов, что стало, безусловно, поворотной страницей генетической науки. Однако достижение данного научного открытия, озадачило людей по всему миру рядом уже известных биоэтических и правовых проблем, которые до сих пор не были разрешены в общественном сознании. В качестве не только возможных юридических фактов, но и вектора генетического прогресса в частности.

Ключевые слова: патент, лицензирование, молекулярные ножницы, редактирование гена, CRISPR

CRISPR: PATENT DISPUTES AND LICENSING ISSUES

Abstract. In 2018, a scientist from the Southern University of Science and Technology in Shenzhen announced that it was the first time in the world that a genome-edited embryo had been implanted into the uterus. The pregnancy resulted in the birth of two healthy twin girls, which was certainly a turning point in genetic science. However, the achievement of these scientific discoveries has puzzled people all over the world along with already known bioethical and legal problems that have not yet been resolved in public order. As an example, we can cite not only legal facts, but also the vector of genetic progress.

Keywords: patent, licensing, molecular scissors, gene editing, CRISPR

Введение. В июне 2019 года в научном журнале Nature была опубликована статья российского ученого генетика Ребрикова Дениса Владимировича, проректора по научной работе РНИМУ им. Пирогова, сотрудничающего с Центром акушерства, гинекологии и перинатологии имени академика В. И. Кулакова, о возможности успешного и эффективного редактирования гена CCR5 в человеческой зиготе (оплодотворенной яйцеклетке) [7]. Вдохновившись успешным результатом китайского коллеги, Хэ Цзянькуем, переступившим через все этические и нормативные запреты ради проведения первого в мире успешного научного эксперимента по редактировнаию генома эмбриона с помощью технологии CRISPR-cas9 («моллекулярные ножницы»), Д.В. Ребриков с группой российских ученых уверенно заявили о том, что данная технология отлично способствует решению вопроса по предотвращению генетических, наследственных заболеваний. В тот момент, когда еще Дженнифер Дудна и Эммануэль Шарпантье не получили Нобелевскую премию по химии за открытие метода редактирования генома CRISPR-cas9 и не проиграли в 2022 году громкий патентный спор, длившийся с 2015 года за

данное изобретение, команде ученого Фэна Чжана из Массачусетского технологического университета [10], российские генетики уже находят ему качественное применение, которое прямо противоречит подпункту 2 пункта 4 статьи 1349 Гражданского кодекса РФ (далее – ГК РФ): не могут быть объектами патентных прав способы модификации генетической целостности клеток зародышевой линии человека [1].

Основная часть. В рамках данной работы важно продемонстрировать несколько возможностей, аргументированных реальным практическим примером, регистрации нового генетического изобретения с целью дальнейшего использования в рамках лекарственного препарата.

В том числе на данный момент Роспатент и Суд по интеллектуальным правам (далее – СИП) своей позицией подтверждают данный законодательный запрет в споре с ученым сообществом, возглавляемым Д. С. Ребриковым, несмотря на приводимую аргументацию экспертов, а также предложение законодательного изменения упомянутой нормы ГК РФ с целью предоставления возможности получить здорового ребенка будущим родителям [5].

В связи с чем в рамках данной научной работы важно продемонстрировать несколько наиболее подходящих стратегий реформирования законодательства Российской Федерации при наличии такого противоречия, которые могли бы способствовать регистрации нового изобретения в Роспатенте и выводу его на рынок.

Так, несмотря на то, что юридические границы не позволяют законно использовать научное открытие Дженнифер Дудны и Эммануэль Шарпантье в полной мере, в нормативном поле существует способ, о котором было упомянуто Д. С. Ребриковым, а именно получение разрешение на однократное применение данного изобретения у консилиума Минздрава РФ, в соответствии с Приказом Министерства здравоохранения РФ от 14 января 2019 г. № 4н, для конкретного пациента и в форме лекарственного препарата.

Более того, российские ученые из Сеченовского университета усовершенствовали новый метод лечения гепатита В при помощи технологии «молекулярных ножниц» (CRISPR/Cas9). Существующие ранее до этого экспериментальные методы лечения гепатита В не могли быть в полной мере эффективными, так как они не учитывали возможность возникновения рецидива в случае, если в организме осталась релаксированная ДНК вируса. Эксперимент показал, что при совместном использовании «молекулярных ножниц» (удаляет из печени основную форму ДНК вируса) и специального ингибитора синтеза ДНК уничтожается более 98% соответствующих молекул ДНК. Данная технология является прорывом отечественной медицины, однако правовая ситуация до сих пор не позволяет активно применять указанную технологию в качестве метода лечения.

Таким образом, наличие оптимальной и универсальной стратегии при регистрации изобретения, связанного с лечением генетических заболеваний, и редактирования генома клетки поможет быстрее выводить такие инновации на отечественный рынок и изменить общественное отношение к таким изобретениям.

Согласно сложившейся практике, подобные изобретения не регистрируются Роспатентом. Так, в заключении Палаты по патентным спорам от 13.09.2023 (приложение к решению Роспатента от 30.10.2023 по заявке № 2021139313/10)

«Об отказе в выдаче патента на изобретение» было указано на невозможность правовой охраны изобретения на основании пункта 4 статьи 1349 Гражданского кодекса Российской Федерации.

Заключение. Таким образом, сложившаяся практика и фактический устаревший подход в законодательстве Российской Федерации создают препятствие для развития отечественных технологий в области здравоохранения.

Список литературы

1. «Гражданский кодекс Российской Федерации (часть четвертая)» от 18.12.2006 № 230-ФЗ (ред. от 30.01.2024).
2. Приказ Минздрава России от 24.11.2021 № 1094н.
3. Эффективность создания делеции CCR5DELTA32 методом CRISPR-CAS9 в эмбрионах человека / Т. А. Кодылева, А. О. Кириллова, Е. А. Тыщик, В. В. Макаров, А. В. Хромов, В. А. Гущин, А. Н. Абубакиров, Д. В. Ребриков. 2018.
4. Заключение Палаты по патентным спорам от 13.09.2023 (Приложение к решению Роспатента от 30.10.2023 по заявке № 2021139313/10).
5. Решение Роспатента от 20.02.2023 по заявке № 2021139313/10.
6. Решение Суда по интеллектуальным правам от 15 июня 2020 г. по делу № СИП-960/2019
7. URL: https://www.nature.com/articles/d41586-019-01770-x
8. URL: https://rg.ru/2024/02/01/tajna-eto-my.html
9. URL: https://hightech.fm/2019/07/15/crisp-ears
10. URL: https://nplus1.ru/news/2020/10/07/nobel-chemistry
11. URL: https://www.forbes.ru/tehnologii/333985-crisprcas9-chto-znachit-dlya-chelovechestva-perehod-ot-chteniya-genoma-k-ego

К. В. Егоров,
кандидат юридических наук, доцент,
Казанский (Приволжский) федеральный университет

ОТДЕЛЬНЫЕ ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ СИСТЕМ С ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ В МЕДИЦИНЕ

Аннотация. Статья посвящена исследованию вопросов правового регулирования использования технологий искусственного интеллекта (далее – ИИ) в медицине, в частности вопросам гражданско-правовой ответственности в рассматриваемой области. Отмечается, что ИИ не обладает признаками правосубъектности и у пациента не возникает с ИИ правоотношений. В случаях использования ИИ генеративного типа в телемедицине пациент должен быть проинформирован, с чем или кем он взаимодействует, и иметь возможность общения с врачом.

Ключевые слова: искусственный интеллект, медицина, правовое регулирование, пациент, врач, гражданско-правовая ответственность, имитация когнитивной функции

SELECTED ISSUES OF LEGAL REGULATION OF THE USE OF SYSTEMS WITH ARTIFICIAL INTELLIGENCE IN MEDICINE

Abstract. The article is dedicated to the investigation of legal regulation concerning the use of artificial intelligence technologies in medicine. Special attention is given to issues of civil liability in the considered domain, imitation of cognitive function. It is noted that AI does not have the attributes of legal personality and no legal relationship arises between a patient and an AI system. In cases where generative AI is used in telemedicine, the patient must be informed about what or whom they are interacting with and have the opportunity to communicate with a doctor.

Keywords: Artificial Intelligence, Medicine, Legal Regulation, Patient, Physician, Civil responsibility, imitation of cognitive function

Введение. Безопасность и эффективность клинических решений, которые принимаются врачом с использованием новейших технологий, в конкретных обстоятельствах имеют значение как непосредственно для пациента, так и для общества и государства в целом. Сегодня на помощь врачам приходят технологии, имитирующие когнитивные процессы человека, в частности автоматическое распознавание изображений на основе глубоко обученных компьютерных «нейронных» сетей. Такие технологии дают возможность увеличить точность суждений в области диагностики, ускорить ее проведение, а в ряде случаев уменьшить стоимость исследований. Тем не менее даже будучи обученными на миллионах примеров «нейронные» сети не лишены недостатков в функции распознавания изображений, допускают ошибки в интерпретациях или выдают данные, которые, не подтверждаются данными обучения нейросети (так называемые «галлюцинации нейросети»).

Основная часть. В 2023 году Росздравнадзор временно остановил применение медицинской системы Botkin.AI – платформы для анализа медицинских снимков – на предмет злокачественных новообразований в связи с угрозой причинения вреда жизни и здоровью граждан [6]. В 2018 году программа Watson for Oncology стала назначать пациентам с онкологическими заболеваниями некорректные лекарства, прием которых мог угрожать здоровью [1]. К ряду вопросов, связанных с использованием систем искусственного интеллекта (далее – СИИ), в здравоохранении относят проблемы прозрачности, объяснимости и интерпретируемости алгоритмов, предвзятости [10], недостаточной для реальной клинической практики точности работы моделей, проблемы конфиденциальности [5, 13].

В таких обстоятельствах крайне важно создать правовые условия принятия решений врачом, которые:

(1) максимально соответствовали бы интересам пациента;

(2) обеспечивали юридическую безопасность врача;

(3) не препятствовали разумному развитию технологий;

(4) были экономически рациональными.

Какие здесь можно предложить деонтологически обоснованные и одновременно прагматически обусловленные подходы к правовому регулированию принятия лечебных решений с использованием СИИ? Будучи ограниченными объемом настоящей публикации, мы остановимся всего на двух аспектах:

(1) вопрос взаимодействия пациента, врача и СИИ;

(2) вопрос гражданско-правовой ответственности в отношениях, в которых используется СИИ в сфере медицины.

В настоящий момент уровень СИИ генеративного типа, имитирующий диалог, не позволяет обычным способом отличить человека от программы. Человеку важно знать, кто или что с ним взаимодействует для того, чтобы принимать осознанное решение о содержании или, в принципе, возможности продолжения взаимодействия, в этой связи мы полагаем, что:

1. В ситуациях непосредственного взаимодействия пациента с приложениями (программами ЭВМ), как, например, в мобильных приложениях при оценке фотоизображений новообразований [7] или в сети «Интернет», пользователю-пациенту должно быть очевидно, с кем он взаимодействует (СИИ, врач-эксперт, медицинская организация, информационный посредник, агрегатор), кто оказывает услугу (разработчик, правообладатель ПО, агрегатор, медицинская организация или врач-эксперт), что это за услуга (неисключительное использование ПО, информационная услуга, медицинская услуга, посредничество) и кто будет отвечать за ее недостатки. Нормативные требования о правосубъектности к таким лицам должны быть адресными и устанавливать соответствующие требования об информировании пользователя и его гарантиях качества услуги;

2. Пользователю-пациенту должно быть очевидно, с чем или кем он взаимодействует в каждый момент времени с человеком или программой ЭВМ (ИИ, робот и т. д.). Это требование, на наш взгляд, касается не только медицинских систем СИИ, но и всех сценариев взаимодействия человека с информационными системами. Рекомендации об этических аспектах искусственного интеллекта ЮНЕСКО 2021 г. [8] содержат аналогичный подход: «Государствам-членам следует обеспечивать пользователям возможность быстро понять, взаимодействуют ли они с живым существом или с ИИ-системой, имитирующей качества человека или животного, а также возможность пользователей отказаться от взаимодействия с ИИ-системой и попросить о вмешательстве человека» (п. 127).

Согласно статье 20 Федерального закона от 21.11.2011 № 323-ФЗ (ред. от 13.06.2023) «Об основах охраны здоровья граждан в Российской Федерации» (далее – ФЗ № 323-ФЗ) [9] необходимым предварительным условием медицинского вмешательства является добровольное информированное согласие (ДИС) гражданина или его законного представителя на медицинское вмешательство на основании предоставленной медицинским работником в доступной форме полной информации о целях, **методах оказания медицинской помощи,** связанном с ними риске, **возможных вариантах медицинского вмешательства,** о его последствиях, а также **о предполагаемых результатах оказания медицинской помощи.** Таким образом, пациент непосредственно вовлечен в процесс принятия решения о вмешательстве в его здоровье.

Заметим, что **закон формально не связывает врача при выборе возможных вариантов медицинского вмешательства** ни объемами помощи в рамках программ государственных гарантий, ни технологическими возможностями конкретной медицинской организации, ни современными возможностями медицины. Тем не менее, **границы возможных вариантов медицинского вмешательства**

конкретным врачом, очевидно, обусловлены техническими и экономическими возможностями медицинской организации.

Здесь мы сталкиваемся с довольно сложным этическим и экономическим вопросом “При формальном соответствии медицинской организации и действий врача требованиям закона, следует ли врачу врачу при разъяснении пациенту возможных вариантов медицинского вмешательства ограничиться таким вариантом, который лежит в пределах и формально соответствует клинической рекомендации, техническим и экономическим возможностям медицинской организации?» Вопрос, безусловно, вызывает к жизни массу глубоких пластов и экономического, и юридического, и деонтологического плана. В связи с этим мы полагаем важным высказаться о принципиальных, на наш взгляд, позициях в регулировании рассматриваемых отношений:

1. В объем разъяснения (ИДС) должны входить технологические возможности исполнителя, не только в части возможности использования СИИ, но и вообще об уровне технической оснащенности медицинской организации.

2. В объем разъяснений пациенту должны входить сведения не только об объеме медицинской помощи в рамках финансирования по ОМС, но и иных современных возможностях медицины, которые могут быть оплачены из других источников.

Что касается вопроса, должно ли в объем ИДС входить согласие на использование СИИ для целей установления диагноза и назначения лечения, то нам представляется, что этот вопрос не актуален, пока в процесс принятия клинического решения вовлечен врач-человек.

СИИ не является субъектом принятия решения. Пункт 3.18 ГОСТ Р 59277-2020 «Системы искусственного интеллекта. Классификация систем искусственного интеллекта» содержит определение ПО с системами искусственного интеллекта. По определению в этом стандарте, искусственный интеллект представляет собой комплекс технологических решений, имитирующий когнитивные функции человека и способный решать задачи обработки данных, сопоставимо с результатами умственной деятельности человека. Система искусственного интеллекта (artificial intelligence system) – это программное обеспечение, в котором используются технологические решения искусственного интеллекта. Последний представляет собой комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение, поиск решений без заранее заданного алгоритма и достижение инсайта) и получать при выполнении конкретных практически значимых задач обработки данных результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных, анализу и синтезу решений [пункт 3.18 ГОСТ Р 59277-2020].

СИИ, определенно, не принимает никаких решений, не является субъектом правоотношений и представляет собой в гражданско-правовом смысле, с одной стороны, вещь, с другой – программу для ЭВМ применительно к медицине, как это будет показано ниже, являющиеся источником повышенной опасности. При отсутствии воли и интереса невозможно говорить о какой-либо субъектности ИИ

[4]. Имитация когнитивной функции человека по распознаванию изображений ничего в правовой сущности СИИ не меняет.

Гражданско-правовая ответственность. Как указано выше, мы исключаем рассуждения в отношении правосубъектности ИИ, как следствие, отказываем ИИ в деликтоспособности (способности нести юридическую ответственность), в том числе по моделям квазисубъектов, рассматриваемые некоторым количеством последователей трансгуманизма [15]. При таком подходе вопрос юридической ответственности при использовании СИИ в медицинской практике представляется авторам достаточно определенным. Рассмотрим этот вопрос в контексте ответственности за ущерб, причиненный в результате функционирования СИИ.

Основаниями для наступления гражданско-правовой ответственности традиционно считают наличие вреда, противоправность действий причинителя вреда и вина последнего либо нарушение субъективного гражданского права, медицинская сфера не является исключением. В предыдущих работах нами рассматривался этот вопрос [3], поэтому считаем возможным не останавливаться на нем подробно. Когда речь идет о причинении вреда здоровью в процессе оказания медицинской помощи, как правило, пациента следует считать потребителем, подробное обоснование такого подхода неоднократно приводилось в специальной литературе [3]. Как следствие, ответственность за такой вред жизни или здоровью наступает независимо от их вины и от того, состоял пациент с исполнителем в договорных отношениях или нет (статья 1905 ГК РФ).

Приказ Минздрава России от 06.06.2012 № 4н утверждает классификацию программного обеспечения, которое является медицинским изделием, по классам в зависимости от потенциального риска их применения. Все российское ПО, созданное с применением технологий ИИ, относится к классу 3 потенциального риска – медицинские изделия с высокой степенью риска. Как следствие, мы не разделяем точку зрения отдельных авторов [14] о том, что статус медицинских СИИ в качестве источника повышенной опасности не определен. СИИ могут быть источником повышенной опасности с точки зрения статей 1100 и 1079 ГК РФ. Но поскольку практическим правовым последствием такой квалификации будет ответственность без вины (так же как и в силу статьи 1905 ГК РФ), особой практической значимости в рассмотрении данного вопроса мы не видим.

Главными, с нашей точки зрения, вопросами гражданско-правовой ответственности в рассматриваемых правоотношениях будет вопрос субъекта ответственности и противоправности его поведения. При этом мы не рассматриваем вред, причиненный правомерными действиями врача при наличии ДИС пациента, так как этому посвящены наши предыдущие исследования [3]. Очевидно, что вред может быть причинен как недостатками аппаратной и программной части СИИ или врачом. В тех случаях, когда пациент использует СИИ без участия врача, как в приведенных выше примерах, формально-юридически он пациентом не является. В тех случаях, когда такое взаимодействие пользователя с СИИ стало причиной причинения вреда здоровью важным будет ответить на вопрос есть ли противоправность в действиях или бездействиях разработчика, правообладателя, агрегатора, информационного посредника или пользователя.

Что же касается медицинского применения СИИ при оказании медицинской помощи, то в этом случае по обязательствам из причинения вреда будет отвечать Исполнитель медицинской услуги (статьи 402, 1095 ГК РФ), которым, как правило, является медицинская организация. У последней в силу регресса (статья 1081 ГК РФ) может возникнуть право требования к врачу, допустившему правонарушение. Даже в тех случаях, когда вред пациенту причинен неисправностями аппаратной части СИИ, ошибками программной части и(или) лицами, проводившими обучение нейросети, переложить на них ответственность перед пациентом у медицинской организации нет возможности, разве что впоследствии использовать право регресса к неисправным разработчикам, посредникам, агрегаторам, лицензиатам и т. д.

Что же может считаться противоправным со стороны врача, который использует СИИ при принятии решения о постановке диагноза и(или) выборе тактики последующего решения (например, выбирая между хирургией, химиотерапией или радиотерапией)? Как было указано выше, на сегодняшний день в порядках, положениях, стандартах и клинических рекомендациях (статья 37 ФЗ №323-ФЗ) не содержатся указания о порядке применения СИИ. Но это не означает, что объективного права на этот счет не существует. Во-первых, СИИ в качестве медицинских изделий и программных продуктов медицинского назначения имеют вполне определенный порядок введения в оборот, настройки и использования – как на уровне государственных стандартов, так и на уровне инструкций по их использованию. Во-вторых, в настоящее время активно складывается практика обычного применения СИИ, которая в силу ст. 5 ГК РФ может стать источником права, относительно которого можно судить о правомерности или противоправности действий или бездействия врача. Тем не менее обычное регулирование, разумеется, не может полноценно компенсировать отсутствие нормативного, закрепленного в положениях, порядках и(или) клинических рекомендациях. В связи с этим мы полагаем, что до появления соответствующего регулирования врачу следует исходить из презумпции недоверия выводам СИИ.

Авторы понимают, что недопустимость использования СИИ в медицинской практике без участия врача, а также введение презумпции недоверия СИИ до появления объективных норм права, регулирующих соответствующие отношения, могут повлиять на сдерживание развития СИИ в сфере медицины. Тем не менее на сегодняшний день такие предложения являются объективно обусловленными необходимостью безопасного использования СИИ для пациентов и могут быть пересмотрены в будущем при появлении достаточной эмпирической базы, свидетельствующей об отсутствии ошибок и других недостатков использования СИИ, о которых упоминалось выше.

Заключение. Мы полагаем, что до появления достаточных, обоснованных данных о надежности СИИ и появления нормативной базы применения СИИ в обычной медицинской практике не допускается использование выводов, полученных с использованием СИИ без их интерпретации врачом и(или) консилиумом соответствующей медицинской специальности. При этом для целей избежания когнитивных искажений (предвзятость суждений в силу эффекта прайминга и(или) эффекта привязки) врач должен интерпретировать данные объективного обследо-

вания до ознакомления с выводами СИИ, и в случае расхождений принять решение самостоятельно или прибегнув к созыву консилиума. То же справедливо и для случаев, когда оценка клинической картины изначально производится группой врачей, людям следует сделать самостоятельную интерпретацию клинической картины до ознакомления с данными СИИ.

С кем правоотношение у пациента? Пользователю-пациенту при самостоятельном использовании приложений, связанных со сбором, оценкой и интерпретацией его анамнеза и клинической картины, должно быть очевидно, с каким субъектом (правообладатель программы ЭВМ, лицензиат, агрегатор, информационный посредник, медицинская организация) он взаимодействует, кто оказывает услугу, и кто будет отвечать за ее недостатки. Нормативные требования к такому лицу должны быть адресными и должны быть закреплены как минимум на уровне приказа Минздрава России от 30.11.2017 № 965н.

С кем или чем общается пациент? В случаях удаленного взаимодействия пользователю-пациенту должно быть очевидно в каждый момент времени взаимодействует он с человеком или ПО имитирующей когнитивную и коммуникативную функцию человека, а также возможность потребовать участия человека в коммуникации. Такое требование может быть так же учтено на уровне Приказа Минздрава России.

Пациент должен знать о больших, чем предлагает программа госгарантий, возможностях медицины. С учетом развития технологий и медицинской науки, мы полагаем, что объем информирования пациента в настоящий момент, должен включать как минимум два дополнительных блока информации: (1) В объем информации, предоставляемой пациенту для целей добровольного согласия на оказание медицинской помощи, должны входить технологические возможности исполнителя не только в части возможности использования СИИ, но и вообще в части технической оснащенности конкретной медицинской организации. (2) В объем разъяснений пациенту должны входить сведения не только об объеме финансирования медицинской помощи по ОМС, но и о современных возможностях медицины, которые могут быть оплачены из других источников (личных средств пациента, средств работодатели или в рамках ДМС).

Список литературы

1. Spitzer J. IBM's Watson recommended 'unsafe and incorrect' cancer treatments, STAT report finds. URL: https://www.beckershospitalreview.com/artificial-intelligence/ibm-s-watson-recommended-unsafe-and-in-correct-cancer-treatments-stat-report-finds.html (дата обращения: 12.07.2024).

2. Егоров К. В. Правомерный вред в медицине. М.: Статут, 2011.

3. Егоров К.В. Вред как условие деликтной ответственности в сфере медицинской деятельности // Практическая медицина. 2006. № 2(16). С. 37–38.

4. Зорькин В. Д. Право и вызовы искусственного интеллекта // Российская газета. 2024. № 9382. Полный текст лекции на сайте Российской Газеты https://rg.ru/2024/06/27/pravo-i-vyzovy-iskusstvennogo-intellekta.html (дата обращения: 12.07.2024).

5. Искусственный интеллект в медицине. Как умные технологии меняют подход к лечению / Э. Тополь; пер. с англ. А. Анваер. М.: Альпина Паблишер, 2022. 398 с.

6. Патологически беспомощный интеллект // Коммерсантъ. 2023. № 216, 21 ноября.

7. Приложение «ПроРодинки 2.0». URL: https://prorodinki.ru (дата обращения: 22.08.2024).

8. Рекомендации об этических аспектах искусственного интеллекта ЮНЕСКО 2021 г. URL: https://unesdoc.unesco.org/ark:/48223/pf0000380455_rus (дата обращения: 22.08.2024).

9. Об основах охраны здоровья граждан в Российской Федерации: Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 13.06.2023) // Собрание законодательства РФ. 2011. № 48. Ст. 6724.

10. Тютчева Е. С. Правосубъектность «электронного лица»: теоретический анализ // Теоретическая и прикладная юриспруденция». 2022. № 2(12). С. 50–58.

11. Ужов Ф. В. Искусственный интеллект как субъект права // Пробелы в российском законодательстве. 2017. № 3. С. 357–360.

12. Харитонова Ю.С., Савина В.С., Паньини Ф. Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права // Вестник Пермского университета. Юридические науки. 2021. № 3. С. 488–515.

13. Шутова А. А. Этический кодекс субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе технологий искусственного интеллекта / А. А. Шутова, И. Р. Бегишев // Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции: в 6 томах, Казань, 22 сентября 2023 года. Казань: Изд-во «Познание», 2023. С. 441–447. EDN: EFUNKM

14. Юхнова Ю. И. Искусственный интеллект и роботы в медицине: проблема ответственности за причинение вреда пациентам // Юрист. 2023. № 1. С. 21–26.

15. Ястребов О. А. Правосубъектность электронного лица: теоретико-методологические подходы // Труды Института государства и права РАН. 2018. Т. 13, № 2. С. 36–55.

О. С. Ерахтина,
кандидат юридических наук, доцент,
Национальный исследовательский университет
«Высшая школа экономики»

К ВОПРОСУ О РАСПРЕДЕЛЕНИИ ОТВЕТСТВЕННОСТИ ЗА ВРЕД ЗДОРОВЬЮ ПАЦИЕНТА, НАСТУПИВШИЙ В РЕЗУЛЬТАТЕ ПРИМЕНЕНИЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ ВРАЧЕБНЫХ РЕШЕНИЙ

Аннотация. В статье исследуется проблема распределения гражданско-правовой ответственности за вред здоровью пациента, наступивший в результате применения систем диагностики и поддержки принятия врачебных решений при оказании медицинской помощи. Автор приходит к выводу о том, что применение

при оказании медицинской помощи технологий искусственного интеллекта, в частности СППВР, приводит к необходимости расширения круга субъектов гражданско-правовой ответственности, включив в него разработчика технологии, оператора, а в случае применения обучаемых систем – учителя. Вопрос распределения ответственности между субъектами правоотношений рассматриваемых правоотношений становится еще более сложным в случае применения высокотехнологичных систем, действующих на основе глубокого машинного обучения. В определенной степени решению этого вопроса будет способствовать дифференциация субъектов рассматриваемых отношений и распределение между ними обязанностей по минимизации риска причинения вреда пациенту.

Ключевые слова: вред здоровью, система поддержки принятия врачебных решений, врач-оператор, субъекты гражданско-правовой ответственности

LIABILITY FOR DAMAGE TO THE PATIENT'S HEALTH RESULTING FROM THE USE OF MEDICAL DECISION SUPPORT SYSTEMS

Abstract. The article examines the problem of distribution of civil liability for harm to a patient's health resulting from the use of diagnostic systems and support for medical decision-making in the provision of medical care. The authors come to the conclusion that the use of AI technologies, in particular SPPV, in the provision of medical care leads to the need to expand the range of subjects of civil liability to include the company of the technology developer, operator, and in cases of using learning systems – teachers.The issue of distribution of responsibility between the subjects of legal relations of the legal relations under consideration becomes even more complex in the case of the use of high-tech systems operating on the basis of deep machine learning. To a certain extent, the solution to this issue will be facilitated by the differentiation of the subjects of the relationship under consideration and the distribution of responsibilities among them to minimize the risk of harm to the patient.

Keywords: harm to health, medical decision support system, doctor-operator, subjects of civil liability

Введение. Как указано в Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники [1], одним из ключевых барьеров действующего регулирования, препятствующим широкому использованию высоких технологий в медицине и требующим решения, является проблема распределения ответственности за вред здоровью пациента, наступивший в результате применения таких технологий при оказании медицинской помощи.

В последнее время активно разрабатываются и внедряются в медицинскую деятельность системы диагностики и поддержки принятия врачебных решений, которые позволяют использовать массивы аналитической информации, недоступные или ограниченно доступные медицинским работникам при обычном взаимодействии с пациентом [1].

Основная часть. Под термином «система поддержки принятия решений» (Decision Support System, DSS) понимается компьютерная система, которая путем сбора и анализа информации может влиять на процессы принятия решений в различных областях человеческой деятельности [2, 7]. В здравоохранении такие ре-

шения называются уточненным термином «системы поддержки принятия врачебных решений» (далее – СППВР). Чаще всего СППВР используются именно для помощи при постановке диагноза, назначении и при необходимости корректировке назначенного лечения [3].

При применении СППВР при оказании медицинской помощи высок риск того, что система может выдать ошибочный диагноз. При этом ошибка может остаться незамеченной лечащим врачом, вследствие чего будет причинен вред жизни и здоровью пациента.

Обычно в случае необходимости возмещения вреда пациенту, причиненного вследствие врачебной ошибки, гражданско-правовую ответственность несут медицинские организации. Существует ли необходимость расширения круга субъектов гражданско-правовой ответственности, если вред пациенту был причинен вследствие ошибочной рекомендации СППВР? Следует ли в определенных случаях привлекать к ответственности за причиненный вред разработчика такой системы или специалиста по машинному обучению? Всегда ли врач-оператор (врач, использующий систему) может и должен контролировать корректность выходных данных СППВР? Будет ли отличаться ответ на последний вопрос в зависимости от того, кто применяет СППВР в своей деятельности – узкий специалист или врач общей практики? Этими и многими другими вопросами задаются специалисты, изучающие влияние технологии искусственного интеллекта в процессе оказания медицинской помощи населению, если в результате будет причинен вред здоровью или жизни [4].

Процесс, с помощью которого система генерирует выходные данные с рекомендациями по лечению, является достаточно сложным и представляет собой так называемую проблему «черного ящика». Как верно отмечается в литературе, врачи, выступающие в качестве операторов, оказываются в ловушке «зоны моральной неуверенности» [6], на них в полном объеме возлагается ответственность за вред, причиненный здоровью и жизни пациента, хотя врачи в данном случае имеют лишь ограниченное влияние на работу системы поддержки принятия врачебных решений в силу отсутствия у них специальных знаний об особенностях функционирования данной системы.

Вопрос определения субъекта ответственности за вред здоровью пациента, наступивший в результате применения СППВР, заслуживает особого внимания в связи с повышением уровня автономности таких систем и их способности к дальнейшему обучению. Автономные системы принимают решения на основе анализа больших объемов информации, которая обрабатывается при помощи машинного обучения.

Заслуживающим внимания является подход нидерландских ученых, которыми исследовался вопрос о субъектах ответственности за вред, причиненный при применении высокотехнологичных систем для терапии аутизма. Особое внимание в исследовании обращается на такого субъекта рассматриваемых отношений, как учитель – специалист по машинному обучению. При этом специалист по машинному обучению может быть как сотрудником организации-разработчика, так и сотрудником организации – пользователя системы, а также может быть сотрудником сторонней организации. Задача такого специалиста состоит в том, чтобы оценить качество разработки.

Предлагаемый нидерландскими учеными подход основан на принципе: «чем выше способность к обучению или уровень автономности системы, тем ниже должна быть ответственность других сторон, и чем дольше длится “образование” системы, тем выше должна быть ответственность его учителя» [5]. Для таких лиц ученые из Нидерландов предлагают внедрить систему сертификации, в соответствии с которой им необходимо будет пройти специальную подготовку, чтобы получить дополнительные навыки для разработки сложных систем.

Вопрос распределения ответственности между субъектами рассматриваемых правоотношений становится еще более сложным в случае применения высокотехнологичных систем, действующих на основе глубокого (неконтролируемого) машинного обучения.

Важно также учитывать тот факт, что машинное обучение представляет собой сложную систему, включающую в себя подсистемы и элементы. Зачастую невозможно отследить вклад отдельных элементов в общий результат причинения вреда пациенту, могут возникать системные ошибки, «наслаивающиеся» друг на друга. Возникает вопрос первопричины: из-за сбоя А пострадала система Б (которая зависела от А), что привело к ложному выводу В. Не всегда можно отследить данную линейность.

Заключение. Как видим, вопрос распределения ответственности за вред здоровью пациента, наступивший в результате применения систем поддержки принятия врачебных решений, является сложным и требует учета многих факторов. В определенной степени решению этого вопроса будет способствовать дифференциация субъектов рассматриваемых отношений и распределение между ними обязанностей по минимизации риска причинения вреда пациенту.

Список литературы

1. Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники: Распоряжение Правительства РФ 19.08.2020. № 2129-р. // СПС «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_ LAW_196819 (дата обращения: 05.09.2024).

2. Литвин А. А., Литвин В. А. Системы поддержки принятия решений в хирургии // Новости хирургии. 2014. Т. 22, № 1. С. 96–100.

3. Фролов С. В., Куликов А. Ю., Остапенко О. А., Стрыгина Е. В. Системы поддержки врачебных решений в медицине // Научный журнал. 2018. № 9(32). С. 9–17.

4. Шутова А. А. Применение технологий искусственного интеллекта в сфере здравоохранения: уголовно-правовые девиации // Правопорядок: история, теория, практика. 2023. № 3(38). С. 92–100. EDN: RKMSGE. DOI: 10.47475/2311-696X-2023-38-3-92-100

5. Bratu Ioana and van der Linden Tina. Assigning Liability for Damages to Artificial Intelligent Systems Used for Autism Therapy. A European Approach (February 1, 2020).

6. Elish M. C. Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction // Engaging Science, Technology and Society. 2019. Vol. 5. Pp. 40–60.

7. Greenes R. A. Clinical decision support: the road ahead. Boston: Elsevier Academic Press, 2007. 581 p.

А. Р. Поздеев,
доктор медицинских наук, доцент,
Ижевская государственная медицинская академия

РОЛЬ ПОДГОТОВКИ КВАЛИФИЦИРОВАННЫХ МЕДИЦИНСКИХ КАДРОВ В ПЕРИОД ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЗДРАВООХРАНЕНИЯ

Аннотация. В статье обобщаются данные о наилучшем здравоохранении в мире по версии сервиса Numbeo в 2024 году в Тайване (86,43 балла), а из европейских государств – на 4-м месте во Франции (80,18) с ранее проводимой там цифровой трансформацией здравоохранения. Важную роль в этом играют высококвалифицированные обученные медицинские кадры с обязательной стажировкой в ведущих медицинских вузах. «Цифровые кафедры» в медицинских вузах нацелены на подготовку таких кадров, однако в Российской Федерации их немного, и половина студентов-медиков не испытывают желания получить дополнительное образование по IT-технологиям.

Ключевые слова: право, цифровые технологии, цифровая трансформация здравоохранения, hard skills, soft skills, медицинское образование, цифровые кафедры

THE ROLE OF TRAINING OF QUALIFIED MEDICAL PERSONNEL IN THE PERIOD OF DIGITAL TRANSFORMATION OF HEALTHCARE

Abstract. The article summarizes the data on the best health care in the world according to the version of the Numbeo service in 2024 in Taiwan (86.43 points), and from European states – in 4th place in France (80.18) with the digital transformation of health care previously carried out there. An important role in this is played by highly qualified trained medical personnel with compulsory internship in leading medical universities. "Digital departments" in medical universities are aimed at training such personnel, but in the Russian Federation there are few of them, and half of medical students do not feel the desire to receive additional education in IT technologies.

Keywords: law, digital technologies, digital transformation of healthcare, hard skills, soft skills, medical education, digital departments

Введение. В отношении медицины государства устанавливают контроль и надзор, организуя систему, обеспечивающую охрану здоровья населения. Здравоохранению в наше время присущи снижение доступности медицинских услуг без улучшения их качества [4, 12], дефицит медицинских кадров, достигающий 58 тыс. врачей в год [8. С. 127], неравномерное распределение ресурсов для медицинских организаций [9], низкие ориентиры для финансирования государством здравоохранения, приводящие к действительным помехам при реализации национальных целей [11], «врачебные ошибки» и потребительский экстремизм, уголовное преследование медиков и многомиллионные гражданские иски к больницам [5].

Основная часть. Подобные проблемы здравоохранения присущи не только России, следствием чего является общемировой тренд в трансформации здраво-

охранения, где ведущий вектор отведен цифровой трансформации здравоохранения (ЦТЗ), которая позволит решить большинство обозначенных кризисов. Известно, что государства располагают разными моделями здравоохранения, мониторинг которых позволяет выявлять их эффективность. Сервис Numbeo в 2024 году выявил наилучшее здравоохранение в Тайване (86,43 балла), а из европейских государств – на 4-м месте во Франции (80,18) [6].

Здравоохранение Тайваня с Национальным управлением медицинского страхования (NHIA) провели ЦТЗ. В Тайване действует система страховых накопительных счетов, которые покрывают до 98 % от стоимости лечения в государственных клиниках, а оплата осуществляется напрямую через Управление здравоохранения. Отличительной особенностью является срочный характер аккредитации работников в медицинской организации (каждые три года). Медицинские организации аккредитуются международной комиссией (JCI), которая оценивает уровень квалификации врачей, технологический и административный сектор, опираясь на цифровой профиль. Врачи дополнительно проходят специальное обучение со стажировкой в ведущих вузах стран Китая, Европы и США [13]. Опыт Тайваня демонстрирует факт, что ЦТЗ обусловлена обучением штата медиков в здравоохранении.

Целью цифровой трансформации здравоохранения в Российской Федерации являются «достижение высокой степени "цифровой зрелости", оптимизация рабочего времени медицинских работников посредством автоматизации процессов управления и внедрения передовых технологий в целях повышения доступности оказания медицинской помощи, обеспечения эффективной и оптимальной маршрутизации пациента, межведомственного взаимодействия, обеспечения высокого качества, необходимой полноты и достоверности информации о состоянии здоровья пациента и увеличения доли раннего выявления заболеваний» [1, 2].

В период ЦТЗ выполняется подготовка кадров новым специальностям и профессиям. Специалисты по анализу «медицинских данных» (Big Data) приходят на помощь медикам, разрабатывают новые методы лечения, на основе выявленных факторов риска для стратегии их предотвращения и др. Инженеры («биомедицинские») совершенствуют технологии и оборудование, создают протезы, искусственные органы, диагностические приспособления и роботов, например, для хирургии. Генетические консультанты помогают разрабатывать персонализированные стратегии лечения на основе генетической информации. Специалисты по кибербезопасности помогают защитить медицинские данные от кибератак, несанкционированного проникновения путем создания мер безопасности, аудита и обучения штата. Телемедицинские координаторы организуют и управляют процедурами телемедицины, работая в сотрудничестве с врачами, инженерами, фармацевтами.

В процессе подготовки высококвалифицированных IT-специалистов для здравоохранения происходит формирование базовых компетенций (hard skills) и мягких компетенций (soft skills). Среди hard skills для новых профессий происходит формирование глубоких технических навыков: программирование, анализ данных, методы шифрования данных и защиты от кибератак, работа с медицинскими устройствами и системами. Soft skills нацелены на формирование комму-

никации (общение как с медицинскими работниками, пациентами, так и техническими специалистами и др.), так и способность работать в команде, адаптироваться к новым условиям и быстро учиться.

Национальная программа «Цифровая экономика Российской Федерации» включает федеральный проект «Развитие кадрового потенциала ИТ-отрасли» [3] и проект «Цифровая кафедра» по программам профессиональной переподготовки. «Цифровые кафедры» – это обеспечение приоритетных отраслей экономики высококвалифицированными кадрами, обладающими вышеозначенными цифровыми компетенциями. Учащихся по специальностям и направлениям подготовки, которые не относятся к IT-сфере, например, будущие медики получают необходимые компетенции и диплом о профессиональной переподготовке. Национальная программа работает в вузах не везде, что обуславливает дефицит высококвалифицированных кадров при ЦТЗ в субъектах РФ. В современном мире образование меняется в соответствии с тенденциями, однако характерен существенный разрыв медицинского образования и компетенций, необходимых для работы в IT-сфере [10]. Проведенный опрос студентов-медиков первого курса об их желании дополнительно обучаться IT-технологиям выявил заинтересованность у половины студентов.

Известно, что ЦТЗ сопряжена с созданием «Цифровых двойников» медицинских работников и пациентов. На протяжении последних десятилетий создание моделей различных процессов является перспективным трендом не только в медицине и IT-сфере. Все дело в том, что, создав модель на основе «цифровых двойников», можно прогнозировать процессы, различные ситуации, высвободить людей, заменив «двойниками». «Цифровой двойник – одна из самых многообещающих технологий нашего времени, позволяющая принимать управленческие решения в логике «из будущего». Характерным свойством цифрового двойника считается бесстыковая интеграция физического и цифрового объекта» [7]. Предполагается резкое увеличение доступности качественных медицинских услуг за счет цифрового наполнения и подключения нейросетей, сокращения врачебных ошибок. Создав цифрового двойника медицинской организации, можно наблюдать за операционными стратегиями, возможностями, кадрами и моделями, для того чтобы определиться с управленческими действиями, обеспечивая устойчивое развитие. Однако в настоящее время не детализированы вопросы на уровне нормативно-правового регулирования биомедицинских данных: права пациента (насколько возможно использовать данные «двойников пациентов», обучая будущих специалистов IT-технологиям, вопросы врачебной тайны и др. [3].

Заключение. Таким образом, цифровая трансформация отечественного здравоохранения неминуемо замедляется в связи с дефицитом обученных квалифицированных медицинских кадров, обладающих необходимыми hard skills и soft skills для реализации поставленных в указах Президента РФ задач. Отдельные вопросы прав и обязанностей, защиты личной тайны требуют нормативно-правовой проработки применительно к «цифровым двойникам».

Список литературы

1. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года: Указ Президента Российской Федерации

от 07.05.2024 № 309 // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_475991/?ysclid=m10k3rt3d8411155741 (дата обращения: 07.09.2024).

2. Об утверждении стратегического направления в области цифровой трансформации здравоохранения: распоряжение Правительства РФ от 17.04.2024 № 959-р // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/law/hotdocs/84471.html?ysclid=m10k72l4ej981767362 (дата обращения: 07.09.2024).

3. Акулин И. М., Чеснокова Е. А., Смирнова К. М., Пресняков Р. А. Трансформация института врачебной тайны в эпоху электронного здравоохранения // Закон. 2019. № 9. С. 179–189.

4. Бондаренко В. А., Бондаренко А. Г., Дадаян Н. А. Вопросы социального неравенства в доступности медицинских услуг населению и дефицита медицинских кадров в сельских территориях // Евразийский юридический журнал. 2020. № 5(144). С. 423–425.

5. Врачебные дела: юридическая и экспертная оценка проблем ненадлежащего оказания медицинской помощи / А. А. Анисимов, О. Ю. Антонов, Е. Х. Баринов и [др.]. М.: Блок-Принт, 2024. 368 с.

6. Где лучшая медицина в мире в 2024: рейтинг стран по уровню медицины (immigrantinvest.com). 2024, September. URL: https://immigrantinvest.com/ru/blog/10-best-medicine-countries/?ysclid=m0ogv6doxh985160040#avstriya_%E2%80%94_lider_po_chislu_meditsinskogo_personala (дата обращения: 07.09.2024).

7. Зверько Е. Г. Цифровые двойники для цифровой трансформации управления региональной системы здравоохранения // Социально-экономические, организационные, политические и правовые аспекты обеспечения эффективности государственного и муниципального управления: матер. IV Всерос. науч.-практич. конф. молодых ученых. Барнаул, 2022. С. 160–161.

8. Медицинское право России: учебник студентам медицинских вузов, организаторам здравоохранения, социальным работникам / Т. В. Клименко, А. А. Мохов, А. В. Пекшев и [др.]. М.: Проспект, 2024. 544 с.

9. Оценка эффективности медицинских организаций, оказывающих первичную медико-санитарную помощь в условиях подушевого финансирования / А. Л. Линденбратен, П. П. Чуваткин, Н. К. Гришина и [др.] // Проблемы социальной гигиены, здравоохранения и истории медицины. 2019. Т. 27, № 2. С. 144–146.

10. Стрельников С. С., Каткова А. Л., Егоров Д. Б., Захаров С. Д. Реализация проекта «Цифровая кафедра» в медицинском вузе: контекст цифровой трансформации здравоохранения // Мир науки. Педагогика и психология. 2024. Т. 12, № 1. https://mir-nauki.com/issue-1-2024.html

11. Улумбекова Г. Э., Альвианская Н. В. Финансирование системы здравоохранения РФ: динамика, прогнозы, сравнение с развитыми странами // Оргздрав: новости, мнения, обучения. Вестник ВШОУЗ. 2021. Т. 7, № 3(25). С. 36–47.

12. Safarov M. A. Quality of accessibility vs quality accessibility of medical service in Russia: measurement issues // J. Of New Economy. 2023. Т. 24, № 1. С. 126–141.

13. Taiwan: Digital Transformation Advancing Healthcare – OpenGov Asia – 2024, April. URL: https://opengovasia.com/2024/01/04/taiwan-digital-transformation-advancing-healthcare (дата обращения: 07.09.2024).

Т. Ф. Тимофеева,
кандидат юридических наук, доцент,
Чувашский государственный университет им. И. Н. Ульянова
В. В. Тимофеев,
кандидат юридических наук, доцент,
Чебоксарский институт (филиал)
Московского гуманитарно-экономического университета

ЕДИНЫЙ ЦИФРОВОЙ КОНТУР ЗДРАВООХРАНЕНИЯ И ЕГО РОЛЬ В СБЕРЕЖЕНИИ НАРОДОНАСЕЛЕНИЯ

Аннотация. С целью повышения эффективности системы здравоохранения в Российской Федерации активно развиваются медицинские информационные системы. В настоящее время наибольшей актуальностью обладает единый цифровой контур здравоохранения, представляющий собой экосистему информационных решений для обеспечения преемственности оказания медицинской помощи пациентам на основе новых стандартов качества и цифрового сервиса. Такая модель обеспечивает систему управления национальным и региональным здравоохранением актуальными первичными данными. Считаем, что это способствует повышению доступности и качества медицинской помощи населению в системе российского здравоохранения, нацеленного на сбережение народонаселения.

Ключевые слова: система здравоохранения, сбережение народонаселения, единый цифровой контур, дистанционные технологии, цифровизация, медицинская информационная система, цифровые технологии, демография

A SINGLE DIGITAL HEALTHCARE CIRCUIT AND ITS ROLE IN SAVING THE POPULATION

Abstract. In order to improve the efficiency of the healthcare system, medical information systems are actively developing in the Russian Federation. Currently, the most relevant is a single digital healthcare circuit, which is an ecosystem of information solutions to ensure the continuity of medical care for patients based on new quality standards and digital service. This model provides the national and regional healthcare management system with up-to-date primary data. We believe that this contributes to increasing the availability and quality of medical care for the population in the Russian healthcare system, aimed at saving the population.

Keywords: healthcare system, population conservation, single digital circuit, remote technologies, digitalization, medical information system, digital technologies, demography

Введение. Согласно Указу Президента Российской Федерации от 6 июня 2019 г. № 254 «О Стратегии развития здравоохранения в Российской Федерации на период до 2025 года» целями развития здравоохранения являются снижение частоты случаев смерти в социальной среде, увеличение численности населения, продолжительности жизни [6] и др. Для достижения поставленных целей в условиях, осложненных «пандемическим кризисом» и его последствиями, особое внимание

уделяется разработке целевых комплексных программ борьбы с важнейшими классами заболеваний и созданию концепции развития здравоохранения страны. На этом фоне совокупность информационных, организационных, программных, технических и иных средств, предназначенных для автоматизации медицинских процессов и организаций, несомненно, играет важную позитивную роль.

Процесс цифровизации системы здравоохранения начался в 2011 году. Именно тогда было введено понятие «цифровой контур здравоохранения» и введены электронные медицинские карты, электронные больничные листы. Новые возможности не ограничились облачным документооборотом. С 2020 по 2024 год разрабатываются и вводятся в действие дополнительные проекты цифровой трансформации, например, избавляющие пациента от повторного визита в больницу для продления рецептов на лекарственные средства, внедряющие удаленный мониторинг хронических пациентов, вводящие системы, управляющие потоками пациентов, предлагающие телемедицину, «машинное зрение», активно применяются медицинские роботы и даже уже нанороботы [2]. Благодаря цифровизации у сельских докторов появилась возможность получить второе мнение узкопрофильных врачей республиканских клиник. Все это, безусловно, качественно меняет существующее здравоохранение. Однако при этом нельзя забывать и о праве каждого пациента на достоверную медицинскую информацию о состоянии своего здоровья, которое закреплено законодательно в ст. 22 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации». В процессе исследования использованы общенаучные и специальные методы познания, позволившие проследить цифровизацию и технологические новации в здравоохранении.

Степень освещения темы в научной литературе невелика. Исследование вопросов создания единого цифрового контура здравоохранения, реализация единого цифрового контура в субъектах Российской Федерации, его влияние на льготное лекарственное обеспечение, упрощение записи на прием к врачу, сокращение времени ожидания медицинской помощи, а также вопросов оптимизации работы медицинских организаций получило распространение в трудах Е. Е. Асташиной, А. В. Вершицкого, О. Г. Басалаевой, Е. Л. Бойко, О. В. Гаспаряна, Р. Н. Гузеева, А. С. Головковой, Т. В. Зарубиной, А. Б. Леонидова, П. С. Пугачева, Н. Г. Сабитовой, И. В. Свешникова, В. И. Стародубова, К. В. Сидорова, К. Ю. Томашевской, Ю. Р. Хайруллиной и др. Анализ отдельных проблем, связанных с особенностями использования информационных систем в структуре единого цифрового контура здравоохранения в современных условиях, отражен в работах А. В. Боярских, В. А. Галицкой, С. А. Ефремова, Н. Н. Мещеряковой, Г. М. Орлова. Работы этих ученых, специалистов датируются преимущественно 2019–2024 годами.

Основная часть. В рамках национального проекта «Здравоохранение» пятый год (2019–2024 гг.) ведется работа над ключевым проектом «цифровизации» медицины. Целью данной работы является повышение эффективности функционирования системы здравоохранения в направление снижения смертности населения трудоспособного возраста (до 350 случаев на 100 тыс. населения); снижения младенческой смертности (до 4,5 случая на 1 тыс. родившихся детей); ликвидация кадрового дефицита в медицинских организациях, оказывающих первичную медико-санитарную помощь; обеспечение охвата всех граждан профилактическими медицинскими осмотрами не реже одного раза в год и т. д.

Сделать российскую медицину удобной за счет цифровых сервисов, внедрения цифровых технологий и платформенных решений предполагается посредством запуска федерального проекта «Создание единого цифрового контура здравоохранения на основе единой государственной информационной системы в сфере здравоохранения» [7]. Это даст возможность собирать, хранить, обрабатывать, передавать и анализировать большие массивы информации. Для этого должны быть созданы механизмы взаимодействия медицинских организаций на основе единой государственной системы в сфере здравоохранения.

В. Ю. Старцев делает выводы, что «внедрение единого цифрового контура позволит сконцентрировать данные лабораторных служб при оказании медицинской помощи, увеличив количество обследуемых лиц, обеспечив доступность записи через единый портал государственных услуг. Кроме того, передача блоков медицинской информации позволит значительно снизить период времени на получение консультации пациентами со злокачественными новообразованиями» [5. С. 46].

По мнению О. В. Краузе, В. И. Тельцовой, О. А. Гармаш, Л. Г. Долецкой, «создание единой информационной системы взаимодействия всех участников процесса оказания медицинской помощи в результате создания единого цифрового контура здравоохранения, позволит значительно повысить качество оказания экстренной медицинской помощи, в том числе в режиме чрезвычайной ситуации» [3. С. 19–24].

«Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения является важнейшим элементом преобразований, его цель – информационная поддержка процессов управления системой медицинской помощи», – отмечают В. А. Галицкая и Н. Н. Мещерякова. Они же выявили явный «цифровой парадокс»: несмотря на то, что информационные системы плотно вошли в практику медицинских организаций, врач обязан не только вести электронный прием, но также дублировать свои действия в бумажном виде [1. С. 176–196].

И. В. Свешников указывает, что «единый цифровой контур будет задавать тон и формировать тренды информатизации государственного здравоохранения Российской Федерации в ближайшие годы» [4. С. 23–34]. В свою очередь мы считаем, что благодаря единому цифровому контуру здравоохранения обеспечивается преемственность технологических и организационных моделей взаимодействия.

В Чувашской Республике, как и во многих других субъектах Российской Федерации, осуществляется работа по созданию единого цифрового контура здравоохранения. Сегодня все медицинские организации Чувашской Республики объединены в единый цифровой контур в рамках нацпроекта «Здравоохранение», а также двух региональных проектов нацпроекта «Демография». Более 30 % граждан республики являются активными пользователями цифровых медицинских сервисов на Едином портале государственных услуг. Это стало возможным благодаря внедрению Республиканской медицинской информационной системы (далее – РМИС), которая развивается и модернизируется в рамках регионального проекта Чувашской Республики «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы здравоохранения» [8].

На сегодняшний день РМИС позволяет врачам медицинских организаций Чувашии вести электронные медицинские карты пациентов, выписывать электронные рецепты для граждан льготной категории, оказывать медицинскую помощь, используя телемедицинские технологии, вести группы диспансерных больных. В РМИС хранятся результаты всех диагностических исследований пациентов. Кроме этого, в информационной системе врачи видят результаты флюорографии всех пациентов и дату ее прохождения. В прививочном кабинете ведется электронная прививочная карта, в нее заносятся все прививки, которые делают пациентам медицинского центра. Врач может отследить статус пациента в других медицинских организациях после транспортировки санавиацией или наземным транспортом для оказания экстренной медицинской помощи. Также медицинским персоналом подаются экстренные извещения в санитарно-эпидемиологическую службу при выявлении больного с инфекционными или вирусными заболеваниями (например, при выявлении больных COVID-19).

Инструменты РМИС, изображения из долговременного архива диагностических исследований доступны в режиме реального времени всем врачам независимо от расположения рабочего места и нахождения медицинской организации. При необходимости по каждому врачебному участку за любой промежуток времени можно просмотреть, как проходит диспансеризация, сколько было вызовов скорой помощи, сколько человек госпитализировали и по каким причинам, скольких вылечили и скольких не удалось. Благодаря такому удачному межведомственному взаимодействию при использовании РМИС медицинским организациям Чувашии удается эффективнее выстроить работу по оказанию медицинской помощи.

Практически с самого начала создания единого цифрового контура также ведется популяризация телемедицины. Благодаря сформированной многоуровневой телемедицинской инфраструктуре в 2021–2022 годах проведено более 32,5 тыс. региональных телемедицинских консультаций в режиме «врач – врач», «врач – пациент». А с ведущими национальными медицинскими исследовательскими центрами – более 7 тыс. сеансов телемедицины.

Все 520 фельдшерско-акушерских пунктов Чувашской Республики оснащены автоматизированными рабочими местами и подключены к региональной медицинской информационной системе по защищенным каналам связи. Обеспечена работа в специализированной подсистеме РМИС «Автоматизированное рабочее место фельдшера» с возможностью доступа к электронной медицинской карте, результатам лабораторных и инструментальных исследований, организована возможность проведения сеансов телемедицинских консультаций формата «врач – врач».

Осуществляется также поэтапный переход к ведению медицинской документации в форме электронных документов. Правовой базой этого выступают Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральный закон от 8 января 1998 г. № 3-ФЗ «О наркотических средствах и психотропных веществах», Федеральный закон от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств», Федеральный закон от 15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния», Федеральный закон от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», Федеральный закон от 6 апреля

2011 г. № 63-ФЗ «Об электронной подписи», Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также ряд постановлений Правительства Российской Федерации и приказов Министерства здравоохранения Российской Федерации. В свою очередь медицинскими организациями был утвержден пакет необходимых локальных нормативных документов. Таким образом, в Чувашской республиканской медицинской информационной системе к настоящему времени реализована возможность формирования медицинских документов 66 видов в формате структурированного электронного медицинского документа с последующей регистрацией их в подсистеме «Федеральный реестр электронных медицинских документов». В результате в 2023 году на прием к врачу с использованием всех способов записались около 10 млн раз, из них удаленно – 99,5 %.

В Чувашии осуществляется внедрение интеллектуального анализа электронной медицинской карты или изображений инструментальной диагностики с применением искусственного интеллекта. Она представляет собой платформу прогнозной аналитики и управления рисками в здравоохранении для автоматического анализа обезличенных медицинских данных с целью прогнозирования возможных осложнений.

Кроме того, внедряется программное обеспечение для автоматизации диагностических процессов с применением системы поддержки принятия врачебных решений на основе технологии искусственного интеллекта, включающее в себя описание и интерпретацию данных флюорографических исследований, компьютерной томографии органов грудной клетки, маммографических исследований, а также программное обеспечение с применением голосового ассистента на основе технологий искусственного интеллекта и т. д.

За период цифровой трансформации возросло число граждан, воспользовавшихся услугами (сервисами) в Личном кабинете пациента «Мое здоровье» на Едином портале государственных услуг: в 2023 году – 421 тыс. человек, что на 130 тыс. человек больше по сравнению с 2022 годом.

Основными проблемами в настоящее время являются следующие: медицинские информационные системы медленно дорабатываются, пациентам не удается пройти идентификацию, отсутствуют в полном объеме цифровые медицинские профили для всех лиц, застрахованных в системе обязательного медицинского страхования, правовое регулирование несовершенно, пятилетние циклы планирования и бюджетирования неэффективны.

Заключение. Переход на медицинскую информационную систему с точки зрения народосбережения сопровождается реализацией приоритетного направления развития системы здравоохранения, опирающейся на создание единого цифрового контура. По мнению большинства специалистов, потенциал единого цифрового контура здравоохранения способен оказывать положительное влияние на индивидуальные жизненные показатели, способствовать повышению уровня здоровья, качества и продолжительности жизни, решать проблемы, связанные с организационными вопросами деятельности медицинских учреждений. Концепция

единого цифрового контура является оболочкой для создания оптимальной системы здравоохранения, способствующей в существенной степени повышению качества жизни населения.

Список литературы

1. Галицкая В. А., Мещерякова Н. Н. «Цифровые парадоксы» в системе здравоохранения // Вопросы государственного и муниципального управления. № 4. С. 176–196.

2. Гуляева П. С. Медицинские нанороботы в фокусе права // Journal of Digital Technologies and Law. 2023. № 1(1). С. 89–122. https://doi.org/10.21202/jdtl.2023.4. EDN: WNRAOE

3. Краузе О. В., Тельцова В. И., Гармаш О. А., Долецкая Л. Г. Региональный проект Чувашской Республики «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы здравоохранения (ЕГИСЗ)» национального проекта «Здравоохранение» // Вестник скорой помощи. 2022. Т. 3, № 1. С. 19–24.

4. Савватеев В. В., Свешников И. В. Проектирование единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения // Цифровая экономика: региональный аспект: сборник статей Всероссийской научно-практической конференции. Чита, 2019. С. 23–34.

5. Старцев В. Ю., Голубев С. В. Единый цифровой контур для улучшения качества оказания онкологической помощи населению // VII Петербургский международный онкологический форум «Белые ночи 2021». Тезисы форума: материалы VII Петербургского международного онкологического форума. СПб., 2021. С. 46.

6. О Стратегии развития здравоохранения в Российской Федерации на период до 2025 года: Указ Президента РФ от 6 июня 2019 г. № 254 // Собрание законодательства Российской Федерации. 2019. № 23. Ст. 2927.

7. Паспорт федерального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)» // Министерство здравоохранения Российской Федерации [Электронный ресурс]. URL: https://www.rosminzdrav.ru/poleznye-resursy/natsproektzdravoohranenie/tsifra (дата обращения: 27.08.2024).

8. Паспорт регионального проекта Чувашской Республики «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы здравоохранения (ЕГИСЗ)» // Министерство здравоохранения Чувашской Республики [Электронный ресурс]. URL: https://medicin.cap.ru/action/activity/organizaciya-medicinskoj-pomoschi-vzroslomu-nasele/chuvashiya-v-21-m-veke-zdravoohranenie/nacionaljnie-proekti-v-sfere-zdravoohraneniya/pasport/pasport-regionaljnogo-proekta-chuvashskoj-respubli-1 (дата обращения: 14.08.2024).

И. Ю. Шэй,
магистр,
Государственный университет просвещения

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ЗДРАВООХРАНЕНИИ

Аннотация. Главной задачей современных информационных технологий является объединение всех процессов в единое систематизированное информационное поле. Телемедицинские технологии непрерывно расширяются, что требует их должного правового регулирования, поскольку их обширное применение приводит к возникновению большого числа новых пробелов правового регулирования. Информация в системе Интернет становится все более доступной, что также требует совершенствования действующих механизмов защиты конфиденциальных данных пациентов.

Ключевые слова: цифровые технологии, здравоохранение, нормативно-правовое регулирование, медицина, информационные технологии, цифровизация

LEGAL REGULATION OF DIGITAL TECHNOLOGIES IN HEALTHCARE

Abstract. The main task of modern information technologies is to combine all processes into a single systematized information field. Telemedicine technologies are continuously expanding, which requires proper legal regulation, since its extensive application leads to a large number of new regulatory gaps. Information on the Internet is becoming more and more accessible, which also requires improving existing mechanisms for protecting confidential patient data.

Keywords: digital technologies, healthcare, regulatory regulation, medicine, information technology, digitalization

Введение. Главной задачей современных информационных технологий является объединение всех процессов в единое систематизированное информационное поле. В этом контексте современная медицина постепенно становится ведущим социально-экономическим сектором. Так, например, повышается потребность в высококвалифицированном медицинском обслуживании, а также в оптимальных средствах хранения и обмена информацией, которая касается здоровья людей. В связи с этим приказом Министерства здравоохранения Российской Федерации совместно с РАМН от 27.08.2001 № 344/76 «Об утверждении Концепции развития телемедицинских технологий в Российской Федерации и плана ее реализации» использование современных информационно-телекоммуникационных технологий при оказании помощи населению было обозначено стратегически важной задачей в условиях реформирования всей системы здравоохранения в целом.

Основная часть. Если обратиться к практике зарубежных стран, стоит подметить, что формирование информационных (также телемедицинских) технологий было определено необходимостью в систематизации сведений о пациентах, а также обеспечении медицинской помощи лицам, для которых она была трудно-

доступна или недоступна вовсе. Например, в 1970-х гг. в академических медицинских центрах США были разработаны системы хранения данных об амбулаторной помощи пациентам [3. С. 907].

С начала 1996 года в США стало разрешено использование изображений, включая фотографии, для диагностики и лечения через электронные коммуникации, а также для предупреждения заболеваний, недомоганий и боли.

Сегодня телемедицина играет ключевую роль в процессе глобальной информатизации здравоохранения, расширяя свои возможности и влияние, и особую значимость, как справедливо отмечает ряд авторов, телемедицинские технологии получили в период пандемии, объявленной ВОЗ в связи с распространением новой коронавирусной инфекции COVID-19 [4. С. 19; 6; 7; 8. С. 241].

В научной литературе в систему обмена информацией медицинского характера посредством информационно-коммуникационных технологий, как правило, включают несколько элементов [1. С. 564] (рис. 1).

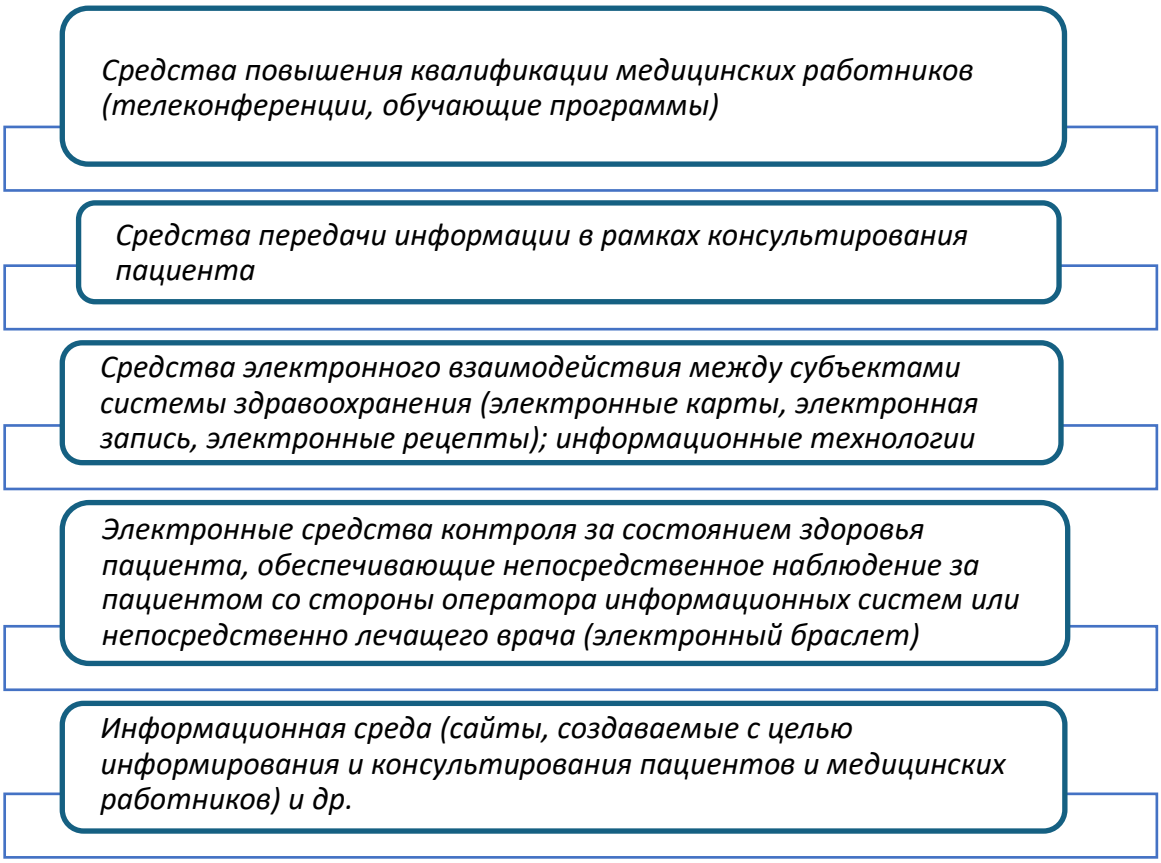

Рис. 1. Элементы обмена информацией медицинского характера

В 2001 году Координационный совет по телемедицине Минздрава России разработал упомянутую ранее Концепцию развития телемедицинских технологий в Российской Федерации, где впервые введено понятие «телемедицина». Теперь это понятие рассматривается в широком смысле, охватывая различные сферы применения информационных технологий в здравоохранении. Оно включает в себя лечебно-диагностические консультации, телемониторинг функциональных

показателей, «интернет-медицину» (веб-сайты, информационные базы данных, справочно-консультативные системы), а также управленческие, образовательные, научные и просветительские мероприятия в области здравоохранения.

Сегодняшний мир стал свидетелем стремительного развития нормативного регулирования в области информатизации здравоохранения. Федеральный закон от 29.07.2017 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» (далее – ФЗ № 242) внес изменения в законодательные акты о применении информационных технологий в сфере здоровья. Данным законом было введено новое понятие – «телемедицинские технологии», которое уже значительно отличается от предложений в Концепции создания единой государственной информационной системы в сфере здравоохранения, утвержденной приказом Минздравсоцразвития России от 28.04.2011 № 364. Теперь эти технологии включают две области – дистанционное оказание медицинской помощи (телеконсультации, дистанционное наблюдение) и электронный медицинский документооборот (электронные карты, электронные рецепты). В связи с этим упомянутая выше Концепция создания единой государственной информационной системы в сфере здравоохранения несет на себе не такую значимость, как прежде, в условиях постоянных изменений и дополнений в законодательстве.

В современной системе здравоохранения России цифровой контур был определен ФЗ № 242. В соответствии с данным нормативным правовым актом медицинская документация может вестись только в электронной форме и нет необходимости делать дубликаты на бумажных носителях. Пациенты или их законные представители могут давать информированное согласие на медицинские вмешательства в электронном виде. Также они могут получать свои медицинские документы, отражающие их состояние здоровья, в электронной форме.

Кроме того, были внесены изменения в Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» и Федеральный закон от 08.01.1998 № 3-Ф «О наркотических средствах и психотропных веществах». Внесенные изменения предусматривают возможность выдачи рецептов на лекарственные препараты в электронной форме с письменного согласия пациента. Также меняется порядок оформления этих рецептов.

Кроме того, получило уточнение понятие «рецепт на лекарственный препарат» в Федеральном законе от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств». Изменения были вызваны требованием подписания рецептов в электронной форме, усиленной квалифицированной электронной подписью медицинского работника или медицинской организации в случае выписки рецептов с наркотическими средствами или психотропными веществами. В рамках данных изменений устанавливается порядок информационного обеспечения в сфере здравоохранения через создание, развитие и использование информационных систем, включая единую государственную информационную систему в сфере здравоохранения (ЕГИЗС), которая позволяет гражданам получать услуги в электронной форме через единый портал государственных и муниципальных услуг, а также вести федеральные реестры в сфере здравоохранения в соответствии с законодательством.

Федеральный закон от 28.12.2017 № 425-ФЗ «О внесении изменений в Федеральный закон «Об обращении лекарственных средств» обязывает производителей применять средства идентификации на упаковке лекарственных средств. В единую систему включены сведения, определенные федеральным законом, о деятельности медицинских организаций и услугах, собираемые, хранимые, обрабатываемые и предоставляемые информационными системами. Взаимодействие информационных систем в сфере здравоохранения и медицинских организаций также происходит.

С 1 июля 2017 года вступил в силу Федеральный закон от 1 мая 2017 г. № 86-ФЗ «О внесении изменений в статью 13 Федерального закона "Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством" и статьи 59 и 78 Федерального закона "Об основах охраны здоровья граждан в Российской Федерации"», которым были установлены новые правила для производителей лекарственных препаратов. Теперь все они должны обязательно вносить информацию о своей продукции в систему мониторинга. Помимо этого, введение электронных больничных листков и функционирование ФГИС ЕИИС «Соцстрах» стали частью новых правовых оснований, предусмотренных законом.

В сфере информатизации здравоохранения Президентом РФ были утверждены значимые документы, определяющие стратегические цели и задачи для развития Российской Федерации до 2024 года. В этих документах предусмотрено использование современных технологий, включая информационные ресурсы и отечественное программное обеспечение.

Оптимизация работы медицинских организаций и внедрение электронных сервисов для пациентов и врачей, предполагаемые приоритетным проектом «Совершенствование процессов организации медицинской помощи на основе внедрения информационных технологий», способствуют повышению эффективности оказания медицинской помощи. Защита населения от фальсифицированных, недоброкачественных и контрафактных лекарственных препаратов обеспечивается приоритетным проектом «Внедрение автоматизированной системы мониторинга движения лекарственных препаратов от производителя до конечного потребителя для оперативного выведения из оборота контрафактных и недоброкачественных препаратов».

Правительство приняло целый ряд мер для содействия информатизации сектора здравоохранения. Законодательные акты, направленные на расширение доступа к медицинским услугам через Интернет, были утверждены на уровне Правительства. В документах, принятых Правительством РФ, предусмотрено использование сервиса личного кабинета пациента «Мое здоровье». Граждане могут обращаться за вызовом врача на дом, получать информацию о медицинском прикреплении, медицинской помощи, полисе ОМС и других медицинских данных. Также в рамках новых нормативных актов граждане имеют возможность записаться на профилактические осмотры и диспансеризацию.

В рамках программы Цифровая экономика Российской Федерации, утвержденной распоряжением Правительства Российской Федерации № 1632-р от 28.07.2017, предусмотрена реализация проекта «Цифровое здравоохранение».

Постановление Правительства Российской Федерации от 12.04.2018 № 447 утверждает Правила взаимодействия информационных систем в сфере здравоохранения и медицинских организаций, позволяя коммерческим организациям создавать сервисы на основе данных из информационных систем, включая запись к врачу, телемедицинские консультации и информирование о медицинской помощи.

Важно отметить Постановление Правительства Российской Федерации от 05.05.2018 № 555 (ред. от 14.12.2021) «О единой государственной информационной системе в сфере здравоохранения» (вместе с «Положением о единой государственной информационной системе в сфере здравоохранения»), установившее основы деятельности общегосударственной информационной системы в сфере здравоохранения. Этот документ определяет задачи, функции, доступ к информации, обмен информацией, участников системы и другие аспекты ЕГИСЗ. Некоторые аспекты цифровизации здравоохранения регламентированы в различных приказах Министерства здравоохранения. Например, приказ Минздрава России от 30.11.2017 № 965н «Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий» установил правила для медицинских организаций всех уровней и форм собственности, включая порядок предоставления медицинской помощи с использованием телемедицинских технологий. Этот документ также определяет процедуру дистанционного оказания медицинской помощи между специалистами и пациентами или их представителями.

Обеспечение развития использования телемедицинских технологий осуществляется при помощи специальных информационных систем, которые способны хранить и обрабатывать информацию о здоровье в электронном виде. По приказу Минздрава России от 09.01.2018 № 2н «О внесении изменений в приказ Министерства здравоохранения Российской Федерации от 15 декабря 2014 г. № 834н «Об утверждении унифицированных форм медицинской документации, используемых в медицинских организациях, оказывающих медицинскую помощь в амбулаторных условиях, и порядков по их заполнению», установлен порядок ведения электронной медицинской документации. В свою очередь, приказом Минздрава России от 04.05.2018 № 201н «Об утверждении показателей, характеризующих общие критерии оценки качества условий оказания услуг медицинскими организациями, в отношении которых проводится независимая оценка» устанавливаются показатели, отражающие общие критерии оценки качества условий предоставления медицинских услуг. Эти показатели включают в себя информационное наполнение сайта медицинской организации, наличие онлайн-сервисов для записи к врачу через Интернет, возможность обращения онлайн, опросы о качестве услуг, специальную версию сайта для людей с нарушениями зрения и другие критерии.

В 2018 году в феврале было принято решение о создании консорциума «Цифровое здравоохранение» по инициативе Минкомсвязи и Минздрава России. Основной целью этого документа стала подготовка к переводу национальной медицины на модель «цифрового двойника» для каждого человека, независимо от его местоположения. Приказ Минздрава России от 14.06.2018 № 341н «Об утверждении Порядка обезличивания сведений о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские

экспертизы, медицинские осмотры и медицинские освидетельствования» определяет порядок обезличивания данных о лицах, получающих медицинскую помощь, а также о лицах, подвергающихся медицинским экспертизам, осмотрам и освидетельствованиям, обеспечивая защиту этих данных от несанкционированного использования и одновременно обеспечивая возможность их дальнейшей обработки.

Эффективное практическое тестирование технологий достигается благодаря тесной координации деятельности ведомств и заинтересованных сторон. Прогноз социально-экономического развития Российской Федерации на период до 2024 года, подготовленный Минэкономразвития в рамках исполнения Указа Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», предусматривает реализацию национального проекта «Здравоохранение». Этот проект включает в себя 8 федеральных проектов, в числе которых «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы здравоохранения (ЕГИСЗ)».

В соответствии с данным прогнозом до конца 2024 года в 85 субъектах Российской Федерации планируется создание централизованных сервисов для обеспечения непрерывной медицинской помощи. Эти сервисы будут включать в себя государственные информационные системы в сфере здравоохранения, которые объединят все медицинские организации региона. Также будет организован мониторинг оказания медицинской помощи по различным профилям заболеваний, маршрутизация пациентов и телемедицинские консультации. Важным элементом проекта будет автоматизированная диспетчеризация санитарного транспорта. Основные направления федерального проекта также включают в себя персонализированную медицину и формирование современной системы непрерывного медицинского образования.

Также, согласно прогнозу, до конца 2024 года более 70 регионов России будут использовать технологию электронных рецептов, автоматизированное управление льготными лекарствами и телемедицинские консультации. Подключение медицинских учреждений и государственных информационных систем к ЕГИСЗ в субъектах Российской Федерации позволит гражданам воспользоваться услугами в личном кабинете пациента «Мое здоровье» на ЕПГУ: к концу 2024 года – доступ к своим электронным медицинским документам.

В соответствии с прогнозом, к концу 2024 года каждый второй человек, имеющий доступ к услугам ЕГИСЗ, сможет воспользоваться единой цифровой платформой в здравоохранении. Доля медицинских организаций, участвующих в информационном взаимодействии с ЕГИСЗ, достигнет 100 %.

С возрастанием использования информационных технологий в сфере медицины возникают новые юридические проблемы. Необходимость защиты конфиденциальных данных пациентов в условиях активного обмена информацией в Интернете требует усовершенствования механизмов защиты, на что обращают внимание многие специалисты. Особенно важным становится обеспечение безопасности и конфиденциальности данных, связанных с жизнью и здоровьем пациентов, в контексте использования ЕГИСЗ [2. С. 13].

Таким образом, следует отметить, что система здравоохранения должна быть современной и адаптированной к цифровой эпохе. Это требует изменений в законодательстве для учета новых реалий. Ответственность, гарантии и контроль в здравоохранении должны быть пересмотрены в соответствии с требованиями цифровой эры [5. С. 95–98]. Участие граждан в здравоохранении также должно быть пересмотрено и увеличено. Все это является основой для модернизации системы здравоохранения.

Список литературы

1. Давыдова М. Л. Телемедицина и экспериментальные правовые режимы в области здравоохранения: проблемы и перспективы внедрения // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2023. Т. 27, № 3. С. 564–582.

2. Карцхия А. А. Информационно-правовое обеспечение цифровой экосистемы здравоохранения // Правовая информатика. 2021. № 1. С. 13–23.

3. Правовые аспекты регулирования закона о телемедицине: российский и американский опыт / Е. А. Короткова, М. А. Башинджагян, И. А. Филонов, Е. Н. Богданова // Актуальные вопросы современной медицинской науки и здравоохранения: материалы V Международной научно-практической конференции молодых ученых и студентов, посвященной 75-летию Победы в Великой Отечественной войне, 90-летию УГМУ и 100-летию медицинского образования на Урале, Екатеринбург, 9–10 апреля 2020 года. Т. 3. Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации, 2020. С. 907–911.

4. Телемедицина в период пандемии COVID-19 / Г. Е. Аимбетова, В. Ю. Байсугурова, М. А. Канушина [и др.] // Наука и здравоохранение. 2022. Т. 24, № 4. С. 19–26.

5. Шутова А. А. Применение технологий искусственного интеллекта в сфере здравоохранения: уголовно-правовые девиации // Правопорядок: история, теория, практика. 2023. № 3(38). С. 92–100. EDN: RKMSGE. DOI: 10.47475/2311-696X-2023-38-3-92-100

6. Гараева А. С., Залоило М. В., Полещук И. А., Власова Н. В., Гераськина Н. С. Исторические предпосылки внедрения телемедицинских технологий в сферу здравоохранения в России // Вопросы истории. 2020. № 12(1). С. 218–225.

7. Гараева А. С., Залоило М. В., Полещук И. А., Власова Н. В., Фомина Е. В. Телемедицина в России: опыт осмысления в юридической доктрине и становление правового регулирования // Вопросы истории. 2020. № 11(1). С. 243–248.

8. Щербакова И. В., Амиров Ш. М. Телемедицина: понятие и роль в период пандемии Ковид-19 // Наука и образование в контексте глобальной трансформации: сборник статей XII Международной научно-практической конференции, Петрозаводск, 7 декабря 2023 года. Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская И.И.), 2023. С. 241–246.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМ

Е. Н. Абрамова,
кандидат юридических наук, доцент,
Санкт-Петербургский государственный экономический университет

АРЕНДА БЕСПИЛОТНОГО ТРАНСПОРТНОГО СРЕДСТВА

Аннотация. Целью исследования является обоснование необходимости внесения в гражданское законодательство новых правовых норм, предусматривающих понятие и особенности договора аренды беспилотного транспортного средства, а также разработку эффективного правового регулирования отношений, специфической особенностью которых является передача во временное пользование нового для большинства национальных законодательств объекта. В статье подчеркивается недостаточность общих норм о договоре аренды, в том числе о договоре аренды транспортного средства, при регулировании названных отношений, которые не позволяют учитывать отсутствие экипажа в салоне арендованного транспортного средства, влекущее неопределенность по поводу субъекта ответственности при причинении арендованным транспортным средством имущественного вреда и вреда жизни и здоровью.

Ключевые слова: беспилотное транспортное средство, автономное судно, беспилотное судно, оператор автоматизированной системы управления, аренда транспортного средства, удаленное управление транспортным средством, искусственный интеллект

RENTAL OF AN UNMANNED VEHICLE

Abstract. The purpose of the study is justify and propose legal regulation for a new type of lease agreement rent – an unmanned vehicle. The author suggests introducing additional responsibilities for the parties to agreement, the introduction of responsibility regardless of guilt when using artificial intelligence and offers the author's definition of an unmanned vehicle lease agreement.

Keywords: unmanned vehicle, drone, automated vessel, control operator, remote control, artificial intelligence

Введение. Беспилотное транспортное средство (далее – БТС) – новое явление для экономики и современного общества, которое все активнее входит в повседневную жизнь каждого человека. При этом развивается не только традиционный транспорт на основе использования технологии искусственного интеллекта, но и новые виды аппаратов, такие как дроны, квадрокоптеры, роботы-доставщики и пр., правовая квалификация которых пока не разработана. Цель статьи – обоснование необходимости внесения в гражданское законодательство новых правовых норм, предусматривающих понятие и особенности договора аренды беспи-

лотного транспортного средства, а также разработка эффективного правового регулирования отношений, специфической особенностью которых является передача во временное пользование нового для большинства национальных законодательств объекта.

Основная часть. Законодательство о таких транспортных и иных средствах только начинает развиваться. Так, в 2015 году в ст. 32 Воздушного кодекса РФ были введены такие новые понятия, как пилотируемое и беспилотное воздушные суда, беспилотная авиационная система и линия управления беспилотными авиационными системами контроля беспилотной авиационной системы, учитывающие широкое применение в воздушных перевозках автоматизированных систем дистанционного управления транспортным средством пилотом, который находится вне его борта. В воздушном законодательстве такой пилот получил наименование внешнего пилота, но наиболее часто его называют оператором управления беспилотного транспортного средства.

Несмотря на то, что с момента указанных новелл воздушного законодательства прошло почти десять лет, продолжения указанным тенденциям учета цифровизации экономических процессов в транспортной деятельности в российском законодательстве долгое время не имелось. В 2023 году понятия автономного суда и полуавтономного суда, которые определяются через признаки осуществления процесса управления в автоматическом режиме и способности осуществления плавания без экипажа на борту, появились в КТМ РФ и КВВТ РФ [6], а также была утверждена Стратегия развития беспилотной авиации на период до 2030 года [8]. В целях регулирования договорных отношений транспортное законодательство пока не отреагировало на цифровые вызовы и фактическое использование автономных судов в морском, автомобильном и иных видах транспорта, в том числе общественного, хотя в юридической литературе отмечается, что анализ законодательных инициатив многих зарубежных стран, таких как США, Япония, Германия и многие другие, показывает, что вопросам правового регулирования отдельных видов БТС, например, беспилотных летательных аппаратов уделяется серьезное внимание [1. С. 131]. Так, в действующем ГК РФ отсутствуют какие-либо попытки учесть особенности правового регулирования БТС. При этом наличие существенной специфики гражданско-правовых отношений, основанных на использовании БТС, очевидна. Представляется важным учитывать ее при регулировании разнообразных договорных отношений, поскольку дистанционность управления транспортным средством приводит к возникновению ряда нерешенных теоретических проблем, что, в свою очередь, ухудшает правовое положение субъектов гражданского оборота, внося неопределенность не только в вопросы выбора (например, способа защиты своих прав при их нарушении), но даже в вопросе самой возможности такой защиты.

Одним из многих гражданско-правовых договоров, при заключении которых необходим учет использования его сторонами БТС, является договор аренды, в котором БТС выступает объектом, передающимся во временное пользование за плату другому лицу. Транспортные средства являются объектами, передача в пользование которых обладает существенной спецификой, что учитывается гражданским законодательством РФ, предусматривающим специальные правила об

аренде такого вида имущества как транспортное средство. Но наличие особенностей, возникающих в арендных отношениях при передаче в пользование БТС, в гражданском российском законодательстве не учитывается.

Например, требующей пересмотра представляется категория «экипаж», которая ранее не вызывала вопросов, поскольку не является цивилистической и всегда трактовалось на бытовом уровне, что было достаточно в условиях обязательного наличия водителя, пилота непосредственно внутри движущегося транспортного средства. В юридической литературе отмечается также проблема отсутствия такой категории, как «транспортное средство без водителя в кабине» [8. С. 103]. Кроме того, в отличие от традиционных транспортных средств для БТС появляется новый участник, правовой статус которого не определен, – оператор, осуществляющий удаленное управление БТС с помощью цифровых технологий. Таким образом, развитие БТС приводит к необходимости разработки, казалось бы, не новой для цивилистики категории – экипаж транспортного средства, чтобы понимать его понятие, состав и значение каждого его участника.

Когда речь идет о БТС, управление им осуществляется дистанционно. При этом возможны разные варианты степени участия человека в управлении БТС. Во-первых, в кабине транспортного средства может находиться некий субъект, которого принято именовать пилотом, водителем, хотя он не управляет движением, а лишь выполняет, скорее, контрольные функции в целях обеспечения безопасности и мониторинга. Само управление движением (маршрутизация, управление техническими функциями движения транспортного средства и т. п.) в таком случае осуществляет либо иной субъект – оператор дистанционного управления, либо технология искусственного интеллекта. Во-вторых, в кабине транспортного средства человека может не быть вовсе или в кабине могут быть иные члены экипажа, не являющиеся водителем, пилотом, – инженеры, механики и т. п. Как представляется, все эти нюансы требуют учета при разработке правового регулирования.

Тем не менее аренду БТС следует рассматривать как вид договора аренды транспортного средства. Если оператором автоматизированной системы управления БТС является арендодатель по договору аренды БТС или привлеченный арендодателем профессиональный оператор, к отношениям по договору аренды БТС могут применяться правила об аренде транспортного средства с экипажем. Если оператором автоматизированной системы управления беспилотным транспортным средством является арендатор по договору аренды БТС или привлеченный арендатором профессиональный оператор, к отношениям по договору аренды БТС могут применяться правила об аренде транспортного средства без экипажа.

Решению подлежит вопрос о виде договора аренды при управлении БТС не человеком, а системой искусственного интеллекта. Действующее законодательство не дает возможности найти ответ на вопрос о том, какая это аренда – с экипажем или без. Арендодатель в этом случае не оказывает услуг по предоставлению квалифицированного экипажа, за действия которого мог бы нести ответственность. Однако он передает транспортное средство на основе искусственного интеллекта, в результате чего у арендатора будут отсутствовать возможности влия-

ния на качество управления транспортным средством. Действующее законодательство не дает возможности найти ответ на данный вопрос. Тем не менее представляется, что в этом случае можно предложить считать передачу в пользование БТС, работающего на базе генеративной сети, арендой транспортного средства без экипажа, поскольку арендатор должен осознавать ответственность за использование подобных объектов и делать выбор в их пользу только в случае полной уверенности в их надежности. Кроме того, именно он будет лицом, обслуживающим бесперебойность функционирования программного и иного оборудования, заинтересованным в его регулярном обновлении и безопасности.

Основная специфика аренды БТС заключена в дополнительных обязанностях сторон договора и распределении ответственности, поскольку именно вопрос о субъекте ответственности является наиболее важным практически.

В частности, как представляется, если БТС передается с экипажем, на арендодателя необходимо возложить дополнительные обязанности, которые на данный момент отсутствуют в ГК РФ, но которые обязан нести арендодатель, помимо тех обязанностей, которые предусмотрены ст. 634–637 ГК РФ. К ним обоснованным видится отнести следующие:

а) принимать меры к обеспечению конфиденциальности и безопасности предоставленной арендатором информации, в том числе полученной в результате обработки предоставленной арендатором информации и информации, передаваемой в системе в рамках осуществления автоматизированного управления;

б) обеспечивать бесперебойное и безопасное функционирование автоматизированной системы управления, не допуская технических сбоев, в том числе принимать профилактические меры в целях предупреждения утечки данных, неавторизированного доступа к системе, искажения передаваемой информации, в том числе распоряжений;

в) обеспечивать своевременное обновление и обслуживание программного обеспечения.

Обязанности, указанные под пунктами б) и в), целесообразно распространить также на арендатора при аренде без экипажа.

Указанные обязанности призваны учесть такую особенность БТС, как риски для приватности [4. С. 23], связанные с возможностью их эксплуатации только при условии наличия большого массива информации об арендаторе, в том числе личных, персональных и иных данных, которые должны быть защищены, а также необходимость эксплуатации, обслуживания и поддержания в актуальном и исправном состоянии не только самого БТС, но и программного обеспечения, на базе которого оно функционирует.

От надлежащего выполнения указанных дополнительных обязанностей качество управления зависит настолько сильно, что представляется обоснованным установить принцип безвиновной ответственности арендодателя за вред, причиненный в результате их неисполнения или ненадлежащего исполнения. Кроме того, поскольку обновление программного обеспечения, поиск новых способов защиты информации, мониторинг качества работы автоматизированных систем, защита целостности системы автоматизированного управления от взлома и многих других факторов, которые могут негативно повлиять на эксплуатацию БТС и его

безопасность для арендатора и третьих лиц, полностью зависят от арендодателя, и в целях стимулирования осуществления указанной и иной деятельности, направленной не только на повседневное удаленное управление БТС, но и на осуществление профилактических мер, направленных на предотвращение возможного вреда, представляется обоснованным возложить на арендодателя несение ответственности независимо от вины за вред, причиненный третьим лицам и арендатору в результате недостатков, сбоев и ошибок автоматизированной системы управления.

В иных случаях обоснованным представляется подход, распространенный в европейском законодательстве о БТС [5], закрепляющий презумпцию виновности водителя [1. С. 124]. Представляется возможным распространить ее на субъекта, предоставившего экипаж в случае договора аренды.

Еще одно исключение из общих правил представляется обоснованным сделать в случае аренды БТС на основе искусственного интеллекта в связи с необходимостью установления субъекта, несущего ответственность за вред, причиненный в результате использования нейротехнологии и технологии искусственного интеллекта. Данный вопрос на сегодняшний день является дискуссионным в цивилистической доктрине. При этом более обоснованной представляется точка зрения, основанная на необходимости возложения ответственности на пользователя объекта на основе искусственного интеллекта как фактического владельца источника повышенной опасности. Хотя окончательную точку в данной дискуссии может поставить только законодатель.

Поскольку представляется обоснованным рассматривать аренду БТС на основе технологии искусственного интеллекта видом аренды без экипажа, то транспортное средство считается управляемым и обслуживаемым силами арендатора. В такой ситуации целесообразным будет считать именно его субъектом ответственности за убытки, причиненные эксплуатацией БТС. Более того, технология искусственного интеллекта не может рассматриваться как полностью обеспечивающая предсказуемость и полную безопасность эксплуатации. Поэтому лицо, решившееся на ее применение, должно нести все риски, связанные с таковой. Поэтому представляется обоснованным возложить на арендатора ответственность независимо от вины за убытки, причиненные жизни и здоровью в результате использования технологии искусственного интеллекта. При этом подобная норма представляется необходимой в качестве общей для любых договорных конструкций.

Наконец, необходима разработка правового положения нового для гражданских правоотношений субъекта, осуществляющего деятельность по удаленному управлению транспортными средствами с помощью цифровых платформ – оператора автоматизированной системы управления. Речь идет о случаях, когда сторона договора не совпадает с оператором БТС в одном лице. Фактически данный субъект становится лицом, от которого зависит исполнение дополнительных для арендатора и арендодателя, предложенных в настоящей статье обязанностей.

В ходе проведения эксперимента [7] в России установлена ответственность оператора БТС за недостатки при выполнении его функций по управлению движением, но не за вред, причиненный в результате технических неисправностей,

хотя в качестве последних могут выступать и неисправности системы автоматизированного управления. При этом субъект ответственности за технические неисправности назван весьма неопределенно, как лица, которые ответственны за техническое обеспечение транспортного средства и (или) единоличный исполнительный орган субъекта экспериментального правового режима. Подобная формулировка допускает двоякий подход к определению субъекта ответственности. Кроме того, наличие множества субъектов, каждый из которых несет ответственность за отдельный блок происшествий, как представляется, при заключении договора аренды не отвечает потребностям торгового оборота, участники которых должны ясно понимать, с кем имеют дело и к кому могут обратиться с соответствующими требованиями. Поэтому в целях регулирования арендных отношений целесообразным видится использование конструкций субсидиарной ответственности и права регресса при общем правиле об ответственности сторон договора аренды друг перед другом и перед третьими лицами, которым причинен вред эксплуатацией БТС.

Заключение. Поэтому, во-первых, целесообразным представляется установить субсидиарную ответственность оператора автоматизированной системы управления за вред, причиненный третьим лицам и сторонам договора аренды при управлении беспилотным транспортным средством. Во-вторых, разумным наделить сторону договора аренды БТС правом взыскать в порядке регресса с привлеченного ею по договору оператора БТС затраты, произведенные стороной договора аренды БТС возмещением убытков, причиненных нарушением дополнительных обязанностей, предложенных в настоящей статье для арендатора и арендодателя. Указанное право регресса позволит защитить права стороны договора аренды, возместившей убытки, причиненные не по ее вине, а по вине оператора управления, поскольку именно от него фактически зависит исполнение таких дополнительных обязанностей, для исполнения которых сторона договора аренды и привлекает оператора по договору об оказании услуг, которые, в свою очередь, также должны быть качественными.

Таким образом, действующее правовое регулирование договора аренды совершенно не учитывает возможность передачи в аренду БТС и в целях ликвидации указанного пробела нуждается в разработке абсолютно новых правовых норм о передаче в пользование БТС.

Список литературы

1. Грищенко Г. А. Правовое регулирование беспилотных летательных аппаратов: российский подход и мировая практика // Вестник университета им. О. Е. Кутафина. – 2019. – № 12. – С. 131.

2. Коробеев А. И., Чучаев А. И. Беспилотные транспортные средства, оснащенные системами искусственного интеллекта: проблемы правового регулирования // Азиатско-Тихоокеанский регион: экономика, политика и право. – 2018. – № 3. – С. 124.

3. Королева Е. Г. Современное состояние правового регулирования беспилотных транспортных средств в России и анализ зарубежного опыта // Криминологический журнал. – 2021. – № 2. – С. 103.

4. Молчанов А. А. Некоторые правовые аспекты и проблемы использования интеллектуальных транспортных систем // Аграрное и земельное право. – 2018. – № 2. – С. 23.

5. Нигматуллин И. Германия придумала 3 этических правила для беспилотных авто // Хайтек. – URL: https://hightech.fm/2016/09/12/3-rules (дата обращения: 01.09.2024).

6. О внесении изменений в отдельные законодательные акты: Федеральный закон от 10 июля 2023 г. № 294 // СПС Консультант-Плюс [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_451655 (дата обращения: 01.09.2024).

7. Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по предоставлению транспортных услуг с использованием высокоавтоматизированных транспортных средств на территориях отдельных субъектов Российской Федерации: Постановление Правительства РФ от 29 декабря 2022 г. № 2495 // СПС Консультант-Плюс [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_436544 (дата обращения: 01.09.2024).

8. Стратегия развития беспилотной авиации на период до 2030 года: Распоряжение Правительства Российской Федерации от 21 июня 2023 г. № 1630-р. // СПС Консультант-Плюс. [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_450667 (дата обращения: 01.09.2024).

О. А. Хотько,
кандидат юридических наук, доцент,
Белорусский государственный университет

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ В СФЕРЕ ОКАЗАНИЯ ТРАНСПОРТНЫХ УСЛУГ НА СОВРЕМЕННОМ ЭТАПЕ: ПРАВОВЫЕ ОСНОВАНИЯ И ЗАКОНОДАТЕЛЬНЫЕ ПОДХОДЫ

Аннотация. В данной работе анализируется роль применения цифровых проектов и потребность цифровых платформ в Республике Беларусь и интеграционных объединениях с ее участием. Особенность статьи заключается в обосновании потребности единых подходов с правовым регулированием Российской Федерации в рамках успешного функционирования Союзного государства, созданием и эксплуатацией интеллектуальных транспортных систем, 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: цифровые технологии, транспортное право, транспортные услуги, транспортное законодательство, интеллектуальные транспортные системы, правовое регулирование, Союзное государство, Евразийский экономический союз

DIGITAL TRANSFORMATION IN THE FIELD OF PROVIDING TRANSPORT SERVICES AT THE PRESENT STAGE: LEGAL BASIS AND LEGISLATIVE APPROACHES

Absract. This paper analyzes the role of the use of digital projects and the need for digital platforms in the Republic of Belarus and integration associations with its participation. The peculiarity of the article is to substantiate the need for unified approaches to the legal regulation of the Russian Federation within the framework of the successful functioning of the Union State, connection with the creation and operation of intelligent transport systems, determining the main directions for improving legal norms and legislative acts in light of the need to ensure national and regional security in the territory of the Eurasian space and the Union State.

Keywords: digital technologies, transport law, transport services, transport legislation, intelligent transport systems, legal regulation, Union State, Eurasian Economic Union

Введение. Внедрение информационно-коммуникативных и цифровых технологий в жизнь человека при оказании тех или иных услуг является неотъемлемой тенденцией современного общества. В связи с этим трансформируются поведенческие мотивы каждого, видоизменяется правовое регулирование соответствующих отношений, а главное – обеспечиваются основные ценности общества, направленные на безопасность личности и государства. Не остались в стороне и процессы в транспортной сфере, тем более что транспорт – это многовекторный и сложный комплекс объектов транспортной инфраструктуры, транспортных средств, систем управления.

На трансформацию транспортных отношений в новых условиях включения цифровых технологий в данную отрасль в современных реалиях обращается внимание в научной литературе [1]. Множество сфер, в которых задействуются цифровые технологии, получают внедрение при эксплуатации объектов транспортной деятельности. В частности, это касается разработки и использования цифровых платформ относительно деятельности транспорта, что обеспечивает прозрачность осуществления перевозки и документооборота. В данной статье приведем примеры нормативного закрепления процессов цифровизации и некоторые вопросы, возникающие в связи с этим.

Обозначим, что вопросы цифровизации становятся актуальнее не только в рамках государства, но и с учетом интеграционных процессов на евразийском пространстве и в рамках Союзного государства. В соответствии с Декларацией о дальнейшем развитии экономических процессов в рамках Евразийского экономического союза до 2030 года и на период до 2045 года «Евразийский экономический путь» государствами – членами данного Союза принимается во внимание актуальность цифровизации экономических процессов как важной составляющей модернизации экономик входящих в объединение стран, а формирование общего транспортно-логистического пространства включает упрощение и цифровизацию транзитных перевозок грузов в международном сообщении. Цифровизация на евразийском пространстве автором данной статьи освещалась ранее, и отмечалось, что цифровые трансформации активнее проникают в процессы перевозки,

что подтверждается принятыми актами Евразийского экономического союза (далее – ЕАЭС) [2]. В целях ускоренного и свободного перемещения товаров в соответствии с Соглашением о применении навигационных пломб для отслеживания перевозок от 19 апреля 2022 г. применяются устройства дистанционного контроля за перемещением товаров и транспортных средств, что способствует оптимизации механизма отслеживания перевозок товаров, обеспечению прозрачности перевозок, минимизации проведения контрольных мероприятий и тем самым законности при данном (ускоренном) подходе доставки грузов.

Безусловно, прав В. Сюн, отмечающий, что «на древнем пути, где раньше звенели колокольчики караванов верблюдов, теперь зазвучали паровые свистки… Здесь столкнулись современная цивилизация и древняя история, но это послужило толчком к дальнейшему развитию» [3. С. 119]. Дальнейшее развитие уже перешло на новый уровень внедрения цифровых технологий, в том числе в свете реализации китайской инициативы международного характера «Один пояс, один путь».

Основная часть. Цифровые проекты относятся к востребованным и своевременным средствам усиления транспортной безопасности и интеграционных связей при оказании транспортных услуг, в первую очередь в таких объединениях, как Союзное государство и ЕАЭС. Современный этап развития транспортных правоотношений достиг уровня, при котором особое внимание уделяется качеству и безопасности оказания услуг, упрощению государственного управления в отношении контроля за деятельностью перевозчиков, недопущения ситуаций нарушения законодательства. Полагаем, нет смысла говорить о положительных и отрицательных тенденциях цифровизации (хотя тотальный контроль и киберпреступность можно отнести к определенным негативным аспектам данного явления), поскольку цифровизация – это давно назревший процесс, нацеленный на автоматизацию управления и формирование системы безопасности, а потому, в частности, цифровизация в сфере пассажирских перевозок определяется как важнейшая стратегическая задача правового обеспечения в данной сфере. Это объясняется необходимостью прозрачности в осуществлении перевозок, недопущения реализации такой деятельности недобросовестными перевозчиками. Соответственно, как замечают исследователи, «в связи с развитием цифровых технологий видится очевидной необходимость изменения правового регулирования» [4. С. 28], прослеживая тенденцию правового эксперимента. В свою очередь важно отметить такую точку зрения, что трансформация правового регулирования в сфере перевозок пассажиров и грузов видится обоснованной не потому, что цифровые технологии развиты, а потому что это требует обеспечения безопасного перевозочного процесса, а цифровые технологии являются средством развития принципа безопасности транспортной деятельности. Тем самым также и устраняются проявления коррупционного характера, поскольку, согласно новому законодательству – Указу Президента Республики Беларусь от 25 января 2024 г. «Об автомобильных перевозках пассажиров», транспортные услуги и операции относительно перевозок пассажиров автомобильным транспортом могут быть выполнены в нерегулярном сообщении только при внесении соответствующих сведений в информационный

ресурс «Реестр автомобильных перевозок пассажиров в нерегулярном сообщении». Тем самым устанавливается новый механизм осуществления перевозок и создаются условия для повышения качества услуг. Отметим, что формирование данного реестра впервые предусматривается в белорусском законодательстве, что на практике, полагаем, повлечет дальнейшие процессы цифровизации в области интеллектуальных транспортных систем. Более того, доступ к Реестру получат и пассажиры, поскольку в него включаются сведения как о самих перевозчиках и водителях, диспетчерах перевозок, так и транспортных средствах.

В Республике Беларусь достаточно актуальным является вопрос о необходимости выработки подхода к систематизации интеллектуальных транспортных систем, в частности, в рамках единого национального оператора, включив платные дороги, весогабаритный контроль, систему фотофиксации нарушений, парковочную систему. И, как обозначил 19 августа 2024 г. глава государства А. Г. Лукашенко, «если уж проводить цифровую трансформацию транспортной инфраструктуры, то самым передовым и удобным для людей способом» [5]. Соответственно, такоие новшества в транспортной сфере находятся еще в стадии проработки в Совете Министров Республики Беларусь с позиции обеспечения государственных интересов. Оптимизация ресурсов при объединении всех интеллектуальных транспортных систем в одну может усилить безопасность в сфере дорожного движения и упростить деятельность с учетом принципа комплексности, а управление в свою очередь будет возложено на эффективно функционирующий единый национальный оператор при соответствующем системном правовом регулировании.

Логичным видится позиция, изложенная в 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» о разработке такого документа, как Концепция взаимодействия интеллектуальных транспортных систем государств – членов ЕАЭС в свете юридического обеспечения цифровизации логистических процессов и на этой основе их упрощения, улучшения взаимодействия.

Так, обоснование существования особого нового вида правоотношений, возникающих в связи с эксплуатацией интеллектуальной транспортной системы как единой комплексной сферы правового регулирования, с определением места в транспортно-правовой науке и подлежащих дальнейшему расширению с определением объектов и субъектов и иных элементов приводилось автором в специальной научной литературе. Сохраняется потребность сформировать направления, развивающие и в том числе систематизирующие основы правового обеспечения данных отношений, включая институциональную среду [6]. Данный подход подтверждается положениями постановления Совета Министров Республики Беларусь от 25 октября 2022 г. № 724 «О порядке функционирования интеллектуальных транспортных систем» (далее – Постановление № 724) относительно применения данных систем на автомобильных дорогах общего пользования и улицах населенных пунктов, что нацелено на повышение эффективности дорожного движения, качество транспортной деятельности. Согласно вышеназванному акту, со-

здание и развитие интеллектуальных транспортных систем разделено на несколько ведомств (Министерство транспорта и коммуникаций Республики Беларусь, местные исполнительные и распорядительные органы, а в отношении обеспечения безопасности и эффективности организации дорожного движения – на Министерство внутренних дел), соответственно, при приведении в систему деятельность данных организаций представляется намного более слаженной и эффективной. Использование интеллектуальных транспортных систем способствует повышению управления транспортной деятельностью, а также при системном правовом обеспечении в рамках цифровой среды – уровень взаимодействия участников дорожного движения.

Сущность и признаки цифровых платформ исследуются в литературе экономико-социологического характера [7. С. 80]. Применительно к оказанию транспортных услуг существенными признаками, с нашей позиции, выступает во-первых, множество участников, в числе которых Министерство транспорта и коммуникаций, которое в своей деятельности направлено на эффективное управление транспортными процессами и качество оказания транспортных услуг, граждане, которым необходимо предоставление транспортных услуг, сочетающих качество, безопасность, комфорт и невысокие финансовые ресурсы при их использовании, а также организации, оказывающие услуги перевозок различными видами транспорта, которые будут включены в Реестр перевозчиков в нерегулярном сообщении на цифровой платформе «Реестр автомобильных перевозок пассажиров» в рамках государственного информационного ресурса; во-вторых, наличие взаимодействия между указанными субъектами, в рамках которого осуществляется процесс обмена информацией в электронном режиме; в-третьих, совокупность принципов, на базе которых данная цифровая платформа получает эффективное действие. При этом обоснованно при включении платформ в систему государственного управления учитывать «цифровую зрелость» социума. Каким образом общество и представители транспортных организаций готовы к работе по новым правилам, можно будет проследить с момента вступления с силу правовых положений. Однако поступающие вопросы и некоторые противоречия обсуждаются на протяжении достаточного времени, чтобы каждый субъект, оказывающий услуги по автомобильной перевозке пассажиров, смог разобраться в правилах и алгоритмах и определил возможности включения в базу данных на цифровой платформе.

Так, создание цифровой платформы при использовании интеллектуальных транспортных систем также оказало бы существенную роль в сборе данных и идентификации участников данной деятельности. На это и нацелено создание Реестра автомобильных перевозок пассажиров в нерегулярном сообщении, что можно считать достижением в области цифрового подхода к регулированию отношений перевозок, реализации положения Директивы Президента Республики Беларусь «О дебюрократизации государственного аппарата и повышении качества обеспечения жизнедеятельности населения» от 27 декабря 2006 г. № 2 с изменениями и дополнениями согласно Указу Президента Республики Беларусь «Об изменении Директивы Президента Республики Беларусь» от 13 июня 2023 г., о масштабном развитии цифровых платформ с целью «выстраивания эффективного взаимодействия и партнерства между государственными органами и гражданами, представителями юридических

лиц, одновременно обеспечивая информационную безопасность». Правы ученые, отмечающие, что «обеспечение информационной безопасности является одним из приоритетов в межгосударственном взаимодействии» [8. С. 317].

Важно отметить, что регулирование отношений в процессе использования цифровых технологий должно быть нацелено на соблюдение интересов и прав личности и государства. Хотя современное общество и характеризуется как цифровое общество, затронем аспекты информационного обеспечения. Обратим внимание на то, что до настоящего времени не сформирован единый подход к правовому регулированию, касающемуся системной цифровизации в сфере транспортной деятельности. Быстрое развитие инновационных подходов требует создания цифровой среды и изменения правового обеспечения при эксплуатации интеллектуальных транспортных систем для хранения данных, их обработки, другими словами, прозрачности, сокращения документооборота при технически сложном взаимодействии в транспортной сфере. Цифровое управление транспортной системой формирует прозрачный юридический механизм осуществления соответствующей деятельности. В то же время в ЕАЭС не указано о цифровизации, хотя нормы об информатизации закреплены. В зарубежной литературе высказывается точка зрения, что цифровизация как процесс предшествует информатизации общества и отражает нынешний этап его развития, а информатизацию необходимо рассматривать как следующий этап во всех сферах, т. е. информатизированное управление на основе цифровых данных [9].

С учетом того, что ЕАЭС, вбирая положительный опыт Союзного государства, реализует инициативы, учитывая сложившийся многолетний опыт добрососедства, отметим, что в рамках Союзного государства сформированы цифровые платформы, что позволяет, например, привлечь к ответственности нарушителей согласно Соглашению между Российской Федерацией и Республикой Беларусь о взаимном признании и исполнении решений по делам об административных правонарушениях в области дорожного движения, ратифицированное Республикой Беларусь от 2 ноября 2023 г. № 51, которое с 13 ноября 2023 г. вступило в силу. Так, принятие вышеназванного Соглашения обусловлено потребностью сближения законодательства двух стран в области обеспечения безопасности дорожного движения. Кроме того, для формирования единого страхового рынка автовладельцев и сближения законодательства в сфере безопасности дорожного движения двух стран 19 июня 2023 г. на шестьдесят четвертой сессии Парламентского собрания принят модельный нормативный акт «О системе обязательного страхования гражданской ответственности владельцев транспортных средств Союзного государства», который направлен на унификацию законодательных систем государств – участников Союзного государства в области транспортной деятельности, что повлекло развитие данного механизма в отношении системы автомобильного страхования применительно к двум странам – участницам Союзного государства. Так, в Российской Федерации подготовлен законопроект, в соответствии с которым действие системы автострахования расширяется на территорию Республики Беларусь, механизм планируется к реализации с 1 октября 2024 г. при сохранении возможности использования электронного документа, что поспособствует упрощению поездок автомобильным транспортом на территорию Республики Беларусь.

Соответственно, развитие цифровизации и систематизации правовых основ, разработка цифровых платформ на базе правового регулирования в совокупности позволяют говорить об информационно-правовом обеспечении в транспортной сфере, что одновременно требует решения вопросов обеспечения информационной безопасности, ведь проблемы киберпреступности все еще сохраняются актуальными. Хотя вопросы новой правовой среды для цифрового развития транспортной деятельности подробно не освещались ранее в учебной и научной литературе по транспортному праву [10, 11], в настоящее время в контексте устойчивого развития и создания благоприятной безопасной среды вызовы цифровизации требуют эффективной реализации принятых решений и в случае успешно разработанных механизмов – новых подходов к уточнению вопросов оказания транспортных услуг. Разработка правовых основ относительно функционирования государственного информационного ресурса автомобильных перевозок в контексте использования новых технологий поспособствует созданию цифрового управления транспортной деятельностью и в перспективе – планированию развития транспортных систем, в том числе интеллектуальных, в цифровом формате.

Заключение. Таким образом, в рамках цифровой трансформации общества существенным преобразованиям подвергается система государственного управления в сфере транспортной деятельности. Прослеживается тенденция оказания государственных услуг в электронном формате посредством информационных реестров, а разработка цифровых платформ служит информационным цифровым инструментом взаимодействия государства, граждан и организаций, оказывающих услуги. Соответственно, приходим к выводу, что цифровизация заключается не только в отдельно взятом реформировании деятельности автомобильных перевозок пассажиров, но и в принципиально новом подходе к обеспечению безопасности цифровыми технологиями на базе правового регулирования [12]. Цифровизация логично формирует новую экономическую и правовую реальность, а именно новый институт в рамках транспортного права, что, полагаем, повлечет расширение доктринальных подходов и эффективных законодательных механизмов. Безусловно, необходимой представляется разработка правовых основ относительно интеллектуальных транспортных систем для систематизации деятельности по их эксплуатации, а в случае особой необходимости – процессов цифровизации в рамках правового обеспечения с учетом баланса национальных и наднациональных интересов.

Список литературы

1. Бажина М. А. Трансформация транспортных отношений в условиях цифровой реальности // Актуальные проблемы гражданского и предпринимательского права: сб. ст. к 70-летию проф. В. С. Белых / отв. ред. В. А. Бублик. М.: Проспект, 2023. С. 57– 66.

2. Сюн В. Магистраль Шелкового пути. Путевые заметки грузовых поездов по маршруту «Китай – Европа». – 2020. – 576 с.

3. 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.

4. Скучаев А. Цифровая реальность пассажирских перевозок // Право и экономика. – 2024. – № 5. – С. 25–30.

5. В Беларуси может появиться национальный оператор интеллектуальных транспортных систем [Электронный ресурс]. – URL: https://belta.by/president/view/v-belarusi-mozhet-pojavitsja-natsionalnyj-operator-intellektualnyh-transportnyh-sistem-655112-2024 (дата обращения: 04.09.2024).

6. Хотько О. А. Правовые проблемы государственного управления в сфере обеспечения транспортной безопасности в контексте эксплуатации интеллектуальных транспортных систем // Совершенствование механизма государственного управления в условиях цифровизации общества и государства: материалы междунар. круглого стола, Респ. Беларусь, Минск, 29 сент. 2023 г. / Белорус. гос. ун-т; редкол.: В. С. Михайловский (гл. ред.), А. В. Шидловский, Н. М. Шевко. – Минск: БГУ, 2023. – С. 196–202. https://elib.bsu.by/bitstream/123456789/303875/1/196-202.pdf

7. Хамутовская С. В. Государственные цифровые платформы как актуальная форма цифровой трансформации государственного управления Республики Беларусь // Социально-политические процессы и явления в современной Республике Беларусь / Е. М. Бабосов и др.; под общ. ред. Е. М. Бабосова; Национальная академия наук Беларуси, Институт социологии. – Минск: Беларуская навука, 2024. – С. 76–97.

8. Макаров О. С., Романовский А. В. Правовое регулирование обеспечения международной информационной безопасности на пространстве ОДКБ // Состояние, проблемы и перспективы развития юридической науки и практики в условиях глобализации общественных отношений: сб. науч. ст. / Гродн. гос. ун-т им. Янки Купалы; редкол.: С. Е. Чебуранова (гл. ред.) [и др.]. Гродно: ГрГУ, 2022. – С. 317–320.

9. Paulin A. Digitalization vs. Innformatization: different Approaches to Governanance Transformation CEE e|Dem and e|Gov Days / A. Paulin. – 2018. P. 251–262.

10. Землин А. И. Актуальные проблемы развития транспортного законодательства и транспортного права России: монография / А. И. Землин, Ю. И. Петров, Ю. А. Харламова. – 2-е изд., перераб. и доп. – М.: Русайнс, 2019. – 191 с.

11. Транспортное право. Общая часть: учебник / отв. ред. Н. А. Духно, А. И. Землин. – М.: Юрид. институт МИИТ, 2017. – 259 с.

12. Бажина М. А. Интеллектуальные транспортные системы – основа de lega ferenda транспортной системы Российской Федерации // Journal of Digital Technologies and Law. – 2023. – № 1(3). – С. 630–649. – EDN: vbowtb. DOI: https://doi.org/10.21202/jdtl.2023.27

В. Е. Чеботарев,
кандидат экономических наук, доцент,
Российский университет транспорта

БЕЗОПАСНОСТЬ БЕСПИЛОТНЫХ ТАКСИ – ТЕХНОЛОГИИ И ПРАВО

Аннотация. В представленной статье раскрывается актуальная проблема обеспечения (технологического и правового) безопасности эксплуатации беспилотного такси как новой современной прорывной цифровой технологии. Анализируются статистические данные, рассматривается проблема привлечения к ответственности за причинение вреда данными транспортными средствами. Приводится критическая оценка основных положений проекта Закона о высокоавтоматизированных транспортных средствах, делаются теоретико-прикладные выводы по результатам исследования.

Ключевые слова: право, цифровые технологии, такси, беспилотное такси, безопасность, риски, ответственность за причинение вреда, высокоавтоматизированное транспортное средство (ВАТС), речное беспилотное такси.

SAFETY OF UNMANNED CABS - TECHNOLOGY AND LAW

Abstract. The presented article reveals the actual problem of ensuring (technological and legal) safety of operation of an unmanned taxi as a new modern breakthrough digital technology. Statistical data are analyzed, the problem of bringing to justice for causing harm by these vehicles is considered. A critical assessment of the main provisions of the draft Law on highly Automated Vehicles is given, theoretical and applied conclusions are drawn based on the results of the study.

Keywords: law, digital technology, cabs, anunmanned cab, security, risks, responsibilities, responsibility for causing harm, river unmanned cab.

Введение. Выбор темы для ее освещения на «полях» международного ежегодного, ставшего уже доброй традицией научного форума на базе Казанского инновационного университета имени В. Г. Тимирясова не случаен.

Исследовательский интерес продиктован как востребованностью в исследованиях аспекта безопасности применительно к развивающемуся беспилотному такси, включая и речное, так и нацеленностью на формирование эффективного правового регулирования [9]. Нельзя не отметить и тот факт, что в последний год на базе Юридического института Российского университета транспорта проводятся самые актуальные исследования транспортного права, и беспилотное такси здесь не только не исключение, но и в центре самого пристального внимания. Так, 1 марта 2024 года в рамках Всероссийского юридического форума «Такси. Курс на право» состоялось торжественное подписание соглашения о сотрудничестве между Юридическим институтом РУТ (МИИТ) и крупнейшей саморегулируемой организацией таксомоторной отрасли – Общественным советом по развитию такси.

Основная часть. Ожидаемый через год массовый выпуск на дороги России беспилотных автомобилей, наряду с ожидаемым вступлением в силу 1 сентября

2025 года разработанного к настоящему моменту проекту Закона о высокоавтоматизированных транспортных средствах (далее – ВАТС) – события, вызывающие ряд опасений, большинство которых взаимоувязывается с проблематикой обеспечения безопасности.

В утвержденной в 2020 году Концепции обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования [3], при перечислении перспективных сфер использования беспилотных и подключенных транспортных средств, а также получаемых от них данных заключено, что в ближайшей и среднесрочной перспективе ожидается активное внедрение в практику перевозок беспилотного такси, сопровождаемое расширением применения бизнес-моделей совместного использования транспортных средств в крупных мегаполисах (каршеринг, райдшеринг).

Примечателен факт, и это отмечается исследователями [5. С. 47], что законодательство большинства стран запрещает использование БТС на дорогах общего пользования, что наблюдается и в законодательстве России (нет разрешения на использование беспилотников на дорогах общего пользования). При этом появляются новые пилотные проекты. Команда Яндекса объявила, что скоро в Москве начнется тестирование сервиса беспилотного такси на живых пассажирах. Такси-беспилотники будут работать в окрестностях ряда станций метро.

Безопасность беспилотного такси мы также связываем, прежде всего, с его безаварийностью, с эксплуатацией в условиях безрисковости для пассажира, для пешехода, для всех участников дорожного движения. Вообще, нередко цифровые технологии связывают с новыми возможностями для обеспечения безопасности дорожного движения [7]. При этом справедливо отмечается, что, «несмотря на тестирование возможностей беспилотного автотранспорта для перевозки грузов, а также испытания тридцати пяти беспилотных автомобилей такси «Яндекса», в современных условиях говорить о массовом внедрении подобного транспорта как в российскую действительность, так и за рубежом пока преждевременно. Основная причина подобного положения – отсутствие необходимой законодательной основы, хотя и сами технологии недостаточны для внедрения в повсеместный процесс передвижения по дорогам общего пользования» [7. С. 52].

Анализ многих открытых для изучения статистических данных (представленных МВД, страховыми кампаниями, ГИБДД Москвы и др.) обнаруживает следующее: за последние пять лет очевидно ежегодное снижение числа ДТП с участием такси, однако аварийность с участием легковых такси всегда кратно (до 7 раз!) превышает аварийность с легковыми автомобилями. С учетом таких данных могут ли беспилотные такси повлиять положительно на такую динамику?

Профессор А. В. Вайпан усматривает «в беспилотном цифровом новшестве… проблемы, которые не решены надлежащим образом, прежде всего в части ответственности и обеспечения безопасности дорожного движения при эксплуатации технологии ВАТС. Например, нет ясности в том, кто будет нести уголовную ответственность в случае причинения тяжкого вреда жизни и здоровью людей при серьезных ДТП, когда транспортным средством полностью управляет искусственный интеллект. Необходимо четкое юридическое определение лица, управляю-

щего автомобилем с искусственным интеллектом, в контексте уголовного законодательства. К тому же следует учитывать, что действующая правовая система не рассматривает искусственный интеллект в качестве субъекта правоотношений» [6. С. 3–6].

Что же касается гражданско-правовой ответственности за вред, причиненный жизни, здоровью, имуществу «третьих лиц, среде», то ее, согласно проекту Закона о высокоавтоматизированных транспортных средствах (ВАТС), будет нести владелец ВАТС, если он не докажет, что вред возник вследствие «непреодолимой силы или умысла потерпевшего». Можно будет переложить ответственность и на производителя автомобиля, если будет доказано, что вред был причинен в связи «с конструктивными особенностями (недостатками) системы управления или ВАТС в целом». Если же авария произошла в связи с «неосуществлением диспетчерского контроля», то ответственность будет лежать на диспетчере (речь идет о сотруднике, который должен будет дистанционно мониторить состояние машины и при необходимости выключать автопилот). Если авария произошла из-за плохого техобслуживания, то ответственность ляжет на дилера.

Тем не менее паспорт федерального проекта «Искусственный интеллект» национальной программы «Цифровая экономика Российской Федерации» прямо определяет, что в качестве одного из показателей будет обеспечена поддержка внедрения ИИ в отраслевые компании, в том числе внедрение следующих юз-кейсов: беспилотные личные, грузовые автомобили, суда, локомотивы, такси и пр. [4].

С 2023 года Федеральная государственная информационная система легковых такси (прежде всего в целях информационного обеспечения создания и функционирования централизованной базы данных перевозчиков легковым такси, легковых такси и служб заказа легкового такси) в своей структуре содержит в том числе подсистему информационной безопасности, которая обеспечивает защиту информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации, законодательством Российской Федерации в области персональных данных [1].

Что касается речного беспилотного такси (не будем фантазировать, насколько близко его появление в России и каковы будут отличия от Нидерландов и Финляндии), то для такого развития пока не созданы все условия. Высказываются мнения, что полностью отказаться от присутствия персонала на борту речных трамваев в Москве невозможно. В отличие от морских судов, которые уже достаточно долго большую часть маршрута проходят в автоматическом режиме, ориентируясь на данные спутниковых систем навигации, данные радиолокационных станций и инерциальных систем (однако при входе в порт или в условиях сложного фарватера судно всегда переходит в ручной режим), в условиях речной навигации, как и при движении в порту, гораздо больше факторов и потенциальных рисков, которые надо учитывать при управлении судном. Причем большинство из них связано с другими участниками движения, а не с условиями плавания.

Заключение. Отметим, что проблема обеспечения безопасности беспилотного такси с учетом наращивания темпов развития этого транспорта будет только набирать свою актуальность.

Список литературы

1. Об утверждении Положения о федеральной государственной информационной системе легковых такси: Постановление Правительства РФ от 24 июля 2023 г. № 1201 // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_453360 (дата обращения: 08.09.2024).

2. Об утверждении стратегического направления в области цифровой трансформации транспортной отрасли Российской Федерации до 2030 года: Распоряжение Правительства Российской Федерации от 3 ноября 2023 г. № 3097-р // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_196819 (дата обращения: 05.09.2024).

3. Об утверждении Концепции обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования: Распоряжение Правительства РФ от 25.03.2020 № 724-р // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_348679 (дата обращения: 05.09.2024).

4. Паспорт федерального проекта «Искусственный интеллект» национальной программы «Цифровая экономика Российской Федерации» (приложение № 3 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 27.08.2020 № 17) // СПС «КонсультантПлюс» [Электронный ресурс]. – https://www.consultant.ru/document/cons_doc_LAW_398627 (дата обращения: 30.08.2024).

5. Благодир А. Л., Михеева И. Е. Лизинг беспилотных транспортных средств: правовое регулирование и практика // Право и экономика. – 2022. – № 12. – С. 47–55.

6. Вайпан В. А. Правовое обеспечение цифровой трансформации транспортного комплекса России // Транспортное право. – 2022. – № 3. – С. 3 - 7.

7. Калюжный Ю. Н. Цифровые технологии как новые возможности обеспечения безопасности дорожного движения // Административное право и процесс. 2021. – № 11. – С. 52–54.

8. Ответят ли роботы за ДТП // Коммерсант. URL: https://www.kommersant.ru/doc/6493016 (дата обращения: 30.08.2024).

9. Бажина М. А. Интеллектуальные транспортные системы – основа de lega ferenda транспортной системы Российской Федерации // Journal of Digital Technologies and Law. – 2023. – № 1(3). – С. 630–649. – EDN: vbowtb. DOI: https://doi.org/10.21202/jdtl.2023.27

DIGITAL FAMILY LAW: ЦИФРОВЫЕ ТЕХНОЛОГИИ В СЕМЕЙНЫХ ПРАВООТНОШЕНИЯХ

Е. А. Селезнева,
кандидат юридических наук, адвокат, управляющий партнер MENSI GROUP, Doctor of Legal Administration НИУ ВШЭ

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ СЕМЕЙНЫХ ПРАВООТНОШЕНИЙ: ПРАВОВЫЕ АСПЕКТЫ И ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Статья посвящена исследованию правовых аспектов и проблем информационной безопасности в контексте цифровой трансформации семейных правоотношений. Анализируется влияние цифровых технологий на традиционные институты семьи и брака, рассматривают процесс цифровизации государственных услуг в сфере регистрации актов гражданского состояния. Особое внимание уделяется вопросам обеспечения баланса между инновационными решениями и сохранением традиционных ценностей, а также проблемам защиты персональных данных граждан в условиях развития цифрового общества. Обсуждаются потенциальные риски, связанные с внедрением цифровых технологий в сферу семейного права, и предлагаются меры по повышению информационной безопасности и цифровой грамотности населения. Подчеркивается необходимость комплексного подхода к цифровой трансформации социальной сферы, учитывающего технологические, правовые и социальные аспекты.

Ключевые слова: цифровая трансформация, семейные правоотношения, информационная безопасность, защита персональных данных, цифровизация государственных услуг, акты гражданского состояния, цифровая грамотность, сетевое общество, правовое регулирование, социальная адаптация

DIGITAL TRANSFORMATION OF FAMILY LAW RELATIONS: LEGAL ASPECTS AND INFORMATION SECURITY ISSUES

Abstract. This article is dedicated to the examination of legal aspects and information security issues in the context of the digital transformation of family law relations. The authors analyze the impact of digital technologies on traditional family and marriage institutions and explore the process of digitizing government services in the area of civil status registration. Special attention is given to ensuring a balance between innovative solutions and the preservation of traditional values, as well as the challenges of protecting citizens' personal data in the context of a developing digital society. The article discusses potential risks associated with the implementation of digital technologies in the field of family law and suggests measures to enhance information security and digital literacy among the population. The authors emphasize the need for a comprehensive approach to the digital transformation of the social sphere, taking into account technological, legal, and social aspects.

Keywords: digital transformation, family law relations, information security, personal data protection, digitization of government services, civil status acts, digital literacy, network society, legal regulation, social adaptation

Введение. В контексте стратегических приоритетов, обозначенных в основополагающих документах Правительства Российской Федерации, касающихся перспектив развития государства до 2024 года [18], особое внимание уделяется процессу цифровой трансформации социальной сферы. Данный процесс, однако, сопряжен с необходимостью имплементации комплексных мер по обеспечению информационной безопасности, что обусловлено потенциальными рисками, связанными с цифровизацией.

Основная часть. Согласно последнему отчету Индекса цифровой конкурентоспособности IMD за 2023 год, Россия занимает 43-е место среди 64 оцениваемых стран. Этот рейтинг оценивает способность и готовность стран к внедрению и исследованию цифровых технологий как ключевого фактора экономических преобразований в бизнесе, правительстве и обществе в целом [1].

Для эффективной модернизации системы социальной защиты и социального обслуживания населения в условиях цифровой трансформации необходима реализация комплекса мер, направленных на оптимизацию и упрощение существующих механизмов. В частности, особое значение приобретает внедрение инновационных электронных технологий в сфере предоставления услуг по реализации прав граждан в семейных правоотношениях. Данные технологии должны обеспечивать уровень качества и доступности, аналогичный услугам, предоставляемым в стационарной форме [26].

Важным аспектом модернизации социальной сферы является развитие системы одного окна, позволяющей гражданам получать широкий спектр услуг в рамках единого интерфейса. Параллельно с этим необходимо осуществлять модернизацию и расширение сети организаций социального обслуживания, внедряя в их деятельность современные технологические решения и методики работы [22].

Следует подчеркнуть, что без реализации вышеуказанных мер невозможно обеспечить эффективное и надлежащее удовлетворение потребностей граждан в контексте современного общества, характеризующегося высокой степенью цифровизации и динамичностью социально-экономических процессов. Таким образом, цифровая трансформация социальной сферы представляет собой не только технологический, но и социальный вызов, требующий комплексного подхода и учета множества факторов для успешной реализации.

Эпидемиологическая ситуация, связанная с распространением коронавирусной инфекции COVID-19, внесла значительные коррективы в нормативно-правовую базу и практику принятия решений государственными органами в сфере семейного права. В частности, произошли существенные изменения в процедуре государственной регистрации заключения брака в торжественной обстановке. Учитывая потенциальные риски распространения инфекции при совместном присутствии большого количества людей, президиум Координационного совета по борьбе с распространением новой коронавирусной инфекции принял решение

о временном приостановлении предоставления государственных услуг по регистрации заключения брака в торжественной обстановке [10].

В результате этих мер наблюдается устойчивая тенденция к увеличению популярности неторжественной регистрации брака в МФЦ и использованию электронных сервисов для подачи заявлений. По данным Управления ЗАГС Москвы, в 2022 году уже более 60 % пар подали заявления на регистрацию брака через портал госуслуг. В первом полугодии 2023 года эта цифра достигла 70 %, что свидетельствует о продолжающемся росте популярности цифровых технологий среди молодоженов при получении данной государственной услуги. Эта статистика наглядно демонстрирует высокий уровень адаптации молодого поколения к использованию цифровых технологий в сфере государственных услуг и подтверждает эффективность реализуемых мер по цифровизации.

За девять лет с момента начала оказания услуг ЗАГС в столичных центрах «Мои документы» москвичи воспользовались ими более трех миллионов раз. Особой популярностью пользуется регистрация брака в неторжественной обстановке. Во флагманских офисах пяти административных округов и в обновленных центрах госуслуг созданы специальные кабинеты с фотозонами для молодоженов.

Для удобства граждан разработан сервис «Наша свадьба» – подробный гид по местам бракосочетания в столице, представляющий более 50 площадок. С его помощью можно выбрать место для торжественной церемонии, используя различные параметры: дату регистрации, близость к метро, стиль интерьера, вместимость и др.

Однако, несмотря на общую тенденцию к цифровизации, наблюдается значительный разрыв в уровне цифровой грамотности между различными возрастными группами населения. Старшее поколение демонстрирует возрастающее понимание необходимости освоения цифровых технологий, однако показатели использования персональных компьютеров и сети Интернет в Российской Федерации остаются существенно ниже по сравнению с европейскими странами [8].

Согласно результатам исследования, проведенного НАФИ в 2022 году, наблюдается значительное повышение уровня цифровой грамотности среди населения Российской Федерации. Анализ данных показывает, что доля граждан с продвинутым уровнем цифровой компетентности увеличилась до 27 %, что на 11 процентных пунктов выше показателя 2021 года.

Одновременно с этим зафиксировано снижение доли населения с начальным уровнем цифровой грамотности на 13 процентных пунктов, составившее 4 % в 2022 году. Исследование также выявило, что 69 % населения обладает базовым уровнем цифровой грамотности, что свидетельствует о сохранении стабильной тенденции в данном сегменте [3].

По данным Росстата за 2022 год, 92,7 % молодых людей в возрасте 15–24 лет являются активными пользователями Интернета, в то время как среди лиц старше 55 лет этот показатель составляет лишь 74,8 %. Анализ пользовательской активности в сети Интернет показывает, что наиболее интенсивными пользователями по-прежнему остаются представители молодежи, что указывает на сохраняющиеся существенные различия в уровне владения электронными технологиями и современными сервисами между различными возрастными группами.

Важно отметить, что за период пандемии COVID-19 наблюдался значительный рост цифровизации среди всех возрастных групп, однако разрыв между поколениями в уровне цифровой грамотности все еще остается заметным.

Данная ситуация создает определенные вызовы для социальной политики государства, требуя разработки и внедрения комплексных программ по повышению цифровой грамотности населения, особенно среди старших возрастных групп. Необходимо также учитывать потенциальные риски социальной изоляции и ограничения доступа к государственным услугам для тех категорий граждан, которые по различным причинам не имеют возможности или навыков использования цифровых технологий.

В современных условиях цифровой трансформации общества наблюдается недостаточный уровень применения населением Российской Федерации комплексных средств защиты информации, эффективных механизмов маршрутизации сетевого трафика в российском сегменте глобальной сети Интернет, а также использования отечественных программных разработок и технологических решений. Данная ситуация обуславливает необходимость имплементации дополнительных мер по обеспечению защиты прав и законных интересов как отдельных граждан, так и государства в целом в динамично развивающемся цифровом пространстве [23].

В рамках реализации стратегии цифровой трансформации к 2024 году планируется достижение качественно нового уровня цифровизации российского общества. Данная стратегия включает в себя следующие ключевые направления:

1. Формирование комплексной системы правового регулирования цифровой экономики, базирующейся на принципах гибкого подхода к нормативно-правовому обеспечению социальной сферы. Это предполагает разработку и внедрение адаптивных механизмов законодательного регулирования, способных оперативно реагировать на изменения в цифровой среде.

2. Интеграция цифровых технологий в гражданский оборот, что подразумевает широкое внедрение электронного документооборота, цифровых подписей и смарт-контрактов в различные сферы гражданско-правовых отношений. Данный процесс направлен на повышение эффективности и прозрачности взаимодействий между субъектами правоотношений.

3. Создание масштабной инфраструктуры для обработки и хранения данных, обладающей глобальным потенциалом. Это включает в себя развитие сети центров обработки данных, внедрение технологий распределенного хранения информации и обеспечение надежной защиты данных от несанкционированного доступа.

4. Имплементация инновационных цифровых технологий и платформенных решений в сфере предоставления государственных услуг, ориентированных на удовлетворение потребностей населения. Данное направление предполагает создание единой цифровой экосистемы государственных сервисов, обеспечивающей удобство и доступность получения услуг для граждан.

5. Оптимизация и стандартизация процессов оказания государственных и муниципальных услуг посредством внедрения унифицированных цифровых платформ и интерфейсов. Это направлено на повышение эффективности деятель-

ности органов государственной власти и местного самоуправления, а также на сокращение временных и финансовых затрат граждан при получении различных видов услуг [4].

Реализация вышеуказанных стратегических направлений призвана обеспечить комплексное развитие цифровой инфраструктуры Российской Федерации, повысить уровень цифровой грамотности населения и создать благоприятные условия для дальнейшего технологического прогресса страны в условиях глобальной цифровой экономики.

В контексте реализации государственной программы цифровизации социальных услуг Министерство юстиции Российской Федерации официально объявило о завершении подготовительного этапа по внедрению инновационных электронных сервисов «Рождение ребенка» и «Утрата близкого человека» [13]. Данные цифровые платформы призваны обеспечить возможность дистанционной регистрации актов гражданского состояния, связанных с рождением и смертью, без необходимости физического присутствия заявителей в органах ЗАГС.

Имплементация вышеуказанных цифровых сервисов является неотъемлемой частью общей стратегии государства по модернизации системы предоставления государственных услуг и отражает глобальную тенденцию к цифровой трансформации социальных процессов. Однако следует отметить, что данная тенденция, несмотря на ее очевидные преимущества в контексте повышения доступности и эффективности государственных услуг, сопряжена с рядом потенциальных рисков и вызовов [5].

В частности, одним из ключевых аспектов, требующих пристального внимания при реализации подобных цифровых инициатив, является обеспечение надлежащего уровня информационной безопасности. Как было неоднократно подчеркнуто в ходе экспертных дискуссий и закреплено в соответствующих нормативно-правовых актах, развитие цифровизации в сфере государственных услуг должно сопровождаться созданием комплексной и надежной системы защиты персональных данных граждан.

Необходимость такого подхода обусловлена тем, что несанкционированный доступ к персональным данным или их утечка могут повлечь за собой широкий спектр негативных последствий как для отдельных индивидов, так и для общества в целом. К потенциальным рискам можно отнести:

1. Нарушение конституционного права граждан на неприкосновенность частной жизни (ст. 23 Конституции РФ).

2. Возможность использования персональных данных в противоправных целях, включая мошенничество и иные виды преступлений.

3. Подрыв доверия граждан к государственным институтам и цифровым сервисам.

4. Потенциальные репутационные и финансовые риски для государства в случае масштабных утечек данных [12].

В связи с этим параллельно с развитием цифровых сервисов необходимо осуществлять комплекс мероприятий по созданию безопасной информационной среды. Данный комплекс мер должен включать в себя:

1. Совершенствование нормативно-правовой базы в области защиты персональных данных и информационной безопасности.

2. Внедрение передовых технологических решений для обеспечения безопасности цифровых платформ и баз данных.

3. Регулярный аудит и мониторинг систем безопасности.

4. Повышение цифровой грамотности населения и сотрудников государственных органов.

5. Развитие механизмов межведомственного взаимодействия в сфере информационной безопасности [2].

Таким образом, реализация проектов по цифровизации государственных услуг, в частности, в сфере регистрации актов гражданского состояния, представляет собой комплексную задачу, требующую сбалансированного подхода к вопросам повышения доступности услуг и обеспечения надлежащего уровня защиты персональных данных граждан.

Одним из ключевых этапов в процессе цифровизации семейно-правовой сферы стало принятие Федерального закона от 31.12.2014 № 517-ФЗ, которым были внесены значительные изменения в существующее законодательство. В частности, данный нормативно-правовой акт ознаменовал введение электронного документооборота в систему ЗАГС, что существенно модернизировало процедуры регистрации актов гражданского состояния [27].

Особого внимания заслуживает трансформация процедуры регистрации брака. Согласно действующему законодательству, юридическим основанием для государственной регистрации заключения брака является совместное заявление лиц, изъявивших желание вступить в брачный союз. Традиционно такое заявление подавалось в органы ЗАГС в письменной форме при личном присутствии обоих заявителей. Однако в результате внедрения цифровых технологий законодатель предусмотрел альтернативный способ подачи заявления – в форме электронного документа посредством Единого портала государственных услуг (ЕПГУ).

При использовании электронной формы подачи заявления каждый из заявителей обязан подписать документ усиленной квалифицированной электронной подписью (УКЭП), что обеспечивает юридическую силу электронного документа, эквивалентную собственноручной подписи на бумажном носителе. Данное нововведение значительно упрощает процедуру подачи заявления, особенно в случаях, когда заявители находятся в разных географических локациях [6].

Следует отметить, что в текущей реализации электронного сервиса подачи заявления на регистрацию брака существуют определенные ограничения. В частности, инициировать процесс может только один из заявителей, заполнив необходимые данные в электронной форме. Второму заявителю предоставляется возможность принять приглашение и осуществить оплату государственной пошлины.

Содержание электронного заявления включает в себя ряд обязательных элементов, а именно: паспортные данные обоих заявителей, номера страхового свидетельства обязательного пенсионного страхования (СНИЛС), а также, в случае если один из заявителей ранее состоял в браке, документальное подтверждение расторжения предыдущего брака. Данный перечень документов соответствует требованиям статьи 26 Федерального закона «Об актах гражданского состояния» от 15.11.1997 № 143-ФЗ (далее – ФЗ № 143) [15].

Инновационным элементом электронной процедуры подачи заявления является автоматизированная система бронирования даты и времени регистрации брака. При выборе желаемых параметров на электронной площадке система осуществляет автоматическое резервирование указанного временного слота. Одновременно с этим второму заявителю направляется электронное приглашение для подтверждения заявления. Важно отметить, что данное приглашение имеет ограниченный срок действия – 24 часа, что обусловлено необходимостью оперативного подтверждения намерений обеих сторон и эффективного управления системой бронирования.

Брачный договор, являясь по своей правовой природе разновидностью гражданско-правовой сделки, теоретически может подпадать под действие норм, регулирующих заключение договоров в электронной форме. В этой связи ряд ученых-правоведов выдвигает гипотезу о возможности применения по аналогии ст. 434 ГК РФ, регламентирующей форму договора, к процедуре заключения брачного договора.

Согласно данной концепции, стороны потенциально могли бы заключить брачный договор в письменной форме посредством обмена электронными документами, например, через электронную почту. Ключевым условием при этом выступает возможность достоверной идентификации отправителя документа второй стороной, намеревающейся заключить брачный договор. В качестве механизма идентификации сторон в научной литературе предлагается использование усиленной квалифицированной электронной подписи, что соответствует положениям Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» [17].

Однако при рассмотрении вопроса о возможности заключения брачного договора в электронной форме необходимо учитывать специфические требования, установленные семейным законодательством. В частности, статья 41 Семейного кодекса Российской Федерации (далее – СК РФ) [24] императивно устанавливает обязательность нотариального удостоверения брачного договора. Данное требование является существенным отличием от общего порядка заключения гражданско-правовых договоров и представляет собой дополнительную гарантию защиты прав и законных интересов сторон брачного договора.

В контексте цифровизации нотариальной деятельности следует отметить, что на территории Российской Федерации уже около восьми лет функционирует Единая информационная система нотариата [19]. Данная система предусматривает обязательную регистрацию каждого удостоверенного брачного договора с присвоением ему уникального идентификационного номера. Имплементация электронного реестра нотариальных действий привела к значительному сокращению количества судебных споров, связанных с договорным режимом имущества супругов, что свидетельствует о повышении правовой определенности в данной сфере.

Тем не менее, несмотря на очевидные преимущества цифровизации, вопрос о возможности полностью электронного заключения брачного договора остается дискуссионным. С одной стороны, развитие цифровых технологий и электронного документооборота создает предпосылки для модернизации процедуры заключения брачного договора. С другой стороны, необходимость обеспечения дополни-

тельных гарантий защиты прав сторон, а также особая значимость брачного договора для регулирования имущественных отношений супругов обусловливают сохранение требования о личном присутствии сторон при нотариальном удостоверении договора.

В перспективе развитие систем удаленной идентификации личности и технологий электронного нотариата может создать условия для полноценного электронного заключения брачных договоров. Однако реализация такой возможности потребует внесения существенных изменений в действующее законодательство, в частности, в СК РФ и Основы законодательства Российской Федерации о нотариате.

В рамках прогрессирующей цифровизации государственного управления и оказания государственных услуг особую актуальность приобретает вопрос о создании Единого регистра населения Российской Федерации. Данная инициатива направлена на оптимизацию процессов предоставления государственных и муниципальных услуг, а также на совершенствование системы статистического учета. Реализация данного проекта предполагает существенные изменения в существующих механизмах фиксации и обработки персональных данных граждан.

Одним из значимых следствий внедрения Единого регистра населения стало изменение порядка внесения информации в основной документ, удостоверяющий личность гражданина Российской Федерации – паспорт. В частности, проставление отметок о регистрации брака и сведений о несовершеннолетних детях в паспорте гражданина РФ приобрело факультативный характер. Теперь, согласно новым правилам, внесение данной информации осуществляется исключительно по волеизъявлению гражданина.

Однако данное нововведение вызывает определенные опасения в научном сообществе. Ряд исследователей в области семейного и гражданского права высказывают обоснованные опасения относительно потенциальных негативных последствий отмены обязательного внесения вышеуказанных сведений в паспорт. В частности, прогнозируется возникновение сложностей при осуществлении сделок с недвижимым имуществом, а также в процессе оформления наследственных прав. Данная проблематика требует дальнейшего тщательного изучения и, возможно, разработки дополнительных механизмов верификации семейного положения граждан при совершении юридически значимых действий.

Несмотря на активное внедрение цифровых технологий в сферу государственных услуг, процедура государственной регистрации актов гражданского состояния, в частности регистрация брака, по-прежнему требует личного присутствия заинтересованных лиц. Данное требование обусловлено необходимостью обеспечения достоверности волеизъявления сторон и соблюдения всех формальностей, предусмотренных законодательством.

В период острой фазы пандемии коронавирусной инфекции (COVID-19) в научных и общественных кругах активизировалась дискуссия о возможности проведения процедуры регистрации брака в дистанционном формате с использованием онлайн-платформ. Предполагалось, что такой формат мог бы обеспечить одновременное виртуальное присутствие обоих заявителей. Однако на текущий момент законодательство Российской Федерации не предусматривает возможности полностью дистанционной регистрации брака [11].

Согласно действующему порядку, каждая запись акта гражданского состояния должна быть лично прочитана и подписана заявителем, а также заверена подписью уполномоченного работника органа ЗАГС и скреплена официальной печатью данного органа. Эта процедура направлена на обеспечение юридической силы и достоверности производимой записи.

По завершении процедуры государственной регистрации брака каждому из супругов выдается на руки свидетельство о государственной регистрации акта гражданского состояния установленного образца. Данный документ является официальным подтверждением факта заключения брака и имеет юридическую силу на всей территории Российской Федерации.

В контексте масштабной цифровой трансформации государственного управления в Российской Федерации особое внимание уделяется модернизации системы регистрации актов гражданского состояния. В ближайшей перспективе планируется полный переход на цифровой формат ведения записей актов гражданского состояния, что ознаменует собой качественно новый этап в развитии данной сферы государственных услуг.

Одним из ключевых аспектов этой трансформации является отказ от использования бумажных свидетельств о заключении и расторжении брака в пользу их электронных аналогов. Данное нововведение призвано повысить эффективность документооборота и минимизировать риски, связанные с утратой или повреждением бумажных носителей информации.

Важным этапом в процессе цифровизации стала масштабная работа по оцифровке архивных записей актов гражданского состояния начиная с 1926 года. По имеющимся данным, в электронный формат переведено около 525 миллионов записей, которые ранее существовали исключительно на бумажных носителях. Этот колоссальный массив информации послужит основой для создания Единого регистра населения на базе Единого государственного реестра записей актов гражданского состояния (ЕГР ЗАГС) [21].

Внедрение цифровых технологий в сферу регистрации актов гражданского состояния призвано значительно упростить и ускорить процесс получения гражданами повторных свидетельств и справок. До недавнего времени эта процедура могла занимать до 30 дней и была жестко привязана к месту совершения юридического действия, что создавало определенные неудобства для граждан. Для получения документа из другого региона требовалось направление письменного запроса, что существенно увеличивало временные затраты.

Существенным прогрессом в этом направлении стала возможность получения повторных свидетельств и справок о заключении и расторжении брака в районных центрах государственных услуг или флагманских офисах, расположенных в непосредственной близости от места проживания граждан. Эта инициатива реализована в рамках концепции «государственные услуги рядом с домом» и направлена на повышение доступности и комфортности получения государственных услуг.

В контексте общей стратегии цифровизации городского хозяйства следует отметить Приказ Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 25.12.2020 № 866/пр, который определяет основ-

ные направления социальной политики в рамках проекта «Умный город». Ключевыми целями данного проекта в социальной сфере являются создание интегрированных сервисов, упрощающих процесс получения социальной поддержки гражданами, особенно представителями социально уязвимых групп населения, а также внедрение систем контроля компетенций [16].

Процесс цифровизации затронул и институт расторжения брака. В случае расторжения брака по взаимному согласию супругов предусмотрена возможность подачи совместного заявления о расторжении брака в электронной форме. При этом законодательство предусматривает различные сценарии подачи такого заявления, учитывающие возможные ограничения в личном присутствии одного из супругов.

В ситуации, когда один из супругов не имеет возможности лично явиться в орган записи актов гражданского состояния или многофункциональный центр предоставления государственных услуг, предусмотрена процедура нотариального удостоверения подписи отсутствующего супруга на совместном заявлении. Однако при подаче заявления через Единый портал государственных услуг необходимость в нотариальном заверении отпадает при условии наличия у заявителя усиленной квалифицированной электронной подписи [7].

Таким образом, процесс цифровизации в сфере регистрации актов гражданского состояния направлен на повышение доступности и эффективности государственных услуг, упрощение административных процедур и создание более комфортных условий для граждан при взаимодействии с государственными органами. Вместе с тем реализация этих инициатив требует тщательной проработки правовых и технических аспектов, обеспечивающих надежность и безопасность обработки персональных данных граждан в цифровой среде.

В рамках модернизации системы предоставления государственных услуг и реализации концепции «электронного правительства» в Российской Федерации законодателем предусмотрен ряд альтернативных способов подачи заявлений и осуществления процессуальных действий в сфере семейного права. Данные нововведения направлены на повышение удобства и доступности соответствующих услуг для граждан, предоставляя им возможность выбора наиболее оптимального способа взаимодействия с государственными органами [25].

Особого внимания заслуживает процесс цифровизации судебного порядка расторжения брака. В контексте развития государственных автоматизированных систем в судах общей юрисдикции и арбитражных судах супруги, в том числе предприниматели, получили возможность реализации своих процессуальных прав в электронной форме. Данное нововведение существенно расширяет спектр доступных процессуальных действий, осуществляемых дистанционно, включая:

1. Подачу искового заявления в электронном виде.
2. Направление возражений и ходатайств посредством электронных систем.
3. Получение актуальной информации о состоянии и движении дел через специализированные информационные порталы.
4. Отслеживание времени судебных заседаний с использованием сети Интернет.
5. Направление апелляционной жалобы в электронной форме [20].

В контексте общей тенденции цифровизации государственных услуг ФЗ № 143 предусматривает возможность подачи заявлений в электронной форме по широкому спектру актов гражданского состояния, включая:

1. Регистрацию рождения.
2. Установление отцовства.
3. Заключение брака.
4. Расторжение брака.
5. Усыновление (удочерение).
6. Регистрацию смерти.

Данные нововведения направлены на оптимизацию процесса взаимодействия граждан с органами записи актов гражданского состояния, сокращение временных затрат на оформление документов и повышение общей эффективности системы регистрации актов гражданского состояния.

Таким образом, процесс цифровизации в сфере семейного права и регистрации актов гражданского состояния характеризуется комплексным подходом, охватывающим как судебные процедуры, так и административные процессы. Эти изменения отражают общую тенденцию к созданию более гибкой и адаптивной системы государственного управления, способной эффективно функционировать в условиях цифровой экономики и отвечать современным запросам общества.

Вместе с тем следует отметить, что внедрение цифровых технологий в сферу семейного права и регистрации актов гражданского состояния требует тщательной проработки вопросов информационной безопасности, защиты персональных данных граждан и обеспечения юридической значимости электронных документов. Эти аспекты остаются предметом активных научных дискуссий и законотворческой деятельности, направленной на создание надежной правовой базы для функционирования цифровых систем в данной области.

Устранение обязательного личного присутствия при государственной регистрации актов гражданского состояния существенно оптимизирует процедуры наследования имущества, заключения повторного брака и усыновления несовершеннолетних. Инициация досудебного этапа усыновления осуществляется путем подачи потенциальным усыновителем заявления в уполномоченный орган опеки и попечительства по месту жительства с целью получения заключения о возможности усыновления. В целях обеспечения конфиденциальности процесса усыновления заявители нередко обращаются в специализированные учреждения, расположенные вне территории их постоянного проживания.

В соответствии с действующим законодательством подача документов для оформления усыновления может осуществляться посредством Единого портала государственных услуг, региональных порталов, официальных сайтов органов опеки и попечительства в информационно-телекоммуникационной сети Интернет, а также через многофункциональные центры предоставления государственных и муниципальных услуг на основании соглашений о взаимодействии с органами опеки и попечительства. Внедрение цифровых технологий в процесс сбора и обработки документации, формирование структурированного электронного банка данных о детях, оставшихся без попечения родителей, способствует интенсификации процедуры усыновления и повышению эффективности реализации прав детей на семейное воспитание.

В сфере регистрации рождения детей, рожденных с применением технологии суррогатного материнства, произошли существенные законодательные изменения. Согласно положениям СК РФ, лица, давшие согласие на имплантацию эмбриона суррогатной матери, могут быть зарегистрированы в качестве родителей только при наличии согласия женщины, выносившей и родившей ребенка. В настоящее время судебная практика требует учета наличия договора о суррогатном материнстве, причин отказа суррогатной матери в даче согласия на регистрацию биологических родителей, а также иных обстоятельств, имеющих юридическое значение.

Процедура регистрации рождения ребенка, рожденного суррогатной матерью, предусматривает возможность обращения биологических родителей (или одного из них) в органы записи актов гражданского состояния по месту рождения ребенка или месту жительства одного из биологических родителей, многофункциональные центры предоставления государственных и муниципальных услуг, а также подачи заявления в электронной форме через Единый портал государственных услуг. При этом необходимо предоставление следующих документов: медицинского свидетельства о рождении, документа медицинской организации, подтверждающего согласие суррогатной матери, и паспорта биологического родителя.

Анализ данных мониторинга экономического положения населения, проводимого Высшей школой экономики совместно с другими научными организациями, показывает, что в 2018 году алименты как один из источников дохода указали представители 2,8 % домохозяйств. Учитывая, что по результатам переписи 2020 года в России насчитывалось около 66 миллионов домохозяйств, можно сделать вывод, что алиментные выплаты получают примерно 1,9 миллиона семей.

Согласно исследованиям Высшей школы экономики, ежемесячные алиментные выплаты варьируются в диапазоне от 1 до 80 тысяч рублей, при этом средняя сумма алиментов составляет 10,1 тысячи рублей.

Статистика Федеральной службы судебных приставов свидетельствует о том, что в 2022 году в ведомстве находилось 1,6 миллиона судебных решений о взыскании алиментов на общую сумму 233 миллиона рублей. Наблюдается тенденция к увеличению количества неплательщиков и росту средней суммы долга: если в 2017 году она составляла 114 тысяч рублей, то к 2022 году достигла 146,2 тысячи рублей [9].

Демографический анализ показывает, что большинство должников по алиментам (90,5 %) составляют мужчины. Среднестатистический неплательщик алиментов – это лицо в возрасте от 30 до 42 лет с задолженностью в среднем 226 тысяч рублей.

Заключение. В результате проведенного исследования можно сделать вывод, что цифровая трансформация семейных правоотношений является неотъемлемой частью общего процесса цифровизации общества и государственного управления. Внедрение цифровых технологий в сферу семейного права и регистрации актов гражданского состояния открывает новые возможности для повышения эффективности и доступности государственных услуг, упрощения административных процедур и улучшения качества обслуживания граждан. Однако этот процесс сопряжен с рядом вызовов и рисков, требующих тщательного анализа

и проработки. Ключевыми проблемами остаются обеспечение информационной безопасности, защита персональных данных граждан и сохранение баланса между инновационными решениями и традиционными семейными ценностями.

Для успешной реализации цифровой трансформации в сфере семейных правоотношений необходим комплексный подход, включающий:

1. Совершенствование нормативно-правовой базы для регулирования цифровых аспектов семейного права.

2. Разработку и внедрение надежных технических решений для обеспечения безопасности и конфиденциальности персональных данных.

3. Повышение цифровой грамотности населения и специалистов, работающих в сфере семейного права.

4. Создание механизмов социальной адаптации для граждан, испытывающих трудности с использованием цифровых технологий.

5. Постоянный мониторинг и оценку влияния цифровизации на институт семьи и брака.

Таким образом, цифровая трансформация семейных правоотношений представляет собой сложный и многогранный процесс, требующий взвешенного подхода и учета интересов всех заинтересованных сторон. При грамотной реализации этот процесс может способствовать модернизации системы семейного права, повышению ее эффективности и адаптации к реалиям современного цифрового общества.

Список литературы

1. IMD World Digital Competitiveness Ranking 2023: [сайт]. – URL: https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness (дата обращения: 11.08.2024).

2. Алиева Э. Цифровизация и безопасность // Научные труды Северо-Западного института управления РАНХиГС. – 2019. – Т. 10, № 3(40). – С. 84–87.

3. В России выросла доля людей с продвинутым уровнем цифровой грамотности: [сайт]. – URL: https://nafi.ru/analytics/v-rossii-vyrosla-dolya-lyudey-s-prodvinutym-urovnem-tsifrovoy-gramotnosti (дата обращения: 11.08.2024).

4. Виклушкина О. А. Цифровизация государственных и муниципальных услуг // Информационная среда в современной России: риски и возможности: материалы Международной научно-практической конференции, Барнаул, 19 марта 2020 года. – Барнаул: Азбука, 2020. – С. 4–7.

5. Ельденев А. Т. Тенденции цифровой трансформации государственных услуг // Интеграция и совершенствование цифровой среды социально-экономического пространства в условиях многополярного мира, Москва, 15 января 2024 года. – Москва: Образовательная автономная некоммерческая организация высшего образования «Институт образовательных технологий и гуманитарных наук», 2024. – С. 77–80.

6. Ерисова А. Д. Тенденции использования электронной подписи / А. Д. Ерисова, А. Е. Васильева // Актуальные аспекты и приоритетные направления развития транспортной отрасли: материалы Молодежного научного форума студентов и аспирантов транспортных вузов с международным участием, Санкт-Петербург, 14–15 ноября 2019 года. – Москва: Перо, 2019. – С. 169–172.

7. Зайков Д. Е. Недостатки правовой регламентации института услуг правового и технического характера, оказываемых нотариусами // Законодательство. – 2019. – № 7. – С. 34–40.

8. Инновационное развитие государства и права в цифровую эпоху: сборник научных трудов XXII Международной научной конференции. Сер. «Муромцевские чтения» / под ред. Н. И. Архиповой, С. В. Тимофеева, О. Н. Васильевой. – Москва, 2022.

9. Итоговый доклад о результатах деятельности ФССП России в 2022 году: [сайт]. – URL: https://fssp.gov.ru/deals/otchet_doklad_9/2837777 (дата обращения: 11.08.2024).

10. Координационный совет при Правительстве Российской Федерации по борьбе с распространением новой коронавирусной инфекции на территории Российской Федерации: [сайт]. – URL: http://government.ru/department/554/events (дата обращения: 11.08.2024).

11. Краснов И. И. Актуальные вопросы регистрации брака: помолвка и цифровизация / И. И. Краснов, Н. В. Ющенко // Теоретическая и прикладная юриспруденция. – 2023. – № 3(17). – С. 70–77. – DOI: 10.22394/2686-7834-2023-3-70-77

12. Никифоров А. О. Проблема защиты приватности в цифровом обществе // Вопросы медиабизнеса. – 2024. – Т. 3, № 1. – С. 69–74. – DOI: 10.24412/3034-1930-2024-0090

13. Николаева О. А. Инновационные аспекты в деятельности органов записи актов гражданского состояния // Мировая наука. – 2022. – № 3(60). – URL: https://cyberleninka.ru/article/n/innovatsionnye-aspekty-v-deyatelnosti-organov-zapisi-aktov-grazhdanskogo-sostoyaniya (дата обращения: 11.08.2024).

14. О внесении изменений в Федеральный закон «Об актах гражданского состояния»: Федеральный закон от 31.12.2014 № 517-ФЗ (ред. от 29.12.2017). – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный.

15. Об актах гражданского состояния: Федеральный закон от 15.11.1997 № 143-ФЗ (ред. от 08.08.2024). – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный.

16. Об утверждении Концепции проекта цифровизации городского хозяйства «Умный город»: Приказ Минстроя России от 25.12.2020 № 866/пр. – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный.

17. Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 04.08.2023). – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный.

18. Основные направления деятельности Правительства Российской Федерации на период до 2024 года: утв. Правительством РФ 29.09.2018 № 8028п-П13. – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

19. Основы законодательства Российской Федерации о нотариате: утв. ВС РФ 11.02.1993 № 4462-1 (ред. от 08.08.2024). – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный.

20. Павлюк Ю. Б. Особенности развития цифровых технологий в российском судопроизводстве // Современное право. – 2020. – № 5. – С. 60–66. – DOI: 10.25799/NI.2020.34.53.014

21. Рослова В. А. Электронная регистрация актов гражданского состояния в документах и процедурах // Гуманитарный акцент. – 2019. – № 4. – С. 49–52.

22. Садыков Р. М. Социальное обслуживание населения в условиях его модернизации: теоретические аспекты / Р. М. Садыков, Н. Л. Большакова, Р. Х. Хамадеева // Вестник университета. – 2021. – № 3. – С. 156–161. – DOI: 10.26425/1816-4277-2021-3-156-161

23. Сайгитмагомедова Х. С. Теоретические основы защиты информации в сети Интернет // Государственная служба и кадры. – 2023. – № 1. – С. 17–18. – DOI: 10.56539/23120444_2023_1_17

24. Семейный кодекс Российской Федерации: Федеральный закон от 29.12.1995 № 223-ФЗ (ред. от 31.07.2023). – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный.

25. Слесарева А. М. Необходимость внедрения и совершенствования предоставления электронных государственных услуг // Грядущим поколениям завещаем: творить добро в защиту права: материалы Всероссийской научно-практической конференции студентов с международным участием, Оренбург, 23–24 марта 2022 года / под ред. Е. В. Ерохина. – Оренбург: типография «Агентство Пресса», 2022. – С. 375–381.

26. Тимонина И. В. О применении цифровых технологий в реализации прав граждан на социальное обслуживание // Искусственный интеллект и тренды цифровизации: техногенный прорыв как вызов праву: материалы Третьего Международного транспортно-правового форума, Москва, 10–11 февраля 2021 года. – Москва: Российский университет транспорта, 2021. – С. 445–453.

А. Е. Тарасова,
кандидат юридических наук, доцент,
эксперт рабочей группы «Ребенок и его право на семью»
Координационного совета при Правительстве РФ
по проведению в РФ Десятилетия детства

SMART-РОДИТЕЛЬСТВО: ВЛИЯНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА СЕМЬЮ КАК МЕГАТЕНДЕНЦИЯ 30-ЛЕТИЯ МЕЖДУНАРОДНОГО ГОДА СЕМЬИ

Аннотация. Целью исследования является рассмотрение влияния на функционирование и благополучие семей в XXI веке такой мегатенденции, как развитие технологий. Мегатенденции и их влияние на институт семьи определены в документах, подготовленных органами ООН и приуроченных к празднованию в 2024 году 30-летия Международного года семьи. Особенностью статьи выступает предложение концепции smart-родительства в аспекте развития цифровых технологий, проникающих в детско-родительские отношения с учетом необходимости формирования новых родительских компетенций, учитывающих пользу и вред диджитализации семейных отношений.

Ключевые слова: развитие технологий, мегатенденции, благополучие семьи, международный год семьи, право на участие в играх

SMART-PARENTHOOD: THE IMPACT OF DIGITAL TECHNOLOGY ON THE FAMILY AS A MEGATREND ON THE 30TH ANNIVERSARY OF THE INTERNATIONAL YEAR OF THE FAMILY

Abstract. The purpose of the study is to consider the impact on the functioning and well-being of families in the 21st century of such megatrends as the development of technology. Megatrends and their impact on the institution of the family are defined in the documents prepared by UN bodies and timed to coincide with the celebration of the 30th anniversary of the International Year of the Family in 2024. The peculiarity of the article is to propose the concept of smart-parenting in the aspect of digital technology development penetrating into child-parent relations, taking into account the need to form new parental competencies that take into account the benefits and harms of digitalisation of family relations.

Keywords: technology development, megatrends, family well-being, international year of the family, right to play games

Введение. В 2024 году отмечается 30-летие со дня учреждения Международного года семьи. Указанной дате посвящена серия международных документов, принятых в рамках универсальной международной организации – Организации Объединенных Наций, среди которых подготовительные резолюции Генеральной Ассамблеи ООН [5–7], а также тематические доклады Генерального секретаря ООН. В частности, в Докладе ГС ООН «Реализация целей Международного года семьи и связанных с ним последующих процессов» проводится анализ влияния новых технологий на семьи, уделяется особое внимание потенциалу цифровых технологий в плане содействия достижению баланса между работой и семейной жизнью и роли таких технологий в популяризации просвещения родителей и содействии ему [12].

На универсальном уровне выделены следующие мегатенденции, оказывающие влияние на функционирование и благополучие семьи:

– развитие технологий,
– урбанизация и миграция,
– демография,
– изменение климата.

Сформирован перечень рекомендаций, которые могут быть восприняты государствами на национальном уровне и включены в государственную семейную и социальную политику:

– улучшить доступ к Интернету, более высокоскоростному Интернету и цифровым устройствам для семей, особенно семей, находящихся в уязвимом положении, и инвестировать в развитие навыков цифровой грамотности членов семьи;

– способствовать обеспечению баланса между работой и семейной жизнью в условиях распространения цифровых технологий в мире, предоставлять работникам с семейными обязанностями возможность работать по гибкому графику, чтобы они могли удовлетворять потребности рабочего и семейного характера, и инвестировать в надежную технологическую поддержку и обучение;

– расширять деятельность по научно обоснованному исследованию последствий использования новых технологий для семей, баланса между работой и се-

мейной жизнью и разработки, предоставления и внедрения программ просвещения родителей с интеграцией технологий для подготовки надлежащей политики в отношении поддержки работников с семейными обязанностями.

Развитие технологий воздействует на формирование универсальных принципов и рекомендаций в аспекте семьи, служит новым вызовом для национальных политик государств (публично-правовой аспект), затрагивает права и свободы всех членов семьи, влияет на родителей и детей, а также на детско-родительские отношения (частноправовой аспект).

Основная часть. Особым направлением изучения развития технологий, в частности цифровых, выступает проведение на международном и национальном уровне дальнейших научных исследований последствий использования новых технологий для семей.

Следует дифференцированно подходить к изучению влияния цифровых технологий на детей, родителей, детско-родительские отношения.

Персональные цифровые устройства и Интернет становятся частью жизни детей уже несколько десятилетий, в то время как Конвенция ООН о правах ребенка, 1989 года отмечает свое 35-летие и не содержит положений ни о цифровых правах, ни об Интернете.

Влияние технологий на детей

Технологии оказывают влияние на все сферы жизнедеятельности ребенка: физическое развитие, познание и обучение, социальное и эмоциональное развитие. Выделяют следующие возрастные циклы, соответствующие этапам развития ребенка: раннее детство (от рождения до 5 лет), среднее детство (5–12 лет), подростковый возраст (13–18 лет) и формирующаяся взрослая жизнь (19–25 лет), что поддерживает перспективу жизненного цикла родительского воспитания. Циклы отражают дифференцированное воздействие в зависимости от ребенка (например, восприимчивость, индивидуальность, состояние здоровья); контекста использования; типа устройства или цифрового приложения; степени воздействия; качества взаимодействия и возможного вытеснения полезных занятий (т. е. того, что ребенок не делает во время использования технологий) [9].

23 сентября на площадке Общественной палаты РФ по инициативе Уполномоченного при Президенте РФ по правам ребенка прошла презентация результатов социологического исследования на тему «Изучение поведения детей и подростков РФ в контексте ведения безопасного образа жизни». По данным указанного исследования, 98,6 % подростков ежедневно пользуются Интернетом и социальными сетями. При этом 63,7 % детей скрывают то, что они делают в Интернете с помощью: 51,8 % – VPN-сервисов; 26 % – режима инкогнито; 24,4 % – очистки истории браузера; 13 % – фейковых аккаунтов; 2,9 % – децентрализованных браузеров [12].

Наблюдается довольно смелая стратегия размещения подростками информации в Интернете, отсутствие боязни делиться личными данными в Сети. Из опрошенных в рамках исследования респондентов (35 000 подростков из 89 регионов России): 56 % размещают личные повседневные фотографии себя и родственников; 35,5 % – фото из окон дома; 27,2 % – адрес проживания; 17,5 % – фото и данные документов; 8,2 % – данные банковских карт; 4 % –интимные фото [12].

Разделение возрастных групп детей и подростков для более глубокого и специфического анализа влияния цифровых технологий и Интернета (в том числе в семейных отношениях), а также для выработки правовых и технических решений безопасности является более оправданным подходом, нежели имеющиеся в гражданском и семейном законодательстве РФ возрастные рамки, например, выделение групп малолетних до 6 лет и от 6 до 14 лет, несовершеннолетних с 14 до 18 лет (для регулирования имущественных отношений и разделения института опеки и попечительства над ребенком), или определение возрастного порога в 10 лет для обязательного или факультативного учета мнения ребенка по вопросам, затрагивающим его в семейных отношениях.

Степень беспокойства по поводу воздействия цифровых технологий на ребенка связана со способностью ребенка к самообслуживанию и принятию решений, чтобы справиться с потенциальными угрозами, исходящими от Интернета. Это влияет и на возможные принимаемые меры как со стороны родителей, так и государства в части регулирования пределов использования цифровых технологий и Интернета детьми и доступа к новым технологиям (примеры – Китай, РФ).

Исследователи предлагают выработать и внедрить необходимые рекомендации, обязывающие промышленный сектор и бизнес-компании принимать меры по разработке, распространению и сбору данных о широком использовании технологий, способствующих развитию детей.

При этом важно продолжать проводить исследования влияния технологий, которое не всегда является предсказуемым и положительным, учитывая, что интенсивное развитие технологий не обеспечено достаточным количеством завершенных исследований.

В частности, интересным представляется Доклад консультативного комитета Совета по правам человека ООН, включающий проблемные вопросы защиты прав ребенка в аспекте влияния нейротехнологий в цифровой среде [1]. В докладе отмечается, что комплексное описание воздействия нейротехнологий на права детей отсутствует. Однако остающиеся неизвестными последствия и риски не мешают продвижению на потребительском рынке наушников или надеваемых на голову повязок для детей и молодых людей с целью улучшения их концентрации или способности к обучению [14].

Степень влияния устройств «нейрогейминга» на когнитивное развитие детей и их долгосрочное психическое здоровье остается в значительной степени неизвестной. Эксперты обращают внимание, что в ближайшие годы широкое распространение получат используемые для видеоигр интерфейсы «мозг – компьютер», что подвергнет юных пользователей непредсказуемому воздействию и, возможно, нанесет им стойкий психический или психологический вред [1].

При использовании коммерческих нейротехнологий дети могут дополнительно подвергаться воздействию методов «нейромаркетинга», которые направлены на приоритизацию коммерческих интересов над интересами ребенка и поэтому могут быть чрезвычайно манипулятивными [3].

Соответственно, проблема противоречия между коммерческими интересами цифровой отрасли и наилучшими интересами ребенка выходит на первый план.

Важными направлениями для национальной политики государств и контроля со стороны родителей становятся образование, сфера развлечений и игр, входящие в фокус внимания как наиболее подверженные развитию новых технологий и к которым дети получают непосредственный доступ.

При разработке образовательных инструментов приоритет должен отдаваться психическому здоровью и благополучию детей, а также обеспечению их прав. Устройства, которые распространяются в образовании для контроля за концентрацией внимания и вовлеченностью, могут представлять угрозу для неприкосновенности детей и создавать условия для осуществления психического и физического насилия [11].

На международном уровне отмечаются следующие важные сферы регулирования в аспекте развития технологий, в которых необходимо определять наилучшие интересы ребенка: игровые решения, созданные с использованием нейротехнологий, реклама и маркетинг, ориентированные на детей и к которым дети имеют доступ.

Принципиальным решением становится и защита самих законных представителей (родителей) от заблуждения и манипуляций относительно полезности цифровых решений. Поскольку последствия использования новых технологий могут быть не вполне понятны детям и лицам, осуществляющим за ними уход, вопросы, связанные с предоставлением информированного согласия, обеспечением неприкосновенности частной жизни и самостоятельности, не менее актуальны. Некоторые родители могут впасть в заблуждение, полагая, что определенные нейротехнологии могут улучшить интеллектуальные способности их детей, и настоять на использовании нейротехнологических продуктов, несмотря на существующие риски [1].

Риски, связанные с использованием Интернета и цифровых технологий в образовании, нашли отражение в двух международных докладах ЮНЕСКО [10, 13], выводы из которых также могут быть полезны государствам в части создания взвешенного подхода к использованию онлайн-образования для детей, а законным представителям детей – для выбора формы образования и контроля за использованием цифровых технологий.

Влияние цифровых технологий на родителей

Цифровые технологии открывают перед родителями множество возможностей. Для многих родителей сегодня более тесное общение с ребенком является основной причиной приобретения мобильного телефона для детей младшего возраста (11 лет и младше). С помощью текстовых сообщений, голосовых и видеозвонков родители могут общаться со своими детьми, координировать действия и оставаться рядом. Эффективность использования ИКТ для общения облегчает отношения между родителями, например, в случае развода родителей, и поддерживает связь между родителями и детьми во время разлуки [9].

Формируется цифровая родительская среда, в которой родители активно обмениваются информацией, своими проблемами, получают новые знания, доступ к семейно ориентированным услугам. Цифровые технологии предлагают родителям новые ресурсы для сбора информации (например, поисковые инструменты, дискуссионные форумы, приложения, веб-страницы) и ресурсы социальной поддержки с помощью средств коммуникации и средства массовой информации. Цифровые ре-

шения и доступ к источникам информации, взаимодействия с родительскими сообществами и семейными (детскими) учреждениями в цифровой среде могут помочь подтвердить обеспокоенность родителей, укрепить их уверенность в родительской роли и определить необходимые ресурсы для решения возникающих проблем. По мнению исследователей в области института семьи, цифровые решения позволяют укреплять социальный капитал родителей в социальных сетях – связях, сформированных в отношениях на основе доверия и взаимной помощи, а также расширять размер (количество членов) сетей, предоставляя родителям более широкий доступ к потоку информации и людям, к которым можно обратиться за помощью.

В экспертных исследования в рамках подготовки к 30-летию Международного года семьи, приводятся данные относительно мнения родителей о вреде цифровых технологиях и Интернете в разных странах. В частности, как правило, подавляющее большинство родителей (98 %) считают своей обязанностью защиту детей от онлайн-контента, более половины родителей (от 60–70 %) обычно полагают, что широкое использование смартфонов может быть вредно для социально-эмоционального развития их детей, дети могут столкнуться с сетевыми мошенниками, с сексуально откровенным контентом или с информацией насильственного содержания. Такие данные свидетельствуют о высоком пороге беспокойства родителей о цифровой безопасности детей и последствиях использования ими Интернета и цифровых технологий.

Ограничения (пределы) использования ребенком новых технологий и smart-навыки родителей

Использование детьми технологий, их безопасность и позитивное вовлечение – относительно новая область для родительского воспитания.

В настоящее время выделяют несколько видов возможных к использованию методов контроля за цифровой активностью детей и обеспечения безопасного доступа, которые как связаны с технической стороной вопроса, так и касаются более ответственного и внимательного отношения самих законных представителей к жизни своих детей, в том числе в социальной цифровой среде.

Ограничения могут быть:

– техническими (ограничение использования оборудования или программного обеспечения, включая изъятие техники в качестве наказания);

– мониторинговыми (отслеживание использования, сообщений и местоположения ребенка);

– активным посредничеством (беседы с детьми об использовании технологий, о содержании контента, доверительное взаимодействие в случае негативного опыта использования Интернета и цифровых технологий).

Особо необходимо обратить внимание на уникальное право, которое принадлежит только детям и закреплено в универсальной международной Конвенции ООН о правах ребенка – право детей на участие в играх (ст. 31 Конвенции ООН о правах ребенка). Данное право, закрепленное в международном договоре, в котором не содержится ни одного положения об Интернете и цифровых технологиях, в цифровой век приобретает двойное значение: как благо для детей и как бремя и риск для их родителей.

Родительские ограничения на использование детьми технологий в значительной степени зависят от возраста и зрелости ребенка.

С одной стороны, родители посредничают через взаимодействие и беседы о влиянии медиа. Совместный просмотр или совместное участие (например, в играх) позволяют родителям активно посредничать и контролировать воздействие медиа на детей, а также моделировать здоровое использование технологий. Любопытно, что специализированные исследования различают и факторы, которые могут варьировать подходы родителей к посредничеству. В частности, выделяют роль более авторитетного и более продвинутого в использовании технологий родителя, проводят различия в зависимости от роли матери или отца в использовании цифровых технологий в семье, уровень доходов и технологической цифровой грамотности родителей и иных членов семьи, кто может выполнять ключевую взаимодействующую с ребенком роль.

Smart-родительство в условиях цифровых технологий. Развитие концепции smart-родительства и использование цифровых технологий как неотъемлемый элемент родительства (родительских компетенций) обеспечивает новые перспективы для целого ряда отношений, в которые вовлечена семья и/или члены семьи как активные участники, в частности:

– международные семейные отношения (особенно в период изменения принципа взаимности, применения различного рода реторсий и санкционных режимов, расторжения государствами договоров о правовой помощи по гражданским и семейным делам, вовлечения государств и частных лиц в различного рода конфликты, включая вооруженные, и действие ограничительных мер, влияющих на частные и публичные отношения в государствах);

– поддержание общения между родителями и детьми при раздельном проживании (особенно актуально в связи с различными ограничительными режимами как правового, так и чрезвычайного характера: пандемией, локдауном, вооруженными конфликтами, санкционным воздействием и др.);

– получение информации о родительстве (цифровая семейная инфраструктура и семейные сервисы);

– цифровая занятость и семейные обязанности (формирование гибких условий труда для лиц с семейными обязанностями);

– межпоколенческая солидарность (просвещение родителей, бабушек и дедушек, вовлечение в цифровое посредничество и взаимодействие с ребенком, создание дружественной, доверительной и при этом технологически развитой для ребенка цифровой семейной среды);

– контроль за ребенком (выполнение родительских обязанностей с учетом развития цифровых технологий, недопущение цифровой безнадзорности несовершеннолетних);

– цифровая безопасность ребенка (совместные усилия государственного, негосударственного и семейного сектора для обеспечения безопасности технологий и цифрового контента);

– реализация права ребенка на игру с учетом развития технологий (соблюдение принципа развивающихся способностей ребенка, полноценного участия в новых направлениях, таких как киберспорт и технологическое моделирование, включая приобретение детьми и развитие навыков для профессий будущего).

Рекомендации для формирования smart-родительства. В качестве общих рекомендаций для развития smart-родительства в прикладном значении необходимо акцентировать внимание на таких аспектах, которые требуют принятия

правовых, организационных, инфраструктурных мер в сфере регулирования как частноправовых семейных отношений, так и иных видов общественных отношений, связанных с семьей, в фокусе внимания на:

– образование родителей, повышающее их компетенции в условиях развития цифровых технологий;

– введение и применение гибких условий (графика) работы, включая цифровые форматы занятости для родителей с семейными обязанностями;

– использование цифровых семейно ориентированных услуг, создание семейных многофункциональных центров и цифровой семейной инфраструктуры с позитивным контентом для родителей и детей (семейно ориентированная защищенная цифровая среда);

– применение технологий, в качестве эффективной превентивной стратегии, направленной на борьбу с кибербуллингом и насилием над детьми в цифровой среде и на сокращение масштабов детской безнадзорности, которая из офлайн-среды трансформируется в онлайн-среду («цифровая детская безнадзорность»).

Перспективные сферы для развития digital family law. В связи с интенсивным проникновением цифровых технологий в семейные отношения и отношения более широкого порядка, связанные с обеспечением функционирования и благополучия института семьи, следует выделить перспективные для развития digital family law области применения цифровых технологий для реализации успешных практик регулирования семейных отношений, разрешения внутрисемейных конфликтов, обеспечения прав членов семьи.

К указанным сферам, где востребованы инструменты цифровых технологий, можно отнести:

– внутренние (национальные) споры о воспитании детей;

– трансграничные споры о воспитании детей (споры об определении права опеки и права доступа, о расторжении брака и взыскании содержания на ребенка, споры о возвращении ребенка, похищенного одним из родителей, и др.);

– семейная медиация;

– формирование и содержательное наполнение концепции ответственного родительства (ответственность родителей за цифровую безопасность ребенка и защиту от негативной информации в Интернете).

Заключение

Пример цифровой гигиены как smart-навык родителей. На законодательном уровне государств могут приниматься довольно интересные решения, формирующие новые цифровые компетенции и ответственность родителей в связи с развитием новых технологий.

В РФ в 2020 году был принят Закон о поправке к Конституции [2], которым усилены государственные приоритеты в сфере защиты семьи и детства, и расширены полномочия субъектов РФ по предметам совместного ведения с РФ в вопросах защиты семьи, материнства, отцовства и детства; защиты института брака как союза мужчины и женщины; создания условий для достойного воспитания детей в семье (п. ж. 1 части 1 ст. 72 Конституции РФ).

Удачным примером формирования smart-родительства и наполнения этой концепции новым содержанием с учетом конституционных приоритетов высту-

пает региональный закон Республики Саха (Якутия) об ответственном родительстве и поправки к этому закону, внесенные в 2020 г., вступившие в силу в 2021 г., касающиеся цифровой гигиены как обязанности родителей.

Закон Республики Саха (Якутия) от 14 марта 2016 г. 1604-З № 737-V «Об ответственном родительстве» (с изменениями, вступившими в силу в 2021 г.) в ст. 7 «Обязанности родителей по сохранению здоровья ребенка» закрепил следующие положения в п. 4: «*Родители обязаны принимать меры по защите ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию, в том числе от национальной, классовой, социальной нетерпимости, от рекламы алкогольной продукции, табачной продукции или никотинсодержащей продукции, от пропаганды социального, расового, национального и религиозного неравенства, от информации порнографического характера, от информации, пропагандирующей нетрадиционные сексуальные отношения, размещаемой в сети Интернет и средствах массовой информации или распространяемых иным способом, а также от распространения печатной продукции, аудио- и видеопродукции, пропагандирующей насилие и жестокость, наркоманию, токсикоманию, антиобщественное поведение*».

Формирование навыков smart-родительства отвечает и национальным целям развития РФ [8].

К национальным целям развития РФ на период до 2030 года и на перспективу до 2036 года отнесены:

– сохранение населения, укрепление здоровья и повышение благополучия людей, поддержка семьи;

– реализация потенциала каждого человека, развитие его талантов, воспитание патриотичной и социально ответственной личности;

– комфортная и безопасная среда для жизни;

– экологическое благополучие;

– устойчивая и динамичная экономика;

– технологическое лидерство;

– цифровая трансформация государственного и муниципального управления, экономики и социальной сферы.

Все, что было отмечено в настоящем исследовании как перспективные направления развития концепции smart-родительства, можно отнести практически к каждой из национальных целей, поскольку семья выполняет несколько значимых функций: воспитательную, социальную, экономическую, демографическую, духовно-нравственного развития и общения, защитную (функцию безопасности).

Список литературы

1. Доклад Консультативного комитета Совета по правам человека «Воздействие, возможности и проблемы применения нейротехнологии в отношении поощрения и защиты всех прав человека» от 08.08.2024 № A/HRC/57/61 // Официальный сайт ООН [Электронный ресурс]. – URL: https://documents.un.org (дата обращения: 11.09.2024).

2. Закон Российской Федерации о поправке к Конституции Российской Федерации от 14 марта 2020 г. № 1-ФКЗ «О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти» // [Электронный ресурс]. Система Гарант (дата обращения: 11.09.2024).

3. Замечание общего порядка Комитета по правам ребенка, 2021 General comment no. 25 (2021) on children's rights in relation to the digital environment, п. 42 // Официальный сайт ООН [Электронный ресурс]. – URL: https://documents.un.org (дата обращения: 11.09.2024).

4. Изучение поведения детей и подростков Российской Федерации в контексте ведения безопасного образа жизни / Авторы исследования подростковой среды: Социологическая клиника прикладных исследований СПбГУ (https://t.me/socioclinic), Федеральный детский общественный совет (https://t.me/federalnyjdetskijsovet) (ФДОС) и фонд «Страна для детей» (https://t.me/stranadlyadetej); https://t.me/oprf_official

5. Резолюция, принятая Генеральной Ассамблеей 16 декабря 2021 года № A/RES/76/139 «Подготовка и проведение тридцатилетнего юбилея Международного года семьи» // Официальный сайт ООН [Электронный ресурс]. – URL: https://documents.un.org (дата обращения: 11.09.2024).

6. Резолюция, принятая Генеральной Ассамблеей 15 декабря 2022 года № A/RES/77/191 «Подготовка и проведение тридцатилетнего юбилея Международного года семьи» // Официальный сайт ООН [Электронный ресурс]. – URL: https://documents.un.org (дата обращения: 11.09.2024).

7. Резолюция, принятая Генеральной Ассамблеей 19 декабря 2023 года № A/RES/78/176 «Подготовка и проведение тридцатилетнего юбилея Международного года семьи» // Официальный сайт ООН [Электронный ресурс]. – URL: https://documents.un.org (дата обращения: 11.09.2024).

8. Указ Президента Российской Федерации от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» / [Электронный ресурс]. Система Гарант. (дата обращения: 11.09.2024).

9. Abujarour S. A., Köster A., Krasnova H., Wiesche M. Technology as a source of power: exploring how ICT use contributes to the social inclusion of refugees in Germany. In Proceedings of the 54th Hawaii International Conference on System Sciences (p. 2637). 2021, January.

10. Global education monitoring report, 2023: technology in education: a tool on whose terms? [Электронный ресурс]. – URL: https://unesdoc.unesco.org/ark:/48223/pf0000385723 (дата обращения: 11.09.2024). DOI: https://doi.org/10.54676/UZQV8501

11. Standaert M. Chinese primary school halts trial of device that monitors pupils' brainwaves // The Guardian. 2019, November 1.

12. Preparations for the thirtieth anniversary of the International Year of the Family, 2024. A/77/61–E/2022/4 // Division for Inclusive Social Development (DISD) (un.org). [Электронный ресурс]. – URL: https://social.desa.un.org/issues/family/news/iyf2024 (дата обращения: 11.09.2024).

13. UNESCO. 2024. Global Education Monitoring Report: Gender report – Technology on her terms. [Электронный ресурс]. – URL: https://unesdoc.unesco.org/ark:/48223/pf0000389406 (дата обращения: 11.09.2024). DOI: https://doi.org/10.54676/WVCF2762

14. United Nations Children's Fund. Neurotechnology and children. 2024, June, pp. 2–3.

ПРАВО ЦИФРОВЫХ ПЛАТФОРМ

А. Ю. Бурова,
кандидат юридических наук, доцент,
Нижегородский государственный университет
имени Н. И. Лобачевского

К ВОПРОСУ ОБ ОТВЕТСТВЕННОСТИ ОПЕРАТОРОВ ФИНАНСОВЫХ ПЛАТФОРМ ЗА НЕНАДЛЕЖАЩЕЕ ИСПОЛНЕНИЕ ФИНАНСОВЫХ СДЕЛОК, СОВЕРШЕННЫХ НА ФИНАНСОВОЙ ПЛАТФОРМЕ

Аннотация. Данная работа посвящена исследованию особенностей ответственности операторов финансовых платформ за ненадлежащее исполнение финансовых сделок, совершенных на финансовой платформе. Проанализированы законодательные акты в рассматриваемой сфере и правила отдельных российских финансовых платформ. По результатам анализа установлено, что подобная ответственность оператора финансовой платформы не предусматривается, поскольку он не является стороной финансовой сделки. В статье моделируются ситуации и описываются условия, при наличии которых оператор финансовой платформы может быть привлечен к ответственности за ненадлежащее исполнение финансовых сделок, совершенных на финансовой платформе.

Ключевые слова: оператор финансовой платформы, финансовый маркетплейс, финансовые сделки, ответственность, цифровой посредник, финансовая организация, получатель финансовых услуг

ON THE LIABILITY OF OPERATORS OF FINANCIAL PLATFORMS FOR IMPROPER PERFORMANCE OF FINANCIAL DEALS CONCLUDED ON FINANCIAL PLATFORMS

Abstract. The paper is devoted to researching for liability of operators of financial platforms for improper performance of financial deals concluded on financial platforms. Legislative acts in this sphere and rules of some Russian financial platforms are analyzed. On the results of analysis it is stated that such liability of operators of financial platforms is not stated as far as it is not a party of a financial deal. The author takes a critical look at this position. In the paper relevant situations are simulated and conditions for possible imposing of liability to operators of financial platforms are described.

Keywords: operator of financial platform, financial marketplace, financial deals, liability, digital intermediary, financial organization, financial service purchaser

Введение. Оператор финансовой платформы относится к категории так называемых цифровых посредников, т. е. лиц, осуществляющих посредничество при совершении сделок на цифровой платформе. С 2019 года законодательно определяются правовые основы регулирования деятельности различных цифровых посредников: владельцев агрегаторов информации о товарах (услугах) [2],

операторов инвестиционных платформ [4], операторов финансовых платформ [5], операторов обмена цифровых финансовых активов [6]. Между тем законодательное регулирование одного из актуальнейших вопросов – вопроса об ответственности цифрового посредника за ненадлежащее исполнение договора, заключенного на платформе цифрового посредника, – крайне скудно, а в ряде случаев его справедливость не так однозначна.

Основная часть. Поскольку произошедшая «интеграция финансовых экосистем и цифровых маркетплейсов» [12] вызвала интерес пользователей к финансовым платформам, в настоящей работе мы кратко обозначим основные аспекты рассматриваемой темы и приведем наши размышления относительно необходимости установления ответственности оператора финансовой платформы за ненадлежащее исполнение сделок, совершенных на финансовой платформе, возможности распространения позиций, выработанных для цифровых посредников в иных сферах на посредничество в финансовой сфере, существования иных механизмов обеспечения законных интересов пользователей финансовых платформ.

1. В настоящее время в правовых актах отражена логичная с юридической точки зрения позиция о том, что оператор платформы не несет ответственность за ненадлежащее исполнение договора, заключенного на платформе, поскольку не является стороной такого договора. Иными словами, он является лишь простым посредником, содействующим заключению договора (маклером), создающим соответствующие условия путем размещения предложения одной стороны и обеспечения возможности другой стороны принять данное предложение. Финансовые платформы в этом аспекте не являются исключением: маркетплейс меняет привычные схемы потребления финансовых услуг [11. С. 419].

2. Обозначенная выше позиция показала свою несостоятельность в потребительских спорах, где периодически возникает вопрос об ответственности владельцев агрегаторов при заказе услуг такси. С 01.09.2023 вступил в силу закон, устанавливающий ответственность службы заказа легкового такси за вред, причиненный жизни, здоровью, имуществу пассажира при перевозке легковым такси: солидарную – в случае если перевозчику не было предоставлено разрешение или действие разрешения которого аннулировано или приостановлено; полную – в случае если в официальных реестрах отсутствуют сведения о перевозчике и транспортном средстве либо если фрахтователь не был уведомлен о наименовании перевозчика; субсидиарную с перевозчиком – физическим лицом – в части возмещения реального ущерба, не покрытого суммой страхового возмещения. [3] Таким образом, в отношении владельцев агрегаторов такси в настоящее время по умолчанию установлена субсидиарная с перевозчиком – физическим лицом ограниченная ответственность за вред, причиненный пассажиру. На владельцев агрегаторов такси законом возложены обязанности по проверке наличия у перевозчика разрешения и сведений о перевозчике и транспортных средствах в официальных реестрах, а ответственность владельца агрегатора дифференцируется в зависимости от нарушения данных обязанностей. Следует отметить, что в зарубежной литературе также предлагается возложить проверку поставщика услуг на оператора платформы с целью освобождения его от ответственности [15. С. 380].

Параллельно отметим, что нам не встретилось релевантной судебной практики по вопросу ответственности операторов инвестиционных, финансовых платформ и операторов обмена цифровых финансовых активов за ненадлежащее исполнение сделок, совершенных на данных платформах. Однако указанный факт не означает отсутствие актуальности рассматриваемой проблемы в данных сферах, а лишь свидетельствует о необходимости предварительной проработки данного вопроса до того момента, как его поставит практика.

3. В соответствии с подп. 2 п. 1 ст. 2 Федерального закона от 20.07.2020 № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы», оператором финансовой платформы признается «юридическое лицо, созданное в организационно-правовой форме акционерного общества в соответствии с законодательством Российской Федерации, оказывающее услуги, связанные с обеспечением возможности совершения финансовых сделок между финансовыми организациями или эмитентами и получателями финансовых услуг с использованием финансовой платформы, и включенное Банком России в реестр операторов финансовых платформ. Оператор финансовой платформы не является стороной финансовых сделок, совершаемых с использованием финансовой платформы».

По состоянию на 02.09.2024 в реестр операторов финансовых платформ включены десять организаций [14]. На финансовых платформах, или финансовых маркетплейсах, как предлагает именовать их Банк России, совершаются разные сделки: договоры банковского вклада (депозита), банковского счета, обязательного и добровольного страхования, кредитования, купли-продажи облигаций, доверительного управления паевым инвестиционным фондом, о брокерском обслуживании, сделки с цифровыми финансовыми активами. Перечень сделок, которые могут совершаться на финансовой платформе, определяется правилами конкретной платформы. В целом в России используется модель «финансового супермаркета» [13. С. 313], где пользователь видит предложения разных финансовых организаций и может отправить заявку на их принятие.

Из представленного перечня следует, что многие из указанных договоров имеют важное значение для получателей финансовых услуг, так как непосредственно отражаются на их финансовом благосостоянии. Указанные договоры заключаются в целях приумножения имеющегося финансового капитала или для достижения иных финансовых целей. Поэтому для получателей финансовых услуг важна надежность как финансовой организации, так и посредника. Многие физические лица предпочитают заключать договоры напрямую с финансовыми организациями, так как опасаются мошенничества со стороны посредников.

4. Действующее законодательство ограничивается упоминанием о том, что оператор финансовой платформы не является стороной финансовых сделок, совершаемых с использованием финансовой платформы. Закон прямо не указывает, что оператор финансовой платформы не несет ответственности за ненадлежащее исполнение финансовых сделок, заключенных на платформе. Однако это вытекает из вышеупомянутого положения. Об этом свидетельствуют и положения правил существующих в России финансовых платформ.

Например, в п. 8.1.11 Правил финансового маркетплейса Финуслуги указывается, что «Оператор платформы не является стороной по Финансовым сделкам и не несет ответственность за неисполнение (ненадлежащее исполнение) любой из сторон Финансовой сделки обязательств по такой сделке» [10].

В п. 6.1.8 Правил финансовой платформы Банки.ру содержится идентичное положение [7].

Оператор финансовой платформы АО «Ванта» снимает с себя ответственность за принятые получателем финансовых услуг инвестиционные решения, указывая в п. 15.16 Правил, что «Оператор не несет ответственности за решения, действия (бездействие) Потребителя финансовых услуг, а также те экономические последствия, которые эти решения, действия (бездействие) могут повлечь для Потребителя финансовых услуг (включая возможные убытки), которые были приняты (совершены) им при осуществлении Финансовых сделок на Финансовой платформе…» [8].

Таким образом, из принятых операторами финансовых платформ правил прямо следует их чисто посредническая роль. Получатель финансовых услуг и финансовая организация самостоятельно определяют условия финансовых сделок и ответственность за их неисполнение. Финансовый маркетплейс лишь содействует заключению договора на этих условиях.

5. На наш взгляд, было бы целесообразным определить наличие возможных исключений из данного правила. Вполне вероятно, что практика в этой сфере со временем поставит перед судами подобные вопросы. Так, следует проработать вопрос об ответственности финансовых маркетплейсов в случаях, когда, например, в период действия договора банковского вклада, заключенного на финансовой платформе, у банка отозвана лицензия на осуществление банковских операций (а сумма вклада превышает гарантированную законом сумму выплаты), в период действия договора страхования у страховой организации отозвана лицензия на осуществление страховых операций, допущен дефолт эмитента облигаций, приобретенных на финансовой платформе, и т. д.

Возможны и нарушения со стороны получателя финансовых услуг, например, нарушение заемщиком графика возврата задолженности по договору кредитования.

Итак, представим, что произошло нарушение финансовой сделки, совершенной при посредничестве оператора финансовой платформы. Банк не имеет возможности вернуть сумму депозита с начисленными процентами, поскольку у него отозвали лицензию на осуществление банковских операций, или, наоборот, заемщик не возвращает кредитору сумму займа в соответствии с графиком погашения задолженности. По общему правилу, финансовый маркетплейс действительно не будет нести ответственность за это. Однако ситуация меняется, если оператор финансовой платформы разместил предложение банка, в отношении которого было достоверно известно, что в ближайшее время он не сможет вернуть вклад клиента, или если оператор передал финансовой организации информацию о кредитном рейтинге получателя финансовой услуги, не соответствующую действительности.

По нашему мнению, если посредник берет на себя важную функцию «сведения» контрагентов в финансовой сфере, он должен максимально обеспечить

надлежащее исполнение обеими сторонами условий совершенной сделки. Тем более что финансовые платформы осуществляют проверку финансовых организаций и запрашивают официальные данные о получателе финансовых услуг.

Например, согласно Правилам финансового маркетплейса Банки.ру, «4.3.12. Оператор платформы проверяет достоверность документов и информации, предоставленных Финансовой организацией.

4.4.1. Финансовыми организациями могут быть только юридические лица, отвечающие требованиям законодательства Российской Федерации, нормативных актов Банка России и Правил платформы.

4.4.2. Финансовая организация должна соответствовать требованиям, содержащимся в Правилах платформы, в течение всего времени, когда такая Финансовая организация допущена к заключению Финансовых сделок. Несоответствие данным требованиям является основанием для приостановления/прекращения Допуска к заключению Финансовых сделок».

Установленные положения прямо свидетельствуют о том, что оператор берет на себя обязанность проверить финансовую организацию, а в случае ненадлежащего исполнения указанной обязанности существуют основания для возложения на финансовый маркетплейс субсидиарной ответственности, которая будет дополнять базовую ответственность финансовых организаций.

В этой связи интересный пункт включен в Правила финансовой платформы Сравни.ру. В п. 15.8 Правил установлено, что в случае если действия Финансовой организации создают или могут создать угрозу интересам Получателей финансовых услуг при совершении Финансовых сделок, с Финансовой организации могут быть взысканы убытки, возникшие у Оператора вследствие действий Финансовой организации [9]. Таким образом, можно предположить, что если иск получателя финансовой услуги к оператору платформы о взыскании понесенных получателем убытков будет удовлетворен, то оператор может взыскать эти средства у финансовой организации в порядке регресса. То есть оператор финансовой платформы заранее желает обезопасить себя от последствий предъявления подобных требований.

В случае принятия концепции субсидиарной ответственности финансовых маркетплейсов можно обсудить вопрос об обязательном страховании такой ответственности, что, однако, повлечет за собой установление комиссий для получателей финансовых услуг (например, за доступ к платформе или за совершение сделки) или повышение тарифов для финансовых организаций.

Что касается ответственности за неисполнение финансовой сделки со стороны получателя финансовых услуг, то оператор финансовой платформы собирает официальные сведения, полученные из ЕСИА, Объединенного кредитного бюро и т. п., и при условии их неизменной передачи финансовой организации не может отвечать за неисполнение обязательств потребителем, так как финансовая организация самостоятельно на основе представленных о клиенте данных принимает решение о заключении с ним договора. Однако если сведения о получателе финансовых услуг были искажены оператором и это прямо повлияло на возникновение убытков у финансовой организации, возможно возложение на маркетплейс солидарной с финансовой организацией ответственности либо, при намеренном искажении сведений, полной ответственности.

Полная ответственность оператора финансовой платформы, на наш взгляд, возможна также и в случае допуска получателя финансовой услуги к финансовой сделке без прохождения соответствующего тестирования. Так, с апреля 2024 г. для получателей финансовых услуг на финансовых платформах стало обязательным прохождение тестирования для приобретения ценных бумаг [1]. Следовательно, если финансовая платформа не обеспечит прохождение тестирования, не уведомит пользователя о необходимости его прохождения и допустит его к совершению сделок с ценными бумагами, в случае возникновения у пользователя убытков от совершения данных сделок может обсуждаться вопрос о взыскании данных убытков с оператора финансовой платформы.

Заключение. Таким образом, концепция ответственности финансовых маркетплейсов за ненадлежащее исполнение финансовых сделок, совершенных на финансовой платформе, не должна ограничиваться простой констатацией факта о том, что такой ответственности нет. Она должна быть усовершенствована исходя из возможных ситуаций, а границы ответственности должны быть четко очерчены законом.

Список литературы

1. О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 11.03.2024 № 45-ФЗ // СЗ РФ. – 2024. – № 12. – Ст. 1569.

2. О защите прав потребителей: Закон РФ от 07.02.1992 № 2300-1 (ред. от 08.08.2024) // СЗ РФ. – 1996. – № 3. – Ст. 140.

3. Об организации перевозок пассажиров и багажа легковым такси в Российской Федерации, о внесении изменений в отдельные законодательные акты Российской Федерации и о признании утратившими силу отдельных положений законодательных актов Российской Федерации: Федеральный закона от 29.12.2022 № 580-ФЗ // СЗ РФ. – 2023. – № 1 (ч. I). – Ст. 27.

4. О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 02.08.2019 № 259-ФЗ (ред. от 08.08.2024) // СЗ РФ. – 2019. – № 31. – Ст. 4418.

5. О совершении финансовых сделок с использованием финансовой платформы: Федеральный закон от 20.07.2020 № 211-ФЗ (ред. от 11.03.2024) // СЗ РФ. – 2020. – № 30. – Ст. 4737.

6. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 08.08.2024) // СЗ РФ. – 2020. – № 31 (ч. I). – Ст. 5018.

7. Правила финансовой платформы Акционерного общества «Банки.ру Маркетплейс»: Приказ Генерального директора АО «Банки.ру Маркетплейс» от 03.06.2024 № 22 (ред. № 10). [Электронный ресурс]. – URL: https://static2.banki.ru/mkp/rules_ofp_10.pdf (дата обращения: 02.09.2024).

8. Правила финансовой платформы Акционерного общества «Ванта»: Приказ АО «Ванта» от 16.11.2023 № 1-2 (ред. № 3). [Электронный ресурс]. – URL:

https://www.vanta.ru/documents/main/Правила_финансовой_платформы.pdf (дата обращения: 02.09.2024).

9. Правила финансовой платформы АО «Финансовый Маркетплейс Сравни.ру»: Приказ Генерального директора АО «Финансовый Маркетплейс Сравни.ру» от 16.07.2024 № 35. [Электронный ресурс]. – URL: https://sravni.market/pdf/platform_rules_from_16.07.2024.pdf (дата обращения: 02.09.2024).

10. Правила финансовой платформы Публичного акционерного общества «Московская Биржа ММВБ-РТС»: Решение Правления ПАО Московская Биржа от 01.08.2024 (Протокол № 59). [Электронный ресурс]. – URL: https://assets.finuslugi.ru/mp-assets/platform-rules.pdf (дата обращения: 02.09.2024).

11. Белоусов А. Л. Теоретические и практические аспекты формирования финансового маркетплейса в Российской Федерации // Russian Journal of Economics and Law. – 2021. – Т. 15, № 3. – С. 413–424.

12. Жигас М. Г. К вопросу о финансовом маркетплейсе // Baikal Research Journal. – 2021. – Т. 12, № 2.

13. Петров Д. А., Тюрина А. В. К вопросу о финансовом маркетплейсе и его правовом регулировании // Цифровые технологии и право: сб. науч. трудов II Межд. науч.-практ. конф., Казань, 22 сентября 2023 г. – В 6 т. Т. 1. – Казань: Познание, 2023. – С. 307–315.

14. Реестр операторов финансовых платформ. [Электронный ресурс]. – URL: https://cbr.ru/finm_infrastructure/registry/?CF.Search=финансовых&CF.Date.Time=Any&CF.Date.DateFrom=&CF.Date.DateTo= (дата обращения: 02.09.2024).

15. Miriam C. Buiten. The Digital Services Act: From Intermediary Liability to Platform Regulation // Journal of Intellectual Property, Information Technology and E-Commerce Law. – 2021. – № 12. – Pp. 361–380.

А. И. Мелешкина,
кандидат экономических наук, младший научный сотрудник,
Московский государственный университет имени М. В. Ломоносова

НЕОБХОДИМОСТЬ РЕГЛАМЕНТАЦИИ ПОРЯДКА ОЦЕНКИ СЕТЕВЫХ ЭФФЕКТОВ НА РЫНКАХ С ПЛАТФОРМАМИ

Аннотация. В статье поднимается проблема правовой неопределенности вокруг методики оценки сетевых эффектов в рамках антимонопольного законодательства. Основой статьи служит анализ изменений, внесенных в антимонопольное законодательство (пятый антимонопольный пакет). В исследовании приведены определение и типология сетевых эффектов с точки зрения экономической теории, без понимания которой невозможно корректно регламентировать процедуру оценки сетевых эффектов. Работа носит междисциплинарный характер – на стыке юриспруденции и экономической теории.

Ключевые слова: сетевой эффект, антимонопольное регулирование, платформы, цифровая экономика, конкуренция, маркетплейсы, ФАС России

THE NEED TO REGULATE EVALUATION OF NETWORK EFFECTS IN MARKETS WITH PLATFORMS

Abstract. The article raises the problem of legal uncertainty around the methodology for assessing network effects within the framework of antitrust legislation. The article is based on the analysis of changes made to the antitrust legislation (the fifth antitrust package). The study provides a definition and typology of network effects from the point of view of economic theory, without understanding which it is impossible to correctly regulate the procedure for assessing network effects. The work is interdisciplinary in nature - at the junction of jurisprudence and economic theory.

Keywords: network effect, antitrust, platforms, digital economy, competition, marketplaces, FAS Russia

Введение. В июле 2023 года был принят Федеральный закон от 10.07.2023 № 301-ФЗ «О внесении изменений в Федеральный закон «О защите конкуренции» (далее – ФЗ № 301-ФЗ), именуемый пятым антимонопольным пакетом. Цель нововведений в антимонопольное законодательство – совершенствование регулирования цифровых рынков. Среди ключевых положений ФЗ № 301-ФЗ, требующих дополнительной проработки со стороны регулятора и особого внимания со стороны участников цифровых рынков, – понятие сетевых эффектов.

Основная часть. «Сетевой эффект – свойство товарного рынка (товарных рынков), при котором потребительская ценность программы (совокупности программ) для электронных вычислительных машин в информационно-телекоммуникационных сетях, в том числе в сети Интернет, обеспечивающей совершение сделок между продавцами и покупателями определенных товаров (далее – цифровая платформа), изменяется в зависимости от изменения количества таких продавцов и покупателей».[1]

Проблема правовой неопределенности. В соответствии с принятыми поправками в антимонопольное законодательство учет сетевого эффекта является частью процедуры проведения анализа состояния конкуренции на товарных рынках с цифровыми платформами. При этом антимонопольный орган устанавливает наличие сетевых эффектов и определяет возможность у платформы оказывать решающее влияние на условия обращения товара на рынке/устранять других участников рынка/создавать барьеры входа на рынок.

Основной проблемой в реализации данного положения ФЗ № 301-ФЗ является отсутствие алгоритма оценки сетевого эффекта, что может вести к ошибкам в правоприменении и созданию отрицательных экономических эффектов для участников цифровых рынков.

Экономический смысл сетевого эффекта заключается не в факте его наличия, а в его параметрах:

1) сетевой эффект может обладать разной интенсивностью. Сила сетевого эффекта в значительной степени зависит от стадии развития рынка – чем более зрелый рынок с точки зрения насыщения спроса, тем сильнее сетевой эффект.

[1] URL: https://www.consultant.ru/document/cons_doc_LAW_61763/baabe5b69a3c031bfb8d4858-91bf8077d6809a94

Однако зависимость «ценности» платформы для потребителей может иметь разные формы зависимости от количества пользователей платформы – линейную, степенную или показательную. Форма зависимости переменных позволяет определить, насколько быстро растет сетевой эффект и когда он начинает замедляться/снижаться. В зависимости от силы эффекта будет отличаться и возможность платформы оказывать влияние на условия конкуренции на рынке [3, 4]. Учет данного параметра в ходе антимонопольного регулирования рынка необходим для оценки преодолимости барьеров входа на цифровые рынки;

2) по направлению сетевые эффекты делятся на прямые и косвенные [1, 2]. Прямые сетевые эффекты характеризуются ситуацией, когда увеличение степени использования платформы ведет к прямому увеличению ее ценности для пользователей, увеличивая их желание платить за услуги платформы. Такого рода эффекты возникают на платформах мессенджерах, предоставляющих возможность обмена сообщениями между пользователями (чем больше пользователей мессенджера, тем привлекательнее он для аудитории).

Косвенный сетевой эффект возникает тогда, когда одна категория пользователей выигрывает от присоединения к платформе другой категории. Например, агрегатор такси становится более востребованным для стороны предложения (таксистов), когда обладает большой аудиторией на стороне спроса (пассажирами, подключенными к сервису заказа такси в рамках платформы).

Направление сетевого эффекта определяет структуру цифрового рынка, его границы и емкость – эти параметры являются ключевыми для определения состояния конкуренции на цифровых рынках и последующего вынесения решения о наличии/отсутствии антиконкурентных действий компании. В случае игнорирования прямых или косвенных сетевых эффектов возможны ошибки антимонопольного регулирования двух типов – слишком узкое определение границ рынка (в таком случае платформа с высокой вероятностью будет признана доминирующей на рынке и будет подвержена избыточному государственному регулированию), и слишком широкое определение границ рынка (в таком случае в границы рынка войдет значительное число компаний и злоупотребление доминирующим положением, проявляющееся в установлении монопольно высоких цен или создании барьеров входа, останется незамеченным);

3) сетевой эффект может быть как положительным, так и отрицательным. Выше говорилось о положительных сетевых эффектах (новый пользователь увеличивает полезность платформы для других пользователей), однако есть и противоположный тип сетевого эффекта. Отрицательный сетевой эффект – снижение полезности платформы для пользователей в случае присоединения нового участника. Такого рода ситуации возможны в условиях большой загрузки сервера и перегрузки сети. Положительные и отрицательные сетевые эффекты могут уравновешивать друг друга, не позволяя платформе безгранично расширяться. Этот фактор должен учитываться в рамках антимонопольной практики регулирования цифровых рынков при оценке возможности злоупотребления доминирующим положением хозяйствующего субъекта. В противном случае возможна ошибка антимонопольного регулирования, связанная с переоценкой положительных сетевых эффектов и завышением оценок рыночной власти компаний. Такие ошибки влекут за собой дополнительные предписания со стороны ФАС России и штрафные санкции.

Перечисленные выше параметры не находят отражения в пятом антимонопольном пакете, в связи с чем возрастает риск некорректного определения границ цифровых рынков и барьеров входа на рынки с платформами.

Кроме того, новые правила регулирования цифровых рынков не учитывают возможность потребителя использовать сразу несколько сетей одновременно. Это явление именуют множественной адресацией (multihoming). Мультихоуминг пользователя снижает его издержки переключения между платформами и ограничивает их рыночную власть.

Перечисленные проблемы в реализации антимонопольного регулирования цифровых рынков с платформами создают риски для участников рынков с точки зрения несения репутационных и финансовых издержек в случае ошибок правоприменения, одновременно приводя к росту административной нагрузки регулятора. В условиях, когда нормативно-правовая база имеет существенные пробелы, компании – участники рынков вынуждены самостоятельно предпринимать меры, направленные на снижение антимонопольных рисков – в рамках антимонопольного комплаенса. В ситуации правовой неопределенности требуются разъяснения со стороны ФАС России относительно процедуры оценки сетевых эффектов на рынках с цифровыми платформами.

Заключение. Описанная проблема может приводить к отрицательным последствиям не только на рынках с платформами в границах РФ, но и распространяться на территории ЕАЭС при формировании общих товарных рынков, а также в ходе развития интегрированной информационной системы ЕАЭС. Биржи и электронные торговые площадки по своей сути также являются платформами и могут вести к ухудшению конкуренции в случае нарушения требований антимонопольного законодательства. В связи с чем регламентация мониторинга и оценки сетевых эффектов имеет значение и для реального сектора экономики, который все в большей степени становится зависим от платформенного ценообразования и обмена ценовыми данными.

Список литературы

1. Маркова О. А. Определение границ рынков с платформами: как учитывать сетевые экстерналии и эффект переноса? // Вопросы теоретической экономики. – 2022. – № 3. – С. 7–30.

2. Рожкина В. С., Голованова С. В., Корнеева Д. В. Количественная оценка перекрестных сетевых эффектов для нетрансакционных платформ // Вестник Московского университета. Серия 6. Экономика. – 2022. – № 4. – С. 17–38.

3. Cen Y., Li L. Effects of network externalities on user loyalty to online B2B platforms: an empirical study // Journal of Enterprise Information Management. 2019. [Электронный ресурс]: https://www.emerald.com/insight/content/doi/10.1108/JEIM-02-2019-0050/full/html (дата обращения: 20.08.2024).

4. Toh P. K., Chung J. S. Competition-Based Network Effect and Heterogeneity in Participation Channels within Platforms // Academy of Management Proceedings. 2023. [Электронный ресурс]: https://journals.aom.org/toc/amproc/2023/1 (дата обращения: 20.08.2024).

С. И. Семцива,
аспирант,
Финансовый университет при Правительстве Российской Федерации

ЦИФРОВЫЕ ПЛАТФОРМЫ КАК НОВЫЙ ЭТАП РАЗВИТИЯ ТРАНСНАЦИОНАЛЬНЫХ КОРПОРАЦИЙ

Аннотация. Развитие цифровых технологий в финансовой сфере обеспечивает оптимальное взаимодействие между гражданами, бизнесом и государством, что требует совершенствования правового регулирования данной сферы как на национальном уровне, так и на уровне интеграционных объединений. В статье рассматривается правовая природа цифровых платформ как транснациональных корпораций нового поколения, приводятся авторская классификация и описание на основе экосистемного подхода.

Ключевые слова: цифровая платформа, экосистема, транснациональные корпорации (ТНК), цифровизация, этапы развития, маркетплейс, финансовый сервис

DIGITAL PLATFORMS AS A NEW STAGE IN THE DEVELOPMENT OF MULTINATIONAL CORPORATIONS

Abstract. The development of digital technologies in the financial sector makes it possible to create digital platforms to optimally build interaction between citizens, business and the state, which in turn requires improving the legal regulation of this issue both at the national level and at the level of the Eurasian Economic Union. The article analyzes the legal nature of digital platforms as multinational corporations of the latest generation, gives the author's classification and definition based on the ecosystem approach.

Keywords: digital platform, ecosystem, multinational corporations (MNCs), digitalization, stages of development, marketplace, financial service

Цифровые платформы играют ключевую роль в стимулировании инноваций в экономике и представляют собой смешанные модели, известные как многосторонние платформы (multi-sided platforms), которые сосредоточены на распространении товаров и предоставлении услуг, включая финансовые. Это происходит благодаря непосредственному взаимодействию между пользователями и операторами данных платформ. В настоящее время нет единого подхода в законодательстве и доктрине к определению термина «платформа» как категории. В зависимости от конкретной юрисдикции законодательные органы используют такие термины, как «платформа», «суперплатформа», «экосистема» и «маркетплейс». Платформа представляет собой совокупность инструментов, действующих в рамках Интернета, которые обычно связаны с реализацией различных форм экономической и социальной активности. Применяя свои уникальные алгоритмы, эти инструменты обеспечивают организацию и систематизацию упомянутых видов деятельности [8]. Решение Высшего Евразийского экономического совета от 11.10.2017 № 12 «Об Основных направлениях реализации цифровой повестки Евразийского

экономического союза до 2025 года» закрепляет «цифровую платформу» как «систему средств, поддерживающих использование цифровых процессов, ресурсов и сервисов значительным количеством субъектов цифровой экосистемы и обеспечивающая возможность их бесшовного взаимодействия» [2].

Исследование уникальных характеристик и сравнительный анализ функционирования традиционных и цифровых транснациональных корпораций представляет собой актуальную тему как в России, так и за рубежом [6]. Считается, что ТНК прошли в своем развитии пять этапов: I этап (с 1860-х гг. по 1917 г.) – добыча и переработка сырьевых ресурсов в колониальных странах Азии, Африки, Латинской Америки, а также странах – владельцах колоний; II этап (с 1917 по 1950-е гг.) – производство вооружений и военной техники ведущими странами Европы, Америки и Азии; III этап (1950–1960-е гг.) – развитие НИОКР и международной кооперации; IV этап (1970–1980-е гг.) – появление «глобальных корпораций». V этап (1990–2010 гг.) – процессы региональной интеграции.

Некоторые исследователи выделяют появление цифровых платформ в качестве нового, VI этапа эволюции ТНК. В отличие от традиционных ТНК одним из критериев цифровых платформ является сетевой эффект от количества пользователей, который способствует увеличению монетизации от рекламной деятельности.

Согласно Конвенции СНГ о ТНК 1998 г., Транснациональные корпорации представляют собой «юридическое лицо (совокупность юридических лиц), которое имеет в собственности, хозяйственном ведении или оперативном управлении обособленное имущество на территориях двух и более сторон; образовано юридическими лицами двух и более сторон; зарегистрировано в качестве корпорации в соответствии с указанной Конвенцией» [1].

Как отмечают А. В. Алтухов и С. Ю. Кашкин, «цифровая платформа является многозначным термином, который в узком смысле употребляется в следующих значениях:

1) производственная система, состоящая из оборудования и управляющего им программного обеспечения;

2) аппаратная (операционная) платформа как совокупность программного обеспечения и совместимых устройств;

3) некоторый продукт (инструмент, способ), позволяющий пользователям находить друг друга и обмениваться ценностями (информационными, культурными, материальными, финансовыми и любыми другими)» [4].

В Программе развития цифровой экономики в Российской Федерации до 2035 года платформа рассматривается как «коммуникационная и транзакционная среда, участники которой извлекают выгоды от взаимодействия друг с другом» [3]. Широкое понимание термина «платформа» как различных цифровых сервисов, разработанных с применением современных информационных технологий, представляется наиболее уместным и помогает лучше понять цифровую природу работы платформ.

Стоит отметить, что в зарубежной практике платформенные сервисы особенно распространены в сфере B2C-контрактов, что обуславливает их в качестве

сервисов электронной коммерции. Как правило, такие сервисы предлагают уникальные решения, а также маркетинговую поддержку и иные услуги, исключая при этом необходимость в самостоятельной разработке/доработке платформы или приобретении прав на интеллектуальную собственность.

В Российской Федерации исторически платформы образовывались вокруг финансового сектора, к которому постепенно присоединялся торговый блок (например, экосистема Сбербанка, в которой к платежному сервису впоследствии был интегрирован СберМегамаркет, выполняющий функционал торгового агрегатора). Это в том числе отражает различные механизмы формирования финансовых платформ. В зарубежной доктрине преобладает их образование на коммерческой основе товарных холдингов, в то время как в России – на государственной основе.

Совокупность открытых и закрытых платформенных решений, предоставляемых одной или несколькими компаниями, формирует экосистему и позволяет пользователям получать широкий спектр финансовых и нефинансовых продуктов в рамках единого интегрированного процесса. Полноценная экосистема должна включать в себя четыре ключевые подсистемы: объектную (участники), средовую (платформа), процессную (сеть), проектную (инновационные решения). Данная конфигурация обеспечивает устойчивость системы и позволяет отдельным элементам (платформам) привлекать недостающие ресурсы внутри самой экосистемы. Эксперты McKinsey прогнозируют, что к 2025 году экосистемы будут составлять около 30 % глобального ВВП [10].

Говоря о различных видах ТНК, стоит выделить четыре основные классификации: по типу интеграции (горизонтальные, вертикальные, раздельные), по форме собственности (частные, государственные, смешанные), по характеру организации (институционные и договорные) и по характеру и масштабу деятельности (интернациональные, мультинациональные, глобальные). Уделяя внимание цифровым платформам как последнему этапу в эволюции ТНК, важно также учитывать критерий классификации в зависимости от уровня цифровизации: 1) полностью цифровые платформы, где практически все бизнес-процессы ориентированы на виртуальную среду, 2) гибридные платформы, которые объединяют традиционные офлайн-продукты и услуги с цифровыми моделями ведения бизнеса [5].

Конференция ООН по торговле и развитию (ЮНКТАД) «классифицирует цифровые ТНК на четыре типа:

1. интернет-платформы: предприятия, управляемые и реализуемые через сеть Интернет;

2. цифровые решения: цифровые агрегаторы, поставщики программного обеспечения (например, услуги SaaS), FinTech в дополнение к решениям для электронных платежей;

3. электронная коммерция: онлайн-платформы, позволяющие осуществлять коммерческие транзакции;

4. цифровой контент: производители и дистрибьюторы товаров и услуг в цифровом формате» [6].

Экосистема имеет широкий, но ограниченный круг участников, объединенных общей концепцией эффективной и успешной конкуренции на рынке. В целях

создания экосистемы крупной финансовой организации круг участников определяется управляющими структурами и разрабатывается так, чтобы платформы удовлетворяли основные потребности клиентов.

Наиболее полное определение платформы было дано Джереми Миллардом, управляющим директором компании Third Millennium Governance, на основе экосистемного подхода. В своей работе он определяет платформу как «открытую среду и экосистему с понятным набором смоделированных правил, вспомогательных руководств для пользователей, ресурсов и службы поддержки, которые стимулируют сотрудничество представителей всех референтных групп для создания не только общественной ценности, но и ценности для каждого участника в отдельности так, как он ее понимает» [9].

Данное определение охватывает ключевые характеристики государственных цифровых платформ, включая: ценность общественного взаимодействия на платформе, содействие механизмам совместной работы, а также четкую и доступную модель взаимодействия с понятными инструкциями для различных категорий пользователей. Еще одним обязательным критерием для функционирования цифровых финансовых платформ является множественность рынков. Такая платформа должна иметь неограниченные финансовые возможности, включая возможность покрыть затраты на IT-услуги, что обеспечивает ее финансовую состоятельность, устойчивость и транснациональный характер.

Таким образом, исходя из экосистемного подхода в рамках новейшего, VI, этапа развития транснациональная корпорация как цифровая платформа представляет собой группу юридических лиц, формирующих закрытую экосистему, действующую на территории двух и более юрисдикций, имеющую единый центр принятия решений и обеспечивающую внутреннее взаимодействие.

Список литературы

1. Конвенция о транснациональных корпорациях (Москва, 6 марта 1998 г.) (Российская Федерация не является участником). – URL: https://base.garant.ru/1154622/?ysclid=ltbl0sr9mz462949105 (дата обращения: 03.09.2024).

2. Решение Высшего Евразийского экономического совета от 11.10.2017 № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года» // Официальный сайт Евразийского экономического союза. – URL: http://www.eaeunion.org/, 10.11.2017.

3. Развитие цифровой экономики в России. Программа до 2035 года. – URL: https://spkurdyumov.ru/uploads/2017/05/strategy.pdf (дата обращения: 02.09.2024).

4. Алтухов А. В., Кашкин С. Ю. Правовая природа цифровых платформ в российской и зарубежной доктрине // Актуальные проблемы российского права. – 2021. – Т. 16, № 7. – С. 86–94.

5. Гуркова М. Д. Цифровые транснациональные компании: особенности и тренды развития // Экономика и бизнес: теория и практика. – 2023. № 4–1(98). – С. 92–95.

6. Официальный сайт Конференции ООН по торговле и развитию (ЮНКТАД). – URL: https://unctad.org (дата обращения: 09.09.2024).

7. Andersson Schwarz J. Platform logic: An Interdisciplinary approach to the platform-based economy // Policy & Internet. – 2017. – Vol. 9, № 4. – Pp. 374–394.
8. Kenney M., Zysman J. The Rise of the Platform Economy // Issues in Science and Technology. – 2019. – Vol. 32, № 3. – Pp. 61–65.
9. Millard J. Open governance systems: Doing more with more // Government Information Quarterly. – 2018. – Vol. 35, № 4. – Pp. 77–87.
10. Digital McKinsey: Insights January-2018: Winning in digital ecosystems. – URL: 14_3004 Digital McKinsey Insights cx.pdf (дата обращения: 05.09.2024).

В. В. Цветков,
главный юрисконсульт,
ООО «Газпром газификация»

ИНИЦИАТИВА ЕС ПО ПРАВОВОМУ РЕГУЛИРОВАНИЮ ТРУДА РАБОТНИКОВ ЦИФРОВЫХ ПЛАТФОРМ

Аннотация. В представленной статье описываются сложности в части правового регулирования деятельности цифровых платформ, с которыми ЕС сталкивается по мере их технического развития, а также предлагаемые пути решения, к которым прибегают компетентные органы ЕС с целью достижения единообразия наднационального правового регулирования труда гиг-работников и гармонизации национального законодательства государств – членов в указанной части.

Ключевые слова: трудовое право ЕС, цифровые платформы, гиг-работники, права человека, цифровые услуги, интеграция

EU INITIATIVE ON THE LEGAL REGULATION OF THE LABOR OF WORKERS ON DIGITAL PLATFORMS

Abstract. The article describes the difficulties in terms of legal regulation of digital platforms, which the EU is facing as they are technically developing, as well as the ways of solution, which the competent EU authorities resort to in order to achieve uniformity of supranational legal regulation of gig workers' labor and harmonization of national legislation of the EU Member States in this part.

Keywords: EU labor law, digital platforms, gig workers, human rights, digital services, integration

Введение. В эпоху цифровизации множество некогда привычных вещей можно делать не выходя из дома. Исследование прилавков гипермаркетов сменяется на пролистывание ленты продуктов на смартфоне, поездка на другой конец города заменяется сервисом доставки в удобное время. Готовую еду, продукты можно получить в течение получаса. Сервис такси позволяет добраться в любую точку города в любое время дня и ночи с подачей автомобиля от одной минуты. И для обеспечения этих теперь уже привычных удобств повсеместно используются специальные приложения, гарантирующие доступ на страницу с перечнем товаров, возможностями доставки, а порой и актуальной информацией в режиме

реального времени за движением заказанного товара. Такие приложения позволяют покупателям и продавцам проводить торговые операции вслепую, а зачастую без личного контакта, посредством обращения к соответствующему цифровому сервису.

Кроме того, далеко не все предприниматели готовы обеспечить разработку собственных приложений, сайтов, а также сложного программного функционала для обеспечения всей логистической цепочки от сбора заказа до его получения покупателем. В данном ключе удобнее возлагать эти функции на агента – цифровой сервис, а самим делать то, что получается лучше всего, к примеру, готовить еду.

Основная часть. Цифровые сервисы принято именовать «цифровыми платформами (площадками)». В сети Интернет распространено следующее определение электронной площадки: «программно-аппаратный комплекс информационных, организационных и технических решений, которые обеспечивают взаимодействие между поставщиком – продавцом товаров (работ, услуг) и заказчиком – покупателем, осуществляющим закупки, через электронные каналы связи» [1].

В связи с резким увеличением потребностей цифровых площадок наблюдается скачок спроса на основной пул работников таких площадок: курьеров, водителей, операторов поддержки, преподавателей онлайн-школ, фрилансеров и прочих специалистов.

«Трудовые платформы существенно отличаются от традиционных организаций. В них отсутствует управленческая иерархия и отношения соподчиненности, работники выступают в роли индивидуальных формально независимых производителей. Количественный состав рабочей силы четко не определен, ее границы размыты, рассредоточенные в пространстве и времени трудящиеся функционируют поодиночке. Сам труд имеет прерывистый, дискретный характер, распадаясь на отдельные эпизоды. Работники социально изолированы друг от друга, не имеют каналов горизонтальной коммуникации, не связаны узами общей корпоративной культуры… В руках государства цифровые платформы становятся инструментом легализации неформальной занятости при отсутствии должного внимания к трудовым правам и социальной защите работников» [2].

С учетом постоянного транснационального расширения бизнеса возникает ряд проблем, связанный с регулированием труда таких работников. В настоящее время в работе цифровых площадок по всему Европейскому союзу (ЕС) задействовано около 28 миллионов человек [3]. Отметим, что на уровне ЕС также отсутствует однозначное определение того, кем является работник, равно и самого понятия трудового договора (как соглашения, юридического факта, письменного документа, трудового правоотношения) [4]. Основная проблема возникает в связи с весьма различным регулированием трудовых отношений в государствах-членах и совершенно различной практикой национальных судов о том, признавать ли водителей, курьеров, онлайн-учителей работниками по смыслу национального законодательства. Каждое государство само разрабатывало свои критерии распространения трудового законодательства на возникшие правоотношения, в большинстве случаев основное внимание уделялось подчиненности работника деятельности работодателя, распорядку дня, инструкциям работодателя (хозяйской власти).

Последние компративистские исследования в части анализа судебной практики показывают следующее [5]:

– водители интернет-платформ по заказу такси признаются наемными работниками самих платформ в Нидерландах и Испании (не считая Швейцарию и Великобританию, не входящих в ЕС), но пока признаются как самозанятые во Франции;

– курьеры служб доставки еды признаются наемными работниками в Нидерландах, Испании, Италии, Франции; признаются самозанятыми в Ирландии; имеется тенденция к признанию их отношений трудовыми в Финляндии и Швеции;

– курьеры по доставке посылок признаны работниками только в Испании;

– лица, осуществляющие клининг, и домработники признаются самозанятыми в Дании и Швеции;

– труд лиц, выполняющих отдельные «микрозадачи», был предметом рассмотрения судов только в Австрии, Франции и Германии, однако практика судов разнородная и не позволяет сделать вывод о какой-либо сложившейся тенденции в этой части.

Суд ЕС до настоящего времени не выработал какую-либо практику в отношении указанных выше случаев, которая бы позволила привести судебную практику национальных судов к единообразию. Учитывая то, что в государствах-членах стала складываться различная практика по отношению к труду гиг-работников (работников платформ), требуется гармонизирующее воздействие со стороны наднационального органа, направленное на обеспечение минимальной и о возможности равномерной социальной защиты для таких работников на территории всего Союза.

11 марта 2024 года министры по делам занятости и социальным вопросам 27 государств – членов ЕС достигли соглашения по новой директиве [6] по улучшению условий труда для работников платформ.

Директива включает в себя, прежде всего, определение цифровой платформы: любое физическое или юридическое лицо, предоставляющее услугу, которая отвечает всем следующим требованиям: a) она предоставляется, по крайней мере частично, на расстоянии с помощью электронных средств, таких как веб-сайт или мобильное приложение; (b) предоставляется по запросу получателя услуги; (c) включает в себя как необходимый и существенный компонент организацию работы, выполняемой отдельными лицами за вознаграждение, независимо от того, выполняется ли эта работа в Интернете или в определенном месте; (d) предполагает использование автоматизированных систем контроля или принятия решений.

Также дается определение автоматизированных систем мониторинга и принятия решений: «автоматизированные системы мониторинга» – это системы, которые используются или поддерживают мониторинг, контроль или оценку трудовой деятельности лиц, выполняющих работу на платформе, или деятельности, осуществляемой в рабочей среде, в том числе путем сбора персональных данных, с помощью электронных средств; «автоматизированные системы принятия решений» означают системы, которые используются для принятия или поддержки с помощью электронных средств решений, которые существенно влияют на права лиц,

выполняющих работу на платформе, включая условия труда работников платформы, в частности, решения, влияющие на их наем, доступ к рабочим заданиям и их организацию, их заработок, включая ценообразование индивидуальных заданий, их безопасность и здоровье, их рабочее время, доступ к обучению, продвижению по службе или его эквиваленту, их контрактный статус, включая ограничение, приостановление или прекращение действия их учетной записи.

Основное достижение директивы заключается в установлении презумпции наличия трудовых отношений между лицом, осуществляющим трудовую деятельность в интересах платформы, и самой цифровой платформой. Критерий наличия трудовых отношений – установленный в соответствии с национальным законодательством, коллективными договорами или практикой, действующими в государствах-членах, и с учетом прецедентного права Суда ЕС, факт контроля и руководства над процессом труда. Бремя доказывания отсутствия трудовых отношений возлагается на саму цифровую платформу. ЕС не обязывает применять презумпцию к разбирательствам, касающимся налоговых, уголовных дел и вопросов социального обеспечения, но государства-члены вправе применять указанную презумпцию и в указанных делах. При этом некоторые средства массовой информации ожидали провала такого положения в финальной редакции директивы из-за чрезмерно размытого и нечеткого критерия распространения презумпции на возникшие отношения [5].

Вводимая презумпция наличия трудовых отношений напоминает уже прописанную презумпцию в разделе 2750(b)(1) Трудового кодекса штата Калифорния (США) [6], однако американское законодательство следует от обратного: отношения считаются трудовыми, пока работодатель не докажет: a) свободу лица, выполняющего работу, от контроля и руководства; b) выполняемая работа выходит за рамки обычной деятельности работодателя; c) лицо за рамками выполняемой работы занимается той же деятельностью.

С одной стороны, можно поприветствовать введение презумпции наличия трудовых отношений к любой человеческой деятельности, возлагая бремя доказывания обратного работодателя. Однако первый критерий кажется чересчур категоричным, поскольку любая деятельность, в том числе осуществляемая по гражданско-правовому договору, контролируется. Калифорнийский и европейский законодатель пытается сделать акцент на отсутствие такого признака как подчиненность, при этом полагаем, что контроль не включает подчиненность, поскольку контроль – одна из важнейших завершающих стадий любого предоставления работ, услуг и даже купли-продажи (подписание акта приема-передачи товара, в котором проверяется состояние передаваемого товара). С другой стороны, на принципала возлагается чрезмерно сложное бремя доказывания – доказать наличие трех критериев одновременно сложно; из всей массы атипичной работы можно исключить, пожалуй, только лиц, предоставляющих услуги «домашнего персонала» напрямую принципалу. Во всех остальных случаях работодателю проще изначально заключить трудовой договор и предусмотреть необходимые гарантии, на что, вероятно, и направлена воля законодателя штата Калифорния. Стоит также заметить, что социальные гарантии для работника в США гораздо более либе-

ральны, чем в странах ЕС: в США большинство гарантий определяются в трудовом договоре по соглашению с работодателем. Соответственно, обширная презумпция наличия трудовых отношений для ЕС не будет стимулировать принципалов к заключению трудовых договоров с каждым лицом, оказывающим хоть какие-то услуги: социальные гарантии могут оказаться неподъемными для бизнеса, что вынудит бизнес скрывать работающих лиц в юрисдикциях третьих стран.

Директива ЕС прямо затрагивает вопрос «посредников» при цифровых платформах и указывает, что лица, выполняющие работы на платформе, которые имеют договорные отношения с посредником, должны пользоваться тем же уровнем защиты, что и те, кто имеет прямые договорные отношения с цифровой платформой (ст. 3 директивы).

Особое внимание уделяется ограничениям на обработку персональных данных с помощью систем автоматизированного мониторинга или принятия решений: запрещено обрабатывать любые персональные данные лица, выполняющего работу на платформе, об эмоциональном или психологическом состоянии, сведения из частных разговоров, вне трудовой деятельности, о здоровье, политических взглядах, сексуальной ориентации. Также содержится общий запрет обработки любых биометрических данных. Лица, выполняющие работу на платформе, имеют право на переносимость персональных данных, полученных в результате выполнения ими работы в контексте автоматизированных систем мониторинга и принятия решений цифровой платформы труда, включая рейтинги и отзывы, без ущерба для прав получателя услуги в соответствии с Регламентом (ЕС) 2016/679 [6]. Цифровая платформа труда должна бесплатно предоставлять лицам, выполняющим работу на платформе, инструменты, способствующие эффективному осуществлению их прав на переносимость, упомянутых в ст. 20 Регламента (ЕС) 2016/679.

Очевидно, что каждая площадка устанавливает свою систему рейтинга и критерии оценки работы каждого специалиста, ввиду чего перенос таких сведений с одной платформы на другую с технической точки зрения вызовет множество вопросов.

Директива также обязывает платформы использовать человеческий фактор в процессе функционирования автоматизированной системы принятия решений. Так, цифровые платформы должны предоставить лицу, выполняющему работу на платформе, письменное изложение причин любого решения, поддержанного или, если применимо, принятого автоматизированной системой принятия решений, об ограничении, приостановке или прекращении действия учетной записи лица, выполняющего работу на платформе, любого решения об отказе в оплате работы, выполненной лицом, выполняющим работу на платформе, любого решения о контрактном статусе лица, выполняющего работу на платформе, любого решения с аналогичными последствиями или любого другого решения, затрагивающего существенные аспекты трудовых или иных договорных отношений, без неоправданной задержки и не позднее дня, когда оно вступает в силу.

ЕС обязывает цифровые площадки обеспечивать прозрачность своих автоматизированных систем не только перед работниками, но и перед компетентными государственными органами, уведомляя последних о характере, целях получения,

движении всех данных, получаемых посредством таких систем, производить оценку влияния обработки на защиту персональных данных лиц.

Примечательно, что платформы должны обеспечивать возможность для общения своих работников между собой в частном и безопасном ключе (ст. 20 директивы).

Заключение. Цифровизация стала актуальным и перспективным направлением в развитии ряда областей [10. С. 7].

В части взаимодействия с представительными органами работников директива не привносит ничего нового, обязанность участвовать во всех формах социального партнерства уже предусмотрена на уровне ЕС, и она распространяется также на цифровые платформы без исключения.

С учетом того, что соглашение по тексту директивы достигнуто, директива ожидает официального принятия со стороны Парламента и Совета, опубликования в официальном журнале ЕС, после чего у государств-членов возникнет обязанность по совершенствованию собственного законодательства во исполнение требований принятой директивы.

Список литературы

1. Электронная торговая площадка. – URL https://www.audit-it.ru/terms/agreements/elektronnaya_torgovaya_ploshchadka.html

2. Шевчук А. В. Роль цифровых трудовых платформ в трансформации занятости: экономико-социологический анализ: резюме дис. … д-ра социол. наук.

3. European Commission. COMMISSION STAFF WORKING DOCUMENT EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Directive of the European Parliament and of the Council On improving working conditions in platform work. Brussels, 09.12.2021. SWD (2021) 397 final.

4. Цветков В. В. Понятие «работник» в трудовом праве ЕС // Вопросы трудового права. – 2021. – № 9. – С. 666–671.

5. Jurisprudence of national Courts confronted with cases of alleged misclassification of platform workers: comparative analysis and tentative conclusions (Updated to 31 August 2022). Pp. 43–44. [Электронный ресурс]. – URL: https://ssrn.com/abstract=3839603 (дата обращения: 18.07.2023).

6. Proposal for the DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on improving working conditions in platform work Brussels, 8 March 2024 (OR. en) 7212/24 ADD 1, Interinstitutional File: 2021/0414(COD) https://data.consilium.europa.eu/doc/document/ST-7212-2024-ADD-1/en/pdf

7. Liboreiro J. EU deal on platform workers falls apart, pushing law into limbo // EuroNews (online). 2024, 16 February.

8. Labor Code of California state / California legislative information (USA). [Электронный ресурс]. – URL: https://leginfo.legislature.ca.gov/faces/codesTOCSelected.xhtml?tocCode=LAB&tocTitle=+Labor+Code+-+LAB (дата обращения: 16.08.2024).

9. О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных): регламент № 2016/679 Европейского

парламента и Совета Европейского Союза [рус., англ.] (Принят в Брюсселе 27.04.2016) // СПС КонсультантПлюс.

10. Бегишев И. Р., Жарова А. К., Громова Е. А., Залоило М. В., Филипова И. А., Шутова А. А. «Цифровой поворот» в правовых исследованиях // Journal of Digital Technologies and Law. – 2024. – № 2(1). – С. 7–13. – EDN: iwwubp. DOI: https://doi.org/10.21202/jdtl.2024.1

Д. К. Чугунов,
кандидат юридических наук,
заместитель управляющего директора по взаимодействию
с государственными органами ООО «Хэдхантер»,
ассистент,
Юридический институт,
Российский университет дружбы народов имени Патриса Лумумбы
С. Е. Шабронова,
старший юрист клиентской практики,
ООО «Хэдхантер»

ПОЛЬЗОВАТЕЛЬСКОЕ СОГЛАШЕНИЕ: МОЖЕТ ЛИ ПОЛЬЗОВАТЕЛЬ ЕГО ОСПОРИТЬ?

Аннотация. Цель статьи – выяснить природу пользовательского соглашения платформ, сайтов и может ли пользователь понудить площадку изменить его условия, каким образом складывается судебная практика в этом контексте. Сделаны выводы о том, что потребитель, группа лиц, Роспотребнадзор могут в суде обязать платформу внести изменения в пользовательское соглашение сайта и анонсировать это на всех пользователей. Авторы предостерегают платформы от размещения правил, которые не учитывают законодательство и ущемляют права пользователей, так как это влечет риск недействительности этих условий и взыскания морального вреда пользователем.

Ключевые слова: пользовательское соглашение, договор присоединения, смешанный договор, неравенство переговорных возможностей сторон, цифровые платформы, навязывание потребителям недопустимых условий договора, Закон о защите прав потребителей

USER AGREEMENT: CAN THE USER CHANGE IT

Abstract. The purpose of the article is to find out the nature of the user agreement of platforms, sites and whether the user can force the site to change its terms, how judicial practice develops in this context. The authors of the study concluded that the consumer, a group of individuals, and Rospotrebnadzor can in court oblige the platform to make changes to the user agreement of the site and announce this to all users. The authors warn the platforms against posting rules that do not take into account the legislation and infringe on the rights of users, as this entails the risk of invalidity of these conditions and the recovery of moral damage by the user.

Keywords: user agreement, accession agreement, mixed agreement, inequality of negotiation capabilities of the parties, digital platforms, imposition of unacceptable contract terms on consumers, Consumer protection law

Введение. Пользовательское соглашение – это документ, регулирующий отношения между администрацией сайта/платформы и пользователем. Законодательного термина нет, поименованной договорной конструкции для пользовательского соглашения нет. Правовое регулирование пользовательских соглашений происходит на двух уровнях:

А. Корпоративный уровень – обусловлен бизнес-моделью платформы (платформа для обмена сконцентрирована на сокращении транзакционных издержек пользователей (Яндекс.Такси, Wildberries, Авито, Profi.ru и др.), платформы для творчества (YouTube, Pinterest, Behance, VC.ru) сконцентрированы на инфраструктуре и распространении контента) и бизнес-процессами внутри компании платформы.

Б. «По аналогии закона» – применяются гражданско-правовые нормы, регулирующие схожие правовые отношения.

Основная часть. Из вышеизложенного можно сделать вывод, что в зависимости от самой платформы, сайта и сущности отношений с пользователем, а также услуг, сервисов, которые пользователь получает на такой платформе, сайте, пользовательское соглашение может иметь смешанный характер и включать в себя элементы как договора на оказание услуг, так и лицензионного договора.

Форма заключения пользовательского соглашения – публичная оферта, что позволяет сделать вывод, что большинство пользовательских соглашений крупных платформ, сайтов носят характер договора присоединения. Порядок заключения таких договоров регламентирован ст. 428 Гражданского кодекса Российской Федерации (далее – ГК РФ). В соответствии с данной нормой условия договора устанавливаются в одностороннем порядке администрацией сайта.

Что делать пользователю, если он считает, что его права нарушены: расторгнуть соглашение или обратиться в суд в связи с нарушением прав?

Если исходить из того, что пользовательское соглашение любой современной платформы имеет правовую природу договора присоединения, так как пользователь сайта в одностороннем порядке не может изменить условия и платформа не может для одного такого пользователя изменить условия работы сайта (только «на бумаге» может – вложить в личный кабинет пользователя индивидуальный текст пользовательского соглашения; изменить логику работы сайта для одного из пользователей не получится).

В соответствии со ст. 428 ГК РФ пользователь сайта как присоединившаяся сторона может направить свои обращения, предложения и претензии к администрации сайта. Часто встречающейся моделью отработки таких обращений является информация о том, что сайт работает по оферте, и если пользователь не согласен с ее условиями, то не должен использовать сайт, а так как платформа работает as is, т. е. как есть, без обработки жалоб на уровень сервиса платформы.

В случае недостижения согласия споры, связанные с исполнением гражданско-правового договора, разрешаются в судебном порядке по заявлению заинтере-

сованной стороны. Кроме того, указанной статьей предусмотрено право Пользователя на судебное обжалование спорных положений Пользовательского соглашения до заключения договора (как правило, до момента регистрации на сайте или в Сети).

Но на практике попытки пользователя понудить администрацию сайтов изменить спорные положения Пользовательского соглашения встречаются крайне редко. Пользователи обычно соглашаются с правилами пользования сервисами сайта.

Пунктами 1, 2 ст. 16 Закона Российской Федерации от 7 февраля 1992 г. № 2300-1 «О защите прав потребителей» (далее – Закон о защите прав потребителей) однозначно определено: любые договорные условия, ущемляющие права потребителя в сравнении с установленными законодательством нормами, являются недействительными.

Инициировать изменение пользовательского соглашения и признать условия пользовательского соглашения недействительным может пользователь, а также Роспотребнадзор.

Хочется обратить внимание платформ, сайтов, работающих с пользователями – физическими лицами на необходимость поддержки соответствия пользовательских соглашений, бизнес-процессов законодательству, а применительно к теме настоящей статьи – Закону о защите прав потребителей.

Поучительным является кейс с ООО «ВсеИнструменты.ру», где суд обязал платформу внести условия в пользовательское соглашение и привести к соответствию закону.

В пользовательском соглашении и общих условиях ООО «ВсеИнструменты.ру», на основании которых заключаются договоры с потребителями, было прописано право для администрации сайта не выполнять обязательства по договору публичной оферты в одностороннем порядке, при условии отсутствия необходимого количества заказанного товара либо нужной модели, возлагая на потребителя обязательства приобрести другой товар или аннулировать заказ.

В нарушение ст. 310 ГК РФ о недопустимости одностороннего отказа от исполнения обязательства ООО «ВсеИнструменты.ру» в условиях пользовательского соглашения, являющегося договором публичной оферты, закрепил себе такое право.

Суд пришел к выводу, что указанные условия договора ущемляют права потребителя, а платформа навязывает потребителям недопустимые условия договора. И обязал ООО «ВсеИнструменты.ру» привести условия Пользовательского соглашения в соответствии с требованиями Закона РФ, исключив возможность изменения продавцом условий соглашения в одностороннем порядке.

Также хочется отметить, что платформа, сайт в разрезе положений пользовательского соглашения может столкнуться со следующими рисками: отдельные положения соглашения просто не будут применяться исходя из их ничтожности.

Вывод: Пользовательское соглашение является договором присоединения, что ограничивает возможности пользователя влиять на его условия. Пользователь может оспорить или расторгнуть соглашение на основании ст. 428 ГК РФ и Закона

о защите прав потребителей. Условия соглашения, ущемляющие права потребителя, могут быть признаны недействительными. Судебная практика показывает редкие случаи успешного оспаривания пользовательских соглашений. Платформам рекомендуется поддерживать соответствие пользовательских соглашений действующему законодательству.

Список литературы

1. Гражданский кодекс Российской Федерации (часть вторая) от 26 января 1996 г. № 14-ФЗ (ред. от 28 декабря 2020 г.) // СЗ РФ. – 1996. – № 5. – Ст. 410.

2. О защите прав потребителей: Закон РФ от 07.02.1992 № 2300-1 (ред. от 08.08.2024) // РГ. – 1992, 7 апреля.

3. Апелляционное определение Московского городского суда от 06.07.2023 по делу № 33-28222/2023, 2-6310/2022.

4. Постановление Арбитражного суда Московского округа от 18.06.2015 № Ф05-7093/2015 по делу № А40-91072/14.

ЦИФРОВЫЕ ПРОДУКТЫ И СЕРВИСЫ: ПРАВОВЫЕ АСПЕКТЫ

Т. И. Минуллина,
руководитель,
Агентство инвестиционного развития Республики Татарстан,
заместитель Председателя Правления,
Национальная Ассоциация агентств инвестиций и развития
Р. Р. Хусяиншин,
директор,
Российский союз промышленников и предпринимателей
по региональному развитию,
исполнительный директор,
Национальная Ассоциация агентств инвестиций и развития
М. Г. Епифанцева,
заместитель руководителя,
Агентство инвестиционного развития Республики Татарстан

ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РАБОТЕ СПЕЦИАЛИЗИРОВАННЫХ ОРГАНИЗАЦИЙ ПО РАБОТЕ С ИНВЕСТОРАМИ В РОССИИ

Аннотация. Внедрение искусственного интеллекта уже является частью так называемой невидимой экономики в России в сфере услуг, и государственных, и частных: пользователям первыми отвечают чат-боты и автоответчики с искусственным интеллектом, и возможность поговорить с оператором-человеком уже стала больше исключением. В приложении «Госуслуги» при записи на подключение услуг связи, в банковских приложениях общение с человеком уже не воспринимается как необходимость. В то же время в кажущихся аналогичными сферах внедрение искусственного интеллекта еще даже не началось, например, во взаимодействии с предпринимателями, реализующими инвестиционные проекты. Вопрос необходимости внедрения искусственного интеллекта в специализированных организациях рассматривается в данной статье на основе изучения релевантной литературы по внедрению искусственного интеллекта и данных опроса специализированных организаций России. Внесены предложения по оценке стадии возможного внедрения искусственного интеллекта в специализированных организациях и возможному плану действий.

Ключевые слова: искусственный интеллект, специализированная организация по работе с инвесторами, информационные системы, социальные навыки, привлечение инвестиций, сопровождение инвесторов, улучшение инвестиционного климата

ISSUES OF USAGE OF THE ARTIFICIAL INTELLIGENCE IN THE WORK OF THE SPECIALIZED INVESTOR RELATIONS ORGANIZATIONS IN RUSSIA

Abstract. The introduction of artificial intelligence is already part of the so-called "invisible" economy in Russia in the service sector, both public and private: chatbots and answering machines with artificial intelligence are the first to respond to users, and the opportunity to talk to a human operator has already become an exception. In the application "Public Services", when signing up for connection of communication services, in banking applications, communication with a person is no longer perceived as a necessity. At the same time, in seemingly similar areas, the introduction of artificial intelligence has not even begun, for example, in interaction with entrepreneurs implementing investment projects. The issue of the need to introduce artificial intelligence in specialized organizations is considered in this article, based on the study of relevant literature on the implementation of artificial intelligence and survey data from specialized organizations in Russia. Proposals have been made to assess the stage of possible implementation of artificial intelligence in specialized organizations and a possible action plan.

Keywords: artificial intelligence, information systems, social skills, investments attraction, investor support, investor facilitation

Введение. В ноябре 2023 года был записан проморолик Международного форума «Россия – Китай – взаимовыгодное сотрудничество», в котором руководитель Агентства инвестиционного развития Республики Татарстан Талия Минуллина говорит на китайском языке [1]. Использование искусственного интеллекта (далее – ИИ) для создания маркетингового продукта помогло стать ближе к партнерам из КНР при отсутствии знания языка. В то же время следующим этапом может стать не только преодоление языкового барьера, но и разработка материалов с учетом особенностей аудитории, как их территория (что требует использования разных диалектов), профессия (что требует использования специализированных терминов) и других отличий. Например, в 2017 году во время поездки Президента США (Дональда Трампа) в Китай было выпущено его выступление с приветствием на китайском, как если бы он вырос в деревне неподалеку от Пекина. Предыдущий Президент США (Барак Обама) также получил запись пресс-конференции, на которой он говорил на идеальном мандаринском наречии, в свойственном ему «профессорском» стиле [3].

Основная часть. В 2023 году Всемирная ассоциация агентств инвестиционного развития провела опрос среди своих членов, в котором выяснила, как они справляются с вызовами, какие шаги предпринимают для привлечения инвестиций. Одним из исследуемых вопросов стало применение технологий ИИ [11]. Правительство Российской Федерации уже на ежегодной основе проводит опрос органов исполнительной власти субъектов Федерации и органов местного самоуправления о внедрении технологий искусственного интеллекта и эффективности их применения [9]. Все эти явления поднимают вопрос о необходимости использования ИИ в работе специализированных организаций по работе с инвестицион-

ными проектами (спецорганизаций). Фронт-офисы специализированных организаций по работе с инвестиционными проектами (уполномоченные для работы с инвесторами региональные агентства инвестиционного развития, корпорации развития, министерства экономики или инвестиций) выполняют похожие рутинные задачи, которые уже не только оцифрованы и автоматизированы, но и дополнены искусственным интеллектом в аналогичных операциях в коммерческой сфере, например, скоринг заявителя, экспертиза финансовых показателей и результативности проектов; «бэк-офисы» используют искусственный интеллект в инструментах для продвижения территории, в обучении сотрудников [10]. Но будет ли инвестор пользоваться чат-ботом на инвестиционном портале, вместо того чтобы позвонить в специализированную организацию, или примет решение на основе результатов калькулятора стоимости локализации проекта вместо того, чтобы обсудить это на офлайн-совещании с представителями специализированной организации?

Для оценки уровня внедрения ИИ в спецорганизациях России был проведен опрос через Национальную ассоциацию агентств инвестиций и развития, в которую на сегодняшний день входят 84 спецорганизации из 89 регионов России. До проведения опроса были сделаны гипотезы о том, что:

– практически все спецорганизации ИИ либо не используют, либо незначительно применяют его для разработки контента для продвижения;

– в спецорганизациях нет понимания необходимости применения ИИ, бюджета и кадровых ресурсов для его внедрения;

– применение ИИ изучается на основе технологий, имеющихся у бизнеса.

Ответы были получены от 31 спецорганизации, что в связи с их преимущественно однородным мандатом можно считать репрезентативной выборкой.

Ответы участников опроса показали следующие результаты.

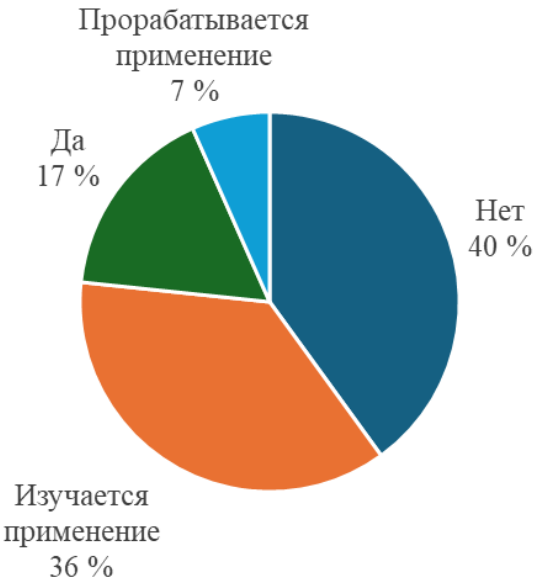

Рис 1. Использование искусственного интеллекта в спецорганизациях

Большинство спецорганизаций (70 %) не использует или только изучает применение ИИ (40 и 36 % соответственно). В то же время часть спецорганизаций уже начала прорабатывать этот вопрос (7 %). В спецорганизациях, ответивших на вопрос о применении ИИ положительно (17 %), его технологии используются только для разработки контента в популярных пользовательских программах и не используются для других процессов, таких как обработка данных, привлечение инвесторов, взаимодействие с ними.

В качестве причин, по которым ИИ не внедрен, спецорганизации отметили все из предложенных вариантов, среди которых: 1) высокая стоимость цифровых продуктов, 2) отсутствие квалифицированных сотрудников, 3) отсутствие предшествующего внедрению искусственного интеллекта уровня развития, 4) отсутствие поручений, курирующих работу органов власти. В то же время на вопрос «Если Вы не были бы ограничены в ресурсах, какие технологии ИИ Вы бы внедрили в деятельности спецорганизации?» все участники опроса ответили положительно и отметили необходимость в использовании ИИ для самых разных задач, таких как стратегического планирования, формирования кластеров и производственных цепочек, анализа финансового состояния компаний и таможенной статистики для определения целевых компаний для привлечения, работы с большими данными (например, анализа компаний на предмет готовности к инвестиционным проектам и др.), разработки типовых бизнес-процессов, аудита земельных участков, выявления инвестиционных ниш, подготовки информационных материалов (презентаций, коммерческих предложений), «умной» рассылки инвестиционных предложений, создания «умных» помощников для заполнения заявок от инвесторов по поданным в свободной форме заявлениям, планировки размещения инвестиционных объектов относительно имеющейся и планируемой инфраструктуры, расчета мер поддержки и подбора площадки для размещения проекта.

Проанализируем причины отсутствия использования ИИ в работе спецорганизаций.

В профессиональном стандарте «Специалист по работе с инвестиционными проектами» к необходимым знаниям в функции «Управление эффективностью инвестиционного проекта» включена работа в специализированных компьютерных программах для подготовки и реализации инвестиционного проекта [5]. К таким программам относятся те, в которых проводится расчет и сравнительный анализ инвестиционных проектов, например, COMFAR, Project Expert, «Альт-Инвест», «ИНЭК-Холдинг», «ТЭО-Инвест» [6]. Профессиональный стандарт специалиста по внедрению ИИ в бизнес был разработан только в начале 2024 года [7], но он еще не принят приказом Министерства труда и социальной защиты Российской Федерации, его текст не находится в открытом доступе в сети Интернет и к тому же является специальностью для отдельной штатной единицы, которая не заложена в штатное расписание не только спецорганизаций, но практически всех организаций, кроме тех, которые занимаются разработкой специализированных программ. Также зачастую в спецорганизациях нет и других специалистов для разработки или интеграции информационных систем, и компетенции работы с информационными технологиями являются приобретаемым навыком, чаще всего в практической деятельности без получения специализированного образования

или даже повышения квалификации. При внедрении информационных технологий стандартной практикой является привлечение подрядных организаций, стоимость услуг которых является на современном этапе развития технологий не только высокой, но и не предусматривается в бюджетах спецорганизаций.

Спецорганизации получат свое определение после принятия изменений в Федеральный закон от 25 февраля 1999 года № 39-ФЗ «Об инвестиционной деятельности в Российской Федерации, осуществляемой в форме капитальных вложений», в проекте которого предусматривается, что спецорганизации осуществляют следующие основные задачи:

– привлечение новых инвесторов;

– сопровождение инвестиционных проектов по принципу одного окна;

– реализация мероприятий, направленных на создание благоприятных условий для осуществления инвестиционной деятельности, осуществляемой в форме капитальных вложений;

– предоставление инвесторам информационно-консультационной поддержки при реализации инвестиционных проектов;

– ведение информационных ресурсов для субъектов инвестиционной деятельности на территории субъектов Российской Федерации;

– рассмотрение обращений инвесторов по вопросам реализации инвестиционных проектов в субъектах Российской Федерации;

– содействие инвесторам в подготовке проектной документации;

– организация и проведение региональных, межрегиональных и международных выставочно-ярмарочных, презентационных и конгрессных мероприятий в сфере инвестиционной деятельности, осуществляемой в форме капитальных вложений.

Эти функции на современном этапе функционирования спецорганизаций практически полностью оказываются предпринимателям, реализующим инвестиционные проекты, персонально, с поддержкой информационных систем взаимодействия с клиентами (CRM), без значительного уровня цифровизации и оказания услуг в электронном формате на всем «клиентском пути» инвестора. Бизнесмены в основном обращаются в спецорганизацию лично, через встречи с руководством и сотрудниками, подача заявки в электронном виде дублируется направлением заявки и сопроводительных документов в печатном виде с физической верификацией личной подписью и печатью организации. Вопрос внедрения ИИ в таком случае выглядит преждевременным, но в то же время заменит ли дальнейшее развитие цифровизации формат офлайн-взаимодействия?

Опыт внедрения ИИ уже показал, что люди предпочитают доступным услугам, даже быстрым и удобным, вызов клиентской службы, потому что им нужно с кем-нибудь поговорить. Даже «умная» машина неспособна к эмоциональному росту и не может открыть для себя ценности служения другим. Некоторые виды взаимодействия требуют человеческого общения, потому что оно помогает клиенту обрести спокойствие и нужный настрой [3].

Причина, по которой социальные навыки продолжают быть такими ценными, состоит в том, что большинство из нас не считают убедительными числа и алгоритмы как таковые. Гораздо больше впечатления производит хорошая исто-

рия или к месту рассказанный анекдот, а не таблица, полная статистически значимых данных. Люди хотят работать вместе и помогать друг другу, и их можно и нужно поощрять к этому [10].

На текущем этапе развития в человекоориентированных специальностях большая часть расчетов или физической работы уже может быть выполнена машинами, но важный фактор социального взаимодействия затрудняет автоматизацию. Если автоматизация этого сектора все-таки произойдет, то, вероятно, следующим образом: машины будут выполнять за кадром работы по оптимизации, а сотрудники-люди – выступать в качестве социального интерфейса для клиентов, что приведет к своеобразному симбиозу между человеком и машиной [3].

Так, в медицине сотрудник выслушивает заказчика, чтобы понять, чего тот желает, а затем предоставляет ему ответ или услугу. Современные технологии берут на себя вторую часть процедуры, потому что труднее автоматизировать не нахождение ответа, а первый этап – выслушать и понять [10].

По мере того как компьютеры все больше берут на себя рутину, людям следует заняться оценкой и вынесением суждений. «Реинжиниринг исключает не только непродуктивные затраты, но и работу, которая не добавляет ценности: большую часть проверок, сверок, ожиданий, отслеживаний… Исполнители должны думать, взаимодействовать, применять здравый смысл и действовать» [3].

Еще один вопрос – это подготовка специалистов спецорганизаций к работе с ИИ. Во многих областях в сфере рекламы и маркетинга, а также в управлении взаимоотношениями с клиентами (CRM) все чаще находят применение методы интеллектуального анализа данных. Располагая большим массивом данных, можно использовать его для анализа предпочтений целевой группы клиентов для дальнейшего оптимального размещения таргетированной рекламы. Использующиеся при этом методы должны быть применимы к очень большим объемам данных при разумных издержках [2]. Здесь кроется ответ еще на один вопрос об использовании ИИ в спецорганизациях: массивы данных не являются настолько «большими», чтобы внедрять ИИ. Например, агентство по привлечению инвестиций Коста-Рики использует ИИ для анализа эффективности инвестиционных проектов по 80 параметрам [11]. Агентство Коста-Рики – агентство целой страны, спецорганизации субъектов Российской Федерации работают только на региональном уровне. Анализ данных в российских спецорганизациях проводится вручную по меньшему в десятки раз количеству параметров, по значительно меньшему количеству проектов, входящими в пакет программ операционной системы офисными инструментами, а издержки на внедрение не то что ИИ, но и систем цифровизации деятельности на данный момент сравнимы с годовыми бюджетами спецорганизаций.

Кроме того, для большинства рядовых сотрудников подбор обучающих программ для получения квалификации по работе с ИИ является затруднительным [3]. Для них проблематично привыкать к новым программам, еще сложнее те из них, которые требуются для анализа и подготовки данных в необходимом для обработки ИИ формате под каждую задачу [2].

Личное общение представителей спецорганизаций с предпринимателями требует развитых навыков общения. Почему ИИ не может заменить на данном этапе развития «социальные навыки»: координирование, переговоры, убеждение

и восприимчивость? Среди них умение чувствовать эмоции и приоритеты людей и обеспечивать их совместную работу. Также с учетом сложности и быстрого изменения мироустройства, требуется постоянная координация действий, а этого не всегда можно добиться автоматическими обновлениями и разговорами равных с равными [10].

Еще одним отличием спецорганизаций от коммерческой деятельности, в которой вознаграждение сотрудника напрямую в денежном выражении зависит от извлекаемой прибыли, является редкое применение механизма материального поощрения в фиксированном проценте от реализованного инвестиционного проекта. Примером используемых в таком случае «социальных навыков», которые мотивируют команду спецорганизации к работе, может быть сравнение со спортом, где важнее всего в такой работе оказывается не умение научить команду выигрывать, а умение добиться, чтобы члены команды сработались и научились общими силами достигать цели, опираясь на способность сопереживать и гордость за победу [10].

С чего может спецорганизация начать внедрение ИИ в своей деятельности?

1. Описать и оценить рутинность бизнес-процессов, а также провести бенчмаркинг информационных систем с использованием ИИ для аналогичных процессов. Например:

a. В продвижении: подготовка аудио, видео, графических и текстовых материалов для контента, оценка присутствия в информационном поле, анализ присутствия конкурентов, написание статей и постов для социальных сетей, проведение рассылок.

b. В маркетинге: исследование групп целевых клиентов, формирование их портретов, прогнозирование их потребностей, разработка стратегий и шаблонов.

c. В принятии решений: расчет и сравнительный анализ инвестиционных проектов.

2. Оценить необходимость обучения кадров, подобрать подходящие курсы, разработать изменения в регламенты работы сотрудников с учетом применения технологий ИИ. Обучение в России можно получить на корпоративном обучении у лидеров отрасли из бизнеса, как Сбер [4], так и на курсах государственного цифрового университета «Университет 2035» [8].

Сеть Интернет предоставляет широкий набор как платных, так и бесплатных инструментов. Гипотезу о необходимости внедрения спецорганизация может опробовать в тестовом режиме перед выбором платного использования инструмента. Так, в 2023 году Агентством инвестиционного развития Республики Татарстан (далее – АИР РТ) был запущен чат-бот для онлайн-чата на Инвестиционном портале Республики Татарстан. Предоставляемый платформой «Битрикс» двухнедельный тестовый период использования штатного чат-бота его CRM показал, что 93 % пользователей портала не готовы были использовать этот инструмент и предпочитали общение с человеком, выбирая пункт меню по приглашению оператора. АИР РТ сделало вывод о незрелости спроса на машинный интерфейс поддержки принятия решений и не внедрило платную версию чат-бота после окончания тестового периода. В то же время в АИР РТ появилось понимание, что при повышении уровня цифровой зрелости целевой аудитории соответствующие инструменты необходимо будет внедрить. Это потребует отдельного изучения.

При использовании инструментов ИИ возникают и другие вопросы. Даже в таких продвинутых системах, как маркетплейсы или сервисы персональных рекомендаций ленты контента, предложения основаны на цифровых следах пользователя и зачастую повторяют то, на что пользователь уже удовлетворил потребность при поиске. Этим вопросом спецорганизациям придется задаться при разработке предложений по подбору объектов для размещения инвестиционных проектов или мер поддержки. Еще одной еще коллизией является использование контента, сформированного подрядчиками, коллегами или исполнителями в нерекомендованных органами власти зарубежных программах из недружественных стран: на текущем этапе развития государственной службы сотрудник органа власти не может оценить происхождение материалов и их соответствие требованиям информационной безопасности из программ, таких как популярный пользовательский продукт ChatGPT. Все спецорганизации образуются с государственным участием либо сами являются органами власти, поэтому проработка этого вопроса имеет существенный смысл для будущего использования инструментов ИИ при разработке контента.

Заключение. На основе развития ИИ в мире и в России вопрос использования ИИ в региональных спецорганизациях нашей страны представляется вопросом времени. Внедрение ИИ в «невидимую» экономику со стороны бизнеса обширно и постоянно углубляется, поэтому пользователи со временем будут ожидать привычных инструментов и уровня сервиса и от деятельности спецорганизаций. Применение рекомендаций по внедрению ИИ в инвестиционной сфере регионов России поможет подготовиться к достижению инвесторами «цифровой зрелости» в этом вопросе.

Список литературы

1. АИР РТ при помощи ИИ сняло ролик с Минуллиной, которая говорит на китайском языке // Бизнес Online [Электронный ресурс]. – URL: https://www.business-gazeta.ru/news/613376 (дата обращения: 15.07.2024).

2. Эртель В. Введение в искусственный интеллект. – М.: Эксмо, 2019.

3. Ли Кай-Фу. Сверхдержавы искусственного интеллекта. Китай, Кремниевая долина и новый мировой порядок. – 2-е изд. – М.: Манн, Иванов и Фербер, 2019.

4. Организация цифровой трансформации государственного управления с использованием механизма руководителей цифровой трансформации на примере Республики Татарстан // Международный форум KAZAN DIGITAL WEEK – 2022: сборник материалов / сост.: Р. Ш. Ахмадиева, Р. Н. Минниханов; под общ. ред. члена-корр. Академии наук Республики Татарстан, д-ра техн. наук, проф. Р. Н. Минниханова. – Казань: ГБУ «НЦБЖД», 2022. – Ч. 1. – С. 123–128.

5. Приказ Министерства труда и социальной защиты Российской Федерации от 16 апреля 2018 г. № 239н «Об утверждении профессионального стандарта «Специалист по работе с инвестиционными проектами» // СПС «ГАРАНТ» [Электронный ресурс]. – URL: https://base.garant.ru/71938730 (дата обращения: 15.07.2024).

6. Программные продукты для оценки эффективности инвестиционных проектов // Сайт компании «Альт-Инвест» [Электронный ресурс]. – URL:

https://www.alt-invest.ru/lib/programmnye-produkty-dlya-ocenki-effektivnosti-investicionnyx-proektov (дата обращения: 15.07.2024).

7. Разработан профстандарт для работы с ИИ // Сайт АНО «Национальное агентство развития квалификаций» [Электронный ресурс]. – URL: https://nark.ru/news/spk/razrabotan-profstandart-dlya-raboty-s-ii (дата обращения: 15.07.2024).

8. Сайт АНО «Университет Национальной технологической инициативы 2035» [Электронный ресурс]. – URL: https://www.2035.university (дата обращения: 15.07.2024).

9. Сайт Национального центра развития искусственного интеллекта при Правительстве Российской Федерации [Электронный ресурс]. – URL: https://ai-region2024.ru (дата обращения: 15.07.2024).

10. Макафи Э., Бриньолфсон Э. Машина, платформа, толпа. Наше цифровое будущее. – 2-е изд. – М.: Манн, Иванов и Фербер, 2019.

11. The new laws of FDI attraction. OCO Global WAIPA Innovation report 2023 // WAIPA website [Электронный ресурс]. – URL: https://waipa.org/waipa-content/uploads/OCO-Global-WAIPA-Innovation-Report-2023.pdf (дата обращения: 15.07.2024).

Д. А. Зубрик,
магистр,
Гродненский государственный университет
имени Янки Купалы

ИСПОЛЬЗОВАНИЕ ЧИТ-КОДОВ КАК НАРУШЕНИЕ ПРАВ ПОЛЬЗОВАТЕЛЕЙ ОНЛАЙН-ИГР

Аннотация. В статье анализируется использование чит-кодов в онлайн-играх. Приводятся примеры зарубежной правоприменительной практики относительно привлечения к ответственности за создание и распространение чит-кодов. Рассматриваются основания привлечения к ответственности за использование чит-кодов: на основе лицензионного соглашения и в рамках действующего белорусского законодательства. Ввиду отсутствия прямых норм в белорусском законодательстве приводится анализ смежных норм. В заключение приводятся доводы относительно актуальности и реальности привлечения субъектов права, выступающих в качестве пользователей онлайн-игр, к ответственности за использование чит-кодов.

Ключевые слова: чит-код, онлайн-игры, правовое регулирование, лицензионное соглашение, информационная сеть, компьютерные игры, пользователи, ответственность

THE USAGE OF CHEAT CODES AS A VIOLATION OF THE RIGHTS OF USERS OF ONLINE GAMES

Abstract. The article is analyzed the use of cheat codes in online games. Examples of foreign law enforcement practice regarding prosecution for the creation

and distribution of cheats are given. The grounds for bringing responsibility for using cheats are considered: based on an End-user license agreement and within the current Belarusian legislation. Due to a lack of direct provisions in Belarusian law, an analysis is provided of related provisions. In conclusion, arguments are provided regarding the relevance and feasibility of bringing legal entities that act as users of online games to justice for using cheats.

Keywords: cheat code, online games, legal regulation, End-user license agreement, information network, computer games, users, responsibility

Введение. Игровая индустрия является важной частью современной культуры. Сотни пользователей ежедневно создают аккаунты в онлайн-играх, где существует возможность взаимодействия с другими игроками. Как правило, в онлайн-играх необходимо получать различные достижения для дальнейшего продвижения. Однако некоторые пользователи прибегают к использованию чит-кодов для упрощения игры.

Чит-коды представляют собой специальные команды (числовые или текстовые), которые необходимо ввести игроку для получения требуемых достижений или преимуществ. Ряд чит-кодов нацелены на быстрое прохождение уровня или получение дополнительных ресурсов. Такое использование специальных команд является несправедливым по отношению к другим пользователям, поскольку создается неравенство в сетевой игре. В связи с этим необходимо определить, каким образом следует привлекать к юридической ответственности игроков, прибегающих к использованию чит-кодов, тем самым нарушая права других пользователей онлайн-игры.

Основная часть. 6 июля 2022 года в Екатеринбуге был вынесен обвинительный приговор в отношении Андрея Кирсанова. Последний был приговорен к двум с половиной годам ограничения свободы. Уголовное дело в отношении А. Кирсанова было возбуждено еще весной 2021 года по части второй статьи 273 Уголовного кодекса РФ («Создание и распространение вредоносных компьютерных программ»). А. Кирсанов обвинялся в том, что создал сайт по продаже чит-кодов для игр World of Tanks и World of Warships. В данном уголовном деле потерпевшей стороной выступила компания Wargaming, так как продаваемые чит-коды создавали преимущество перед другими игроками, что нарушало равенство. Было установлено, что Кирсанов занимался продажей чит-кодов с 2014 года. Ущерб, причиненный компании Wargaming, оценивается в 670 млн рублей [1].

Также в июле 2023 года в Шанхае были арестованы несколько человек по подозрению создании чит-кодов для онлайн-игры Genshin Impact. Сами разработчики игры указали, что в дальнейшем будут упорнее бороться с подобными незаконными проявлениями. Более того, разработчики напомнили, что это не первый арест по подозрению в создании чит-кодов: в предыдущий раз создателям чит-кодов назначили тюремный срок и штраф в размере $16,3 тыс. [2].

29 мая 2024 года стало известно, что Activision одержала вторую победу в судебном деле против EngineOwning, разработчика читов для Call of Duty. Изначально исковые требования были предъявлены только к компании EngineOwning, однако в 2022 году исковые требования были также предъявлены к ряду других

компаний, занимающихся продажей чит-кодов. Но после второго судебного заседания суд обязал нескольких ответчиков (в том числе и компанию EngineOwning) выплатить денежную компенсацию Activision, составляющую $14,5 млн. В судебном решении также было определена обязанность EngineOwning прекратить деятельность по созданию и распространению чит-кодов и при этом передать свой сайт в собственность Activision. Более того, EngineOwning обязана покрыть расходы компании Activision на адвокатов (общая сумма расходов составляет $292,9 тыс.) [3].

Как мы видим, на данный момент существует практика привлечения к ответственности за создание и распространение чит-кодов. Однако можем ли мы привлекать к ответственности лиц, использующих чит-коды для упрощения получения достижений в онлайн-играх?

Необходимо подчеркнуть, что у каждой игровой компании существует лицензионное соглашение, или EULA (End-user license agreement). В рамках соглашения указываются правила пользования и условия игры. То есть можно сказать, что лицензионное соглашение – это договор, в котором предоставляются права на пользование игровой продукцией компании. Также в рамках лицензионного соглашения может предусматриваться ответственность за использование чит-кодов в онлайн-игре. Как правило, используется блокировка, бан, ограничение по пользованию или удаление аккаунта в отношении тех пользователей, которые применили чит-код. Однако в рамках предупреждения совершения незаконных действий может применяться предупреждение.

Рассмотрим для примера лицензионное соглашение от компании Wargaming. Раздел 12 лицензионного соглашения содержит в себе Кодекс поведения пользователей игры. Так, п. 12.1 предусматривает запрет на создание, использование, предоставление, распространение неавторизованных программ или инструментов. Сюда также относится использование различных инструментов (хаки, читы, эксплойты, скрипты, боты, тренеры, программы автоматизации и др.), направленных на взаимодействие с продуктом Wargaming любым способом и в любых целях: 1) перехват информации; 2) имитация информации; 3) перенаправление коммуникации; 4) искажение информации о месте нахождения пользователя для получения выгоды. Если будет установлено, что такое использование было, то Wargaming, согласно разделу 19 лицензионного соглашения, имеет право: 1) на определенное время или навсегда ограничить доступ к некоторым функциям: 2) на определенное время или навсегда ограничить доступ к учетной записи; 3) на определенное время или навсегда ограничить доступ к некоторым продуктам; 4) расторгнуть лицензионное соглашение и удалить учетную запись пользователя [4]. Можно сказать, что Wargaming достаточно строго относится к тем пользователям, которые используют чит-коды в онлайн-игре. Однако в рамках лицензионного соглашения также присутствует раздел 20, который регламентирует применимое законодательство при выявлении нарушений. Такое введение позволяет не только урегулировать правоотношения пользователей локально в онлайн-игре, но и учитывать особенности правовой системы каждого пользователя.

Действительно, принятие лицензионных соглашений значительно упрощает правовое регулирование. Однако необходимо учитывать также и особенно-

сти законодательства конкретной страны. Ниже будут рассмотрены нормы из белорусского законодательства, которые могли бы регулировать ответственность за использование чит-кодов в онлайн-играх.

Необходимо указать, что онлайн-игры строятся на сетевой архитектуре. Сетевые архитектуры бывают двух видов: 1) peer-to-peer (передача данных осуществляется между подключенными игроками); 2) клиент-серверная (передача данных осуществляется исключительно только между игроком и сервером). Также необходимо выделить основные компоненты сетевых игр: 1) транспортный протокол – содержит в себе порядок передачи информации между игроками и сервером; 2) протокол приложения – отражает передачу информации от игрока к серверу и наоборот; 3) логика приложения – охватывает правила использования полученных данных [5]. В связи с этим возникает вопрос: можем ли мы говорить, что онлайн-игры – это информационная сеть?

В Законе Республики Беларусь «Об информации, информатизации и защите информации» от 10 ноября 2008 г. № 455-З (далее – Закон) указано, что информационная сеть – совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих посредством сетей электросвязи. В то же время под информационной системой подразумевается совокупность банков данных [6]. Так как онлайн-игры содержат в себе банки данных пользователей, программ и иной информации, можно сказать, что каждая онлайн-игра содержит в себе информационную систему. Более того, таких информационных систем может быть множество (например, протоколы сетевых игр), поэтому каждая онлайн-игра является информационной сетью. Ко всему этому, пользователи могут взаимодействовать друг с другом в режиме реального времени, что также характерно для информационной сети.

Следует указать, что если признавать онлайн-игру информационной сетью, то игроки выступают в качестве пользователей информационной сети. Необходимо отметить, что в Законе определены права пользователей информационной сети: 1) использование информационной сети для доступа к информационным ресурсам; 2) получение, распространение и предоставление информации, полученной от информационной сети. Также в Законе определены обязанности пользователей информационной сети: 1) соблюдение прав других лиц при использовании информационной сети; 2) соблюдение действующего законодательства [6]. Можно сказать, что обязанность по соблюдению прав других лиц при использовании информационной сети является отражением нормы из лицензионного соглашения онлайн-игр, где пользователи должны соблюдать права других игроков и не использовать различные модификации для получения преимущества. Более того, за использование подобных модификаций в отношении такого лица применяются различные санкции (бан, удаление аккаунта, ограничение по функционалу и др.). Также следует подчеркнуть, что права и обязанности пользователей информационных систем коррелируются с нормами из лицензионного соглашения, что еще больше подчеркивает тезис о том, что онлайн-игра – это информационная сеть.

Следует указать, что прямой нормы, определяющей ответственность пользователя онлайн-игры, использующего чит-коды, нет. Несмотря на это, существуют смежные нормы, которые могут быть использованы при квалификации деяния.

Необходимо подчеркнуть, что онлайн-игры являются компьютерными программами. Поэтому при правовой регламентации использования чит-кодов в онлайн-играх требуется обратиться к Закону Республики Беларусь «Об авторском праве и смежных правах» от 17 мая 2011 г. № 262-З (далее – Закон об авторском праве). Деятельность пользователей онлайн-игр регулируется ч. 3 ст. 13 Закона об авторском праве, в которой определено, что лицо, правомерно владеющее экземпляром компьютерной программы, имеет право на использование такой программы по ее прямому назначению. Сюда также включается деятельность по установке программы на компьютер или иное устройство, запуску и работе с программой (т. е. использование заложенного функционала) на тех условиях, которые были определены автором или иным правообладателем [7]. Таким образом, мы можем сделать вывод, что указанная норма определяет порядок пользования онлайн-игрой по ее прямому назначению. Из этого следует, что пользователь может осуществлять свою деятельность в онлайн-игре исключительно только на основе норм и принципов, заложенных в лицензионном соглашении.

Использование чит-кода также подразумевает внесение изменений в код игры для получения конкретных благ. Статья 39 Закона об авторском праве определяет порядок свободного пользования компьютерными программами и базами данных. Устанавливается, что если лицо правомерно владеет экземпляром компьютерной программы, то оно [лицо] имеет право на адаптацию программы без изменений исходного кода или с внесением изменений при условии, что код находился в открытом доступе либо же лицу было предоставлено такое право [7]. Из этого следует, что если в лицензионном соглашении было отражено, что пользователь может применять чит-коды, либо же такая деятельность была разрешена на основе других локальных документов, то такое использование является правомерным. Если же такое разрешение отсутствует, то применение чит-кодов является нарушением порядка функционирования онлайн-игры и нарушает авторские права игровой компании.

В свою очередь, следует указать, что в ч. 1 ст. 55 Закона об авторском праве установлено, что нарушением авторского или смежного права являются любые действия, противоречащие нормам законодательства об авторском праве [7]. Поэтому, если игровая компания рассмотрит в действиях пользователя нарушение авторского права (под действиями рассматривается использование чит-кодов), то такая компания имеет право подать исковое заявление с требованием о возмещении причиненных убытков.

Рассмотрим уголовную ответственность за использование чит-кодов. При анализе правоприменительной практики было выявлено, что на данный момент лица привлекаются к ответственности за создание и распространение чит-кодов. К примеру, в Российской Федерации ответственность наступает по ст. 273 Уголовного кодекса Российской Федерации. В белорусском законодательстве предусмотрена ответственность за подобное деяние по ст. 354 Уголовного кодекса Республики Беларусь (далее – УК). В ч. 1 ст. 354 УК указано, что разработка, использование, распространение либо сбыт компьютерной программы или специального программного или аппаратного средства, заведомо предназначенных для нарушения системы защиты, несанкционированного доступа к компьютерной системе,

сети или машинному носителю, несанкционированного уничтожения, блокирования, модификации компьютерной информации или неправомерного завладения компьютерной информацией либо нарушения работы компьютерной системы, сети или машинного носителя, наказываются штрафом, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок [8]. Действительно, чит-код нарушает последовательность получения достижений, тем самым облегчая саму игру. Однако мы не можем сказать, что чит-код является компьютерной программой, поскольку чит-код – это набор чисел или букв, который вносится в саму игру (т. е. введение конкретной команды на что-то). Из этого следует, что сейчас привлекать к уголовной ответственности за использование чит-кода в онлайн-игре не представляется возможным. Более того, трудностью в определении квалификации является и тот факт, что в Республике Беларусь на данный момент отсутствует правоприменительная практика по данному вопросу.

Заключение. Таким образом, можно сделать вывод, что на данный момент в белорусском законодательстве отсутствуют прямые нормы, регулирующие ответственность за нарушение прав пользователей онлайн-игр посредством использования чит-кодов. Однако анализ действующего законодательства показал, что такое лицо можно привлечь к ответственности на основании смежных норм. Но, с нашей точки зрения, такое привлечение не является актуальным, поскольку при регистрации в онлайн-игре каждый пользователь подписывает лицензионное соглашение, в котором указана ответственность за использование чит-кодов. При этом не исключается возможность игровой компании направить исковые требования о получении возмещения убытков, причиненных использованием чит-кодов.

Список литературы

1. Главные юридические конфликты в игровой индустрии (июль – декабрь 2022) // App2Top [Электронный ресурс]. – URL: https://app2top.ru/pravo/glavny-e-yuridicheskie-konflikty-v-igrovoj-industrii-iyul-dekabr-2022-205348.html (дата обращения: 15.07.2024).

2. В Китае арестовали создателей читов для Genshin Impact // Хабр [Электронный ресурс]. – URL: https://habr.com/ru/news/750080 (дата обращения: 15.07.2024).

3. Activision получила $14,5 млн от создателей читов для Call of Duty // Хабр [Электронный ресурс]. – URL: https://habr.com/ru/news/818161 (дата обращения: 15.07.2024).

4. Лицензионное соглашение Wargaming.net // Wargaming.net. [Электронный ресурс] – URL: https://legal.eu.wargaming.net/ru/eula (дата обращения: 15.07.2024).

5. О сетевой модели в играх для начинающих // Хабр [Электронный ресурс]. – URL: https://habr.com/ru/articles/467025 (дата обращения: 15.07.2024).

6. Об информации, информатизации и защите информации: Закон Респ. Беларусь, 10 ноября 2008 г. № 455-З // ЭТАЛОН. Законодательство Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

7. Об авторском праве и смежных правах: Закон Респ. Беларусь, 17 мая 2011 г. № 262-З // ЭТАЛОН. Законодательство Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

8. Уголовный кодекс Республики Беларусь: 9 июля 1999 г., № 275-З: принят Палатой представителей 2 июня 1999 года г.: одобр. Советом Респ. 24 июня 1999 года г.: в ред. Закона Респ. Беларусь от 08.07.2024 г. // ЭТАЛОН. Законодательство Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

М. Ю. Осипов,
кандидат юридических наук,
Международная полицейская академия ВПА

К ВОПРОСУ ОБ ОСОБЕННОСТЯХ ПРОЕКТИРОВАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ДЛЯ ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Статья посвящена особенностям проектирования автоматизированных систем управления для юридической деятельности. Предметом исследования, результаты которого изложены в настоящей статье, выступают особенности и закономерности проектирования автоматизированных систем управления для юридической деятельности. Цель исследования заключается в том, чтобы рассмотреть особенности и закономерности проектирования автоматизированных систем управления для юридической деятельности. К числу методов исследования, при помощи которых были получены результаты, изложенные в настоящей статье, можно отнести общенаучные методы: анализ, синтез, индукцию, дедукцию, абстрагирование, обобщение, моделирование. В ходе исследования было установлено, что процесс проектирования автоматизированных систем управления для юридической деятельности включает в себя несколько этапов: 1) осуществление реинжиниринга юридической деятельности с целью выделения в ней ключевых моментов; 2) определение того, какие ключевые моменты юридической деятельности подлежат автоматизации; 3) определение платформы для осуществления автоматизации юридической деятельности; 4) создание автоматизированных систем управления юридической деятельностью. Также в статье рассмотрены факторы, влияющие на особенности протекания каждого этапа проектирования автоматизированных систем управления для юридической деятельности.

Ключевые слова: право, цифровые технологии, автоматизированные системы управления, юридическая деятельность, этапы, факторы, проектирование

ON THE QUESTION OF THE FEATURES OF DESIGNING AUTOMATED CONTROL SYSTEMS FOR LEGAL ACTIVITIES

Abstract. The article is devoted to the features of designing automated control systems for legal activities. The subject of the study, the results of which are presented in this article, are the features and patterns of designing automated control systems for legal activities. The purpose of the study is to consider the features and patterns of designing automated control systems for legal activities. The research methods by which the results presented in this article were obtained include general scientific methods: analysis, synthesis, induction, deduction, abstraction, generalization,

modeling. In the course of the study, it was found that the process of designing automated control systems for legal activities includes several stages: 1) reengineering of legal activities in order to highlight key points in it; 2) determining which key points of legal activity are subject to automation; 3) determining a platform for the automation of legal activities; 4) creating automated systems for managing legal activities. The article also considers the factors influencing the features of each stage of designing automated control systems for legal activities.

Keywords: law, digital technologies, automated control systems, legal activity, stages, factors, design

Введение. Проблема проектирования автоматизированных систем управления для юридической деятельности – это одна из актуальных проблем, стоящих перед современной юридической наукой. Исследованию данной проблемы посвящен целый ряд работ [1. С. 109–112; 2. С. 24–28; 3. С. 394–402; 4. С. 238–241; 5. С. 117–146; 6. С. 155–167].

В указанных работах рассматриваются различные аспекты использования автоматизированных систем для юридической деятельности. Так, в работе Т. В. Савиной, Е. М. Филипповой рассматриваются особенности «автоматизации юридической деятельности в части работы портала государственных услуг» [4. С. 238–241].

В работе, подготовленной коллективом авторов под редакцией В. А. Погонышева, рассматриваются «особенности и возможности различных IT решений, для осуществления юридической деятельности» [2. С. 24–28]. В работе А. А. Котова рассматриваются «особенности автоматизации обработки юридических документов, задачи автоматизации и возможные IT-решения, для осуществления каждой из задач автоматизации» [3. С. 394–402]. В работе D. Barysė, R. Sarel рассматриваются «особенности и проблемы применения технологий искусственного интеллекта при осуществлении правосудия и проблемы, связанные с этим» [5. С. 117–146]. В работе H. Hirvonen «рассматриваются проблемы правового регулирования автоматизации процессов принятия правовых решений, включая технологии искусственного интеллекта» [6. С. 155–167]. В работе В. А. Варламова и С. В. Местникова «рассматриваются особенности проектирования приложений для автоматизации учета договоров и юридической деятельности» [1. С. 109–112], однако каких-либо примеров разработки и функционирования данных приложения с выделением основных этапов разработки данных приложений в указанной работе не приведено [1. С. 109–112]. Таким образом, анализ литературы показывает наличие проблемы определения особенностей и закономерностей проектирования автоматизированных систем управления для юридической деятельности, включая определение основных этапов проектирования автоматизированных систем управления для юридической деятельности, особенностей протекания данных этапов; определение основных факторов, влияющих на процесс проектирования автоматизированных систем управления, для юридической деятельности.

Основная часть. Основные этапы проектирования автоматизированных систем управления для юридической деятельности.

Прежде чем начинать проектирование автоматизированных систем управления юридической деятельностью представляется очень важным понять, какие виды

юридической деятельности или отдельные аспекты юридической деятельности подлежат автоматизации и почему именно они подлежат автоматизации. Необходимость ответа на данный вопрос представляется очень важной, поскольку различные виды юридической деятельности имеют свои специфические ключевые моменты, от специфики которых зависит специфика автоматизации юридической деятельности.

Так, например если необходимо осуществлять автоматизацию учета изменений в действующее законодательство, ключевыми моментами такого вида деятельности будут: 1) факт изменений в действующее законодательство; 2) содержание изменений в действующее законодательство; 3) правовые последствия изменений в действующее законодательство.

Если же надо оценить качество того или иного вида юридической деятельности, то ключевыми моментами в данном случае будут следующие: 1) перечень требований, которые предъявляются к тем или иным видам юридической деятельности; 2) вопросы, которые позволяют проверить соблюдение или несоблюдение этих требований при осуществлении того или иного вида юридической деятельности, 3) типы возможных ошибок при осуществлении того или иного вида юридической деятельности или отдельных его аспектов; 4) число несоблюдения требований, предъявляемых к тому или иному виду юридической деятельности; 5) причины и условия, приведшие к несоблюдению тех или иных требований при осуществлении юридической деятельности; 6) возможные мероприятия, направленные на устранение ошибок при осуществлении юридической деятельности.

Когда необходимо автоматизировать составление процессуальных документов (искового заявления, апелляционной, кассационной и надзорной жалобы), ключевыми моментами в данном случае будут: наличие обязательных предусмотренных в законодательстве реквизитов указанных процессуальных документов и приложений к ним.

Для проведения автоматического анализа обращений в суд ключевыми моментами при автоматизации подобного рода юридической деятельности будут: 1) вид спора; 2) факт обращения в суд; 3) стадия процесса по рассмотрению данного обращения; 4) результат рассмотрения данного обращения; 5) причины и условия вынесения судом того или иного решения по результатам обращения.

Если необходимо осуществлять учет правонарушений в течение года в организации, то ключевыми моментами при осуществлении подобного рода деятельности будут являться: 1) отчетный год; 2) правовые основания для привлечения организации к ответственности; 3) причины и условия совершения организацией правонарушения; 4) вид правонарушения организацией; 5) величина наложенных на организацию имущественных санкций.

Когда нужно осуществить автоматизированный учет договоров и их исполнения, ключевыми моментами будут: 1) контрагенты по договору; 2) вид и предмет договора; 3) права и обязанности сторон договора; 4) возможные правовые последствия неисполнения тех или иных пунктов договора; 5) число договоров, исполненных ненадлежащим образом; 6) цена договора; 7) перечень возможных доказательств, подтверждающих ненадлежащее исполнение по данному договору; 8) наличие у организации доказательств, подтверждающих ненадлежащее исполнение по данному договору.

Если, к примеру, необходимо выполнить автоматизированную оценку соблюдения организацией установленных законодательных требований, тогда ключевыми

моментами для автоматизации подобного рода деятельности будут: 1) перечень законодательных требований и их содержание; 2) соответствие деятельности организации данным требованиям; 3) перечень мероприятий, необходимых для оценки соответствия деятельности организации законодательным требованиям; 4) стоимость данных мероприятий; 5) оценка результативности данных мероприятий.

При осуществлении учета локальных правовых актов ключевыми моментами для осуществления автоматизации подобного рода деятельности будут: 1) вид локального правового акта; 2) дата принятия локального правового акта; 3) предмет регулирования данного локального правового акта; 4) соответствие данного локального правового акта законодательным требованиям и т. д.

Таким образом, первым этапом проектирования автоматизированных систем управления для юридической деятельности будет: осуществление реинжиниринга юридической деятельности с целью выделения в ней ключевых моментов.

После того как виды юридической деятельности, подлежащие автоматизации, и ключевые моменты этой деятельности были определены, наступает второй этап проектирования автоматизированных систем для юридической деятельности, который состоит в определении тех ключевых моментов в этих видах деятельности, которые подлежат автоматизации.

Этот этап представляется очень важным, поскольку, если, к примеру, не все ключевые моменты того или иного вида юридической деятельности будут подлежать автоматизации, это приведет к снижению эффективности функционирования автоматизированных систем управления юридической деятельностью, поскольку потребует внесения изменений и дополнений в автоматизированную систему управления юридической деятельностью, что в ряде случаев не всегда возможно.

Третьим этапом проектирования автоматизированных систем управления для юридической деятельности является выбор платформы для осуществления автоматизации управления юридической деятельностью. При выборе платформы для автоматизации управления юридической деятельностью необходимо исходить из того, что данная платформа имеет встроенные механизмы учета ключевых моментов юридической деятельности, которые могут быть легко заданы разработчиком данной системы, при этом стоимость данной платформы должна быть приемлемой для большинства разработчиков автоматизированных систем управления юридической деятельностью и не должна предусматривать глубокого знания разработчиком различных языков программирования, что позволяет достаточно быстро разрабатывать подобного рода системы.

По нашему мнению, наиболее оптимальной платформой для разработки подобного рода автоматизированных систем управления юридической деятельностью выступает платформа 1С предприятие 8.3. Она позволяет осуществлять учет ключевых моментов юридической деятельности благодаря встроенным в нее объектам конфигурации: справочникам, документам, регистрам накопления, регистрам сведений, отчетам, в которых будут находить свое отражение те или иные ключевые моменты юридической деятельности. Поэтому никак нельзя согласиться с выводами некоторых авторов о том, что система 1С предприятие «может быть неэффективна для небольших компаний и индивидуальных юристов» [1. С. 111], поскольку данная платформа позволяет разрабатывать решения в сфере автоматизации управления юридической деятельностью вне зависимости от масштаба данной деятельности.

Последним этапом проектирования автоматизированных систем управления юридической деятельностью выступает этап непосредственного проектирования автоматизированных систем управления юридической деятельностью. В ходе данного этапа определяются и закладываются все необходимые справочники, регистры сведений, документы и отчеты, необходимые для осуществления автоматизации юридической деятельности, что позволяет осуществлять ее автоматизацию.

Далее рассмотрим основные ошибки, возникающие при осуществлении проектирования автоматизированных систем управления для юридической деятельности и пути их профилактики.

Основные ошибки, возникающие при осуществлении проектирования автоматизированных систем управления для юридической деятельности, и пути их профилактики: а) неверное определение видов юридической деятельности, которые подлежат автоматизации; б) неверное определение ключевых моментов тех или иных видов деятельности, которые подлежат автоматизации; в) неправильное определение платформы, которая используется для осуществления автоматизации тех или иных видов юридической деятельности; г) технологические ошибки при осуществлении проектирования автоматизированных систем управления юридической деятельностью. Для профилактики подобного рода ошибок необходимо осуществить целый ряд действий, перечень которых приведен в следующей таблице.

Таблица 1

Алгоритм профилактики ошибок при осуществлении проектирования автоматизированных систем управления для юридической деятельности

Вопрос	**Возможные варианты ответа**	**Необходимые действия при положительном ответе**	**Необходимые действия при отрицательном ответе**
Определены ли виды юридической деятельности, подлежащие автоматизации	Да, определены	Можно приступать к следующему шагу	Необходимо определить виды деятельности, подлежащие автоматизации
	Нет, не определены		
Определены ли ключевые моменты юридической деятельности, подлежащие автоматизации	Да, определены	Можно приступать к следующему шагу	Необходимо определить ключевые моменты юридической деятельности, подлежащие автоматизации
	Нет, не определены		
Определена ли платформа, на которой будет осуществляться автоматизация юридической деятельности	Да, определена	Можно приступать к следующему шагу	Необходимо определить платформу, на которой будет осуществлена автоматизация юридической деятельности
	Нет, не определена		
Правильно ли осуществлено проектирование автоматизированной системы управления юридической деятельностью, нет ли технических ошибок	Да, правильно	Можно приступать к работам по внедрению	Необходимо провести тестирование разработанной конфигурации на предмет выявления технических ошибок, а также работы по их устранению
	Нет, неправильно, есть технические ошибки		

Далее рассмотрим основные факторы, влияющие на процесс проектирования автоматизированных систем управления для юридической деятельности.

Основные факторы, влияющие на процесс проектирования автоматизированных систем управления для юридической деятельности.

Под основными факторами, влияющими на процесс проектирования автоматизированных систем управления юридической деятельностью, автором статьи понимаются обстоятельства, которые влияют на процесс проектирования автоматизированных систем управления юридической деятельностью.

К числу этих факторов можно, в частности, отнести следующие факторы:

1. Степень понимания того, какие виды юридической деятельности подлежат автоматизации и каковы их ключевые моменты.

2. Степень понимания того, какие ключевые моменты юридической деятельности подлежат учету в автоматизированных системах управления юридической деятельностью.

3. Степень понимания возможностей тех или иных платформ, на которых осуществляется проектирование автоматизированных систем управления юридической деятельностью.

4. Наличие умения проектировать автоматизированные системы управления юридической деятельностью на указанных платформах.

5. Умение выявлять и справлять ошибки при проектировании автоматизированных систем управления юридической деятельностью на указанных платформах.

Заключение

1. Процесс проектирования автоматизированных систем управления для юридической деятельности включает в себя несколько этапов: 1) осуществление реинжиниринга юридической деятельности с целью выделения в ней ключевых моментов; 2) определение того, какие ключевые моменты юридической деятельности подлежат автоматизации; 3) определение платформы для осуществления автоматизации юридической деятельности; 4) создание автоматизированных систем управления юридической деятельностью.

2. К числу основных ошибок, возникающих при осуществлении проектирования автоматизированных систем управления для юридической деятельности можно отнести следующие ошибки: а) неверное определение видов юридической деятельности, которые подлежат автоматизации; б) неверное определение ключевых моментов тех или иных видов деятельности, которые подлежат автоматизации; в) неправильное определение платформы, которая используется для осуществления автоматизации тех или иных видов юридической деятельности; г) технологические ошибки при осуществлении проектирования автоматизированных систем управления юридической деятельностью. Для профилактики подобного рода ошибок необходимо использовать определенный алгоритм, указанный в данной статье.

3. Под основными факторами, влияющими на процесс проектирования автоматизированных систем управления юридической деятельностью, автором статьи понимаются обстоятельства, которые влияют на процесс проектирования автоматизированных систем управления юридической деятельностью.

Таковы, по нашему мнению, особенности и проблемы проектирования автоматизированных систем управления для юридической деятельности.

Список литературы

1. 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-2024»: материалы Всероссийской студенческой научно-практической конференции с международным участием, Якутск, 22–23 марта 2024 г. – Ульяновск: ИП Кеньшенская Виктория Валерьевна (издательство «Зебра»), 2024. – С. 109–112. – EDN: WONLBK

2. Вопросы автоматизации юридической деятельности / В. А. Погонышев, Д. А. Погонышева, Т. М. Хвостенко [и др.] // Вестник образовательного консорциума Среднерусский университет. Информационные технологии. – 2020. – № 2(16). – С. 24–28. – EDN: MUHQWQ

3. 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. – EDN: ZULBYJ. – DOI: 10.52575/2687-0932-2022-49-2-394-402

4. Савина Т. В., Филиппова Е. М. Автоматизация юридической деятельности: портал государственных услуг Российской Федерации // Актуальные социально-экономические проблемы развития общества в России и за рубежом: материалы Международной научно-практической конференции, Волгоград, 24 мая 2019 г. / Волгоградский институт бизнеса. – Волгоград: Волгоградский государственный медицинский университет, 2019. – С. 238–241. – EDN: JRNDNW

5. Barysė D., Sarel R. Algorithms in the court: does it matter which part of the judicial decision-making is automated? // Artificial intelligence and law. – 2024. – Т. 32, № 1. – С. 117–146.

6. Hirvonen H. Just accountability structures–a way to promote the safe use of automated decision-making in the public sector // AI & SOCIETY. – 2024. – Т. 39, № 1. – С. 155–167.

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ИНТЕЛЛЕКТУАЛЬНЫЕ ПРАВА

Н. А. Айрапетов,
аспирант,
Государственный академический университет
гуманитарных наук

ОТДЕЛЬНЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ И ЗНАЧЕНИЯ ПРИНЦИПА ДОБРОСОВЕСТНОСТИ ПРИ РАСПОРЯЖЕНИИ ИСКЛЮЧИТЕЛЬНЫМ ПРАВОМ

Аннотация. В статье рассматриваются вопросы применения и значения принципа добросовестности при распоряжении исключительным правом.

Ключевые слова: интеллектуальные права, распоряжение правом, соправообладание, соавторство, прекращение исключительного права

CERTAIN ISSUES OF APPLICATION AND SIGNIFICANCE OF THE PRINCIPLE OF GOOD FAITH IN THE DISPOSAL OF AN EXCLUSIVE RIGHT

Abstract. The article focuses on the issues of application and significance of the principle of good faith in the disposition of the exclusive right.

Keywords: intellectual rights, disposal of right, co-ownership, co-authorship, termination of exclusive right

Особенность гражданско-правового метода регулирования общественных отношений состоит в том, что, с одной стороны, само гражданское право характеризуется определенным внутренним единством, а с другой – тем, что те или иные приемы гражданско-правового регулирования общественных отношений различаются в зависимости от конкретных подотраслей гражданского права, что является отражением его дифференциации [1].

В качестве одного из самых ярких выражений единства в дифференциации гражданского права выступают принципы гражданского права. Они задают общие фундаментальные начала, на которых строится сама отрасль гражданского права, позволяют отделить гражданское право от иных отраслей права и предопределяют выстраивание всего гражданско-правового регулирования в определенном ключе. Принципы по-разному проявляют себя в различных подотраслях гражданского права, их применение также различается в зависимости от конкретной подотрасли.

Принцип добросовестности признается одним из базовых принципов гражданских правоотношений. Причем, как и любой другой принцип гражданского права, принцип добросовестности задает упомянутые «единство и дифференциацию». Это обусловлено тем, что данный принцип является синонимом справедли-

вости, выражая идею подлинного, а не конвенционального права, задачей «нахождения» которого в той или иной степени занимается правоприменитель, законодатель или судья. В связи с этим Д. В. Дождев подчеркивает, что добросовестность отнюдь не является неким этическим, моральным стандартом, позволяет изменять право тогда, когда оно не дает прийти к справедливому результату, напротив, понятие справедливости является синонимом подлинного (объективного) права, поиск которого являлся главной задачей римского юриста, в противовес праву строгому (писаному) [2].

Добросовестность может пониматься как некий нравственный стандарт, описывающий допустимые этические рамки поведения лица. Так, И. Б. Новицкий подчеркивал, что добросовестность «таит в себе такие элементы, как знание о другом, о его интересах; знание, связанное с известным доброжелательством; элемент доверия, уверенность, что нравственные основы оборота принимаются во внимание, что от них исходит каждый в своем поведении» [2]. Добросовестность представляет собой поиск некоторого нравственного баланса между эгоизмом и альтруизмом в поведении лица: лицо не должно вести себя чрезмерно эгоистично, учитывая лишь свои собственные интересы и не считаясь с интересами других, но при этом оно и не обязано действовать только в соответствии с интересами другого лица.

Похожее мнение высказал А. Г. Карапетов, отмечая, что «зачастую ссылка на нарушение принципа добросовестности означает моральное осуждение некоего поведения участника оборота, нарушающего представления о должной деловой этике и справедливости» [3].

Следует обозначить определенную специфику, которая усматривается за принципом добросовестности в сфере интеллектуальных прав.

Если в классическом обязательственном праве принцип добросовестности требует учета интересов контрагента при возникновении, изменении или прекращении правоотношения, то в нормах об интеллектуальных правах его содержание представляется более широким: очевидно, что вполне допустимо говорить об обязанности действовать добросовестно не только по отношению к конкретному контрагенту, но и по отношению ко всем лицам в принципе. Эта специфика предопределяется в первую очередь абсолютным характером исключительного права. Лицо, которое обладает исключительным правом или претендует на то, чтобы им обладать, обязано вести себя добросовестно по отношению ко всем участникам оборота в сфере исключительных прав в силу абсолютного характера данных прав, поскольку абсолютному праву корреспондирует всеобщая пассивная юридическая обязанность третьих лиц воздерживаться от их нарушения. В связи с этим интерес вызывает позиция С. А. Синицына, который считает, что всеобщая пассивная юридическая обязанность третьих лиц воздерживаться от нарушения субъективного права не является по своей природе гражданско-правовой. С. А. Синицын подчеркивает, что «ее соблюдение не влечет возникновения гражданско-правовых последствий, являясь общей публичной регулятивно-охранительной юридической обязанностью, касающейся всех без исключения лиц, подчиненных государству и санкционированным им источникам права» [4].

Особенно интересно обратить внимание на то, как добросовестность правообладателя при осуществлении своих интеллектуальных прав проявляется в ситуации с распоряжением своего права. При этом как в рамках единой правовой общности соправообладателей, так и за ее пределами при вступлении в договорные отношения с третьими лицами.

Исключительное право на большинство объектов интеллектуальной собственности может принадлежать как одному, так и нескольким лицам. Статья 1229 ГК РФ предусматривает, что исключительное право на результат интеллектуальной деятельности или средство индивидуализации за исключением фирменного наименования может принадлежать одному лицу или нескольким лицам совместно, и каждый из правообладателей может использовать соответствующий объект по своему усмотрению, за исключением случаев, установленных законом или соглашением между соправообладателями.

Как отмечал Р. Зорм, «совместное авторское право и совместное изобретательское право являются разновидностью юридической общности» [5]. В то же время В. О. Калятин подчеркивает: «Самостоятельность прав влечет возможность каждого правообладателя использовать объект и распоряжаться правом по своему усмотрению без согласования с другими независимыми создателями того же объекта. Однако здесь возникает и точка пересечения: действия одного из обладателей исключительного права могут повлиять на интересы других правообладателей» [6].

Действия автора или правообладателя, которые приводят к прекращению исключительного права на объект интеллектуальных прав в рамках соправообладания, вряд ли можно назвать добросовестными. Это связано с тем, что в итоге один из соправообладателей может лишить исключительного права других соправообладателей помимо их воли. В сфере результатов интеллектуальной деятельности такое возможно в отношении патентоохраняемых объектов, а именно при признании патента недействительным.

Согласно абз. 1 п. 2 ст. 1398 ГК РФ, патент в течение срока его действия может быть оспорен путем подачи возражения в федеральный орган исполнительной власти по интеллектуальной собственности любым лицом, которому стало известно о нарушениях, предусмотренных пп. 1–4 п. 1 ст. 1398 ГК РФ. В силу п. 7 ст. 1398 ГК РФ признание патента недействительным означает отмену решения федерального органа исполнительной власти по интеллектуальной собственности о выдаче патента на изобретение, полезную модель или промышленный образец (ст. 1387 ГК РФ) и аннулирование записи в соответствующем государственном реестре (п. 1 ст. 1393 ГК РФ). В связи с этим возможность оспаривания патента создает риск для существования запатентованного объекта.

При этом абз. 2 п. 2 ст. 1398 ГК РФ наравне с учетом частного интереса лица, подающего возражение, преследует и публичные интересы, заключающиеся в том, чтобы неправомерно выданные патенты не создавали препятствия развитию науки и ведению третьими лицами деятельности с использованием неохраноспособных технических решений, вследствие чего допускается оспаривание патентов в период срока действия любыми лицами [7]. По смыслу ст. 1229 ГК РФ распоряжение исключительным правом при соправообладании должно осуществляться совместно. При этом нельзя не замечать, что практике известны случаи,

когда правообладатель патента сам оспаривал регистрацию своего патента, например, в связи с несением бремени уплаты покупной цены [8]. Поскольку подача возражения против выдачи патента в конечном счете влияет на существование исключительного права, есть основания полагать, что подача возражения против собственного патента соавтором такого патента возможна только по совместному решению сопатентообладателей и не может осуществляться по инициативе одного из них. Такие действия в ущерб интересам остальных сопатентообладателей с учетом обстоятельств может свидетельствовать о его недобросовестном поведении. Если сопатентообладатель хочет прекратить действие патента, у него есть возможность обратиться в патентное ведомство с заявлением о досрочном прекращении действия патента, но для этого указанное заявление должно быть подписано всеми соправообладателями. Действия по оспариванию патента соправообладателем единолично являются прямым обходом закона (запрещенным ст. 10 ГК РФ) с целью обойти требование о совместном подписании заявления о досрочном прекращении патента.

Признание таких действий недобросовестными важно и с той точки зрения, что необходимо разграничивать правовые последствия признания досрочного прекращения действия патента по заявлению и подобного признания в результате несоответствия объекта условиям патентоспособности. Если в последнем случае патент признается недействительным, то это означает, что объект не подлежал правовой охране, и он исключается из реестра, а при рассмотрении последующих заявок не учитывается экспертизой. В случае досрочного прекращения действия патента без его оспаривания он будет присутствовать в реестре и учитываться при анализе новизны и изобретательского уровня поданных заявок.

Важно заметить, что полномочия Роспатента не позволяют ему на стадии рассмотрения заявления о признании патента недействительным, если такое заявление подано соправообладателем, применять ст. 10 ГК РФ. Но и отмена такого решения в условиях злоупотребления права одним из соправообладателей будет неверным, поскольку интересы частных лиц не могут противоречить публичным интересам общества в охране патентоспособных объектов. Представляется, что в таком случае несоответствие действий принципу добросовестности может быть основанием для взыскания убытков соправообладателей с другого соправообладателя, который инициировал оспаривание спорного патента.

Следует учитывать, что такие же рассуждения применимы и к автору патента, который уже не является правообладателем. Как известно, в соответствии с п. 3 ст. 1228 ГК РФ исключительное право на результат интеллектуальной деятельности, созданный творческим трудом, первоначально возникает у его автора. Исключительное право может быть передано автором другому лицу по договору, а также может перейти к другим лицам по иным основаниям, установленным законом [9].

Таким образом, в ситуации, когда соправообладатель или автор пытается оспорить патент, такое поведение должно быть расценено как недобросовестное, поскольку подобные действия представляют собой попытку обхода закона (ст. 10 ГК РФ), который предусматривает необходимость совместного волеизъявления в случае принятия решения о досрочном прекращении действия патента.

В контексте распоряжения исключительным правом на объекты авторских и смежных прав возникает сложность, связанная с отсутствием государственной регистрации таких прав. В этих условиях сторона, заинтересованная в приобретении исключительных прав или в предоставлении права использования, вынуждена полагаться на систему заверений и гарантий (ст. 431.2 ГК РФ), которая предусматривает ответственность за предоставление недостоверной информации при заключении договора.

В отсутствие обязательной регистрации контрагент не имеет возможности получить достоверное подтверждение того, что правообладатель обладает исключительными правами единолично или что конкретный соправообладатель, который выступает стороной по сделке, имеет полномочия на заключение сделки от имени всех соправообладателей. В этом контексте гарантии и заверения, данные стороной при заключении договора, служат важным инструментом для обеспечения правовой определенности и защиты интересов контрагента, поскольку в случае предоставления недостоверной информации виновная сторона может быть привлечена к ответственности.

Таким образом, важность четких и достоверных гарантий и заверений от правообладателя становится ключевым элементом в процессе правового регулирования распоряжения исключительным правом на нерегистрируемые объекты интеллектуальной собственности.

По смыслу п. 1 и 3 ст. 1229 ГК РФ следует, что незаконным признается только использование, осуществляемое иными лицами, нежели правообладатель [10]. Как отмечается в судебной практике, если соправообладатель реализует самостоятельно исключительное право на объект авторских или смежных прав без получения на это согласия другого соправообладателя, то на его контрагента может возлагаться ответственность, поскольку необходимо установить наличие между соавторами соглашения, которое бы предусматривало право соправообладателя использовать объект и распоряжаться исключительным правом самостоятельно и единолично [11]. При этом заключение договора только с одним соправообладателем позволяет не учитывать такой договор суду для легализации факта использования произведения, поскольку он не соответствует положениям п. 3 ст. 1229 ГК РФ [12].

Как видно из указанных примеров, лицо, вступающее в правоотношения по поводу объектов авторских или смежных прав, соправообладателями которых являются несколько субъектов, сильно ограничено в проверке достоверности состава правообладателей и их полномочий, что создает для него соответствующие правовые риски. В обозначенных выше случаях добросовестный контрагент может быть признан нарушителем исключительного права, поскольку не приобретает законных оснований для использования объекта. Совершенная сделка нарушает требование закона и является недействительной в силу ст. 168 ГК РФ как нарушающая требование закона – в данном случае требование абз. 2 п. 3 ст. 1229 ГК РФ о совместном распоряжении исключительным правом [13].

При этом действия лица, которое не имело права на совершение подобной сделки, очевидно, должны квалифицироваться как недобросовестные. Это связно с тем, что обманом считается не только сообщение информации, не соответствующей действительности, но также и намеренное умолчание об обстоятельствах,

о которых лицо должно было сообщить при той добросовестности, какая от него требовалась по условиям оборота [14], а наличие соправообладателей как раз и является таким обстоятельством. Следовательно, заключая сделку, правообладатель должен уведомлять своего контрагента о наличии соправообладателей. Только в таком случае его действия могут считаться добросовестными.

Таким образом, добросовестность соправообладателя при распоряжении исключительным правом в пользу третьих лиц проявляется в виде необходимости получения разрешения от других соправообладателей того же объекта. Это означает, что правообладатель должен добросовестно проинформировать своего контрагента обо всех соправообладателях и их правах, что могут оказать влияние на действительность сделки. Сокрытие такой информации может рассматриваться как умышленное введение в заблуждение и, следовательно, как нарушение принципа добросовестности. Добросовестное поведение требует от правообладателя полной прозрачности в отношениях с контрагентами, что обеспечивает защиту интересов всех участников гражданского оборота.

Развитие принципа добросовестности в направлении предотвращения недобросовестного поведения в сфере исключительных прав может быть достигнуто через внесение законодательных изменений. Одним из таких законодательных актов может стать проект Федерального закона № 479514-8 [15], регулирующий вопросы выделения долей в исключительных правах. Этот законопроект предполагает введение существенного условия в соглашения между правообладателями, которое будет определять порядок их совместных действий при распоряжении исключительными правами. Это будет гарантировать, что любые решения относительно исключительных прав будут приниматься коллективно и с согласия всех долевых правообладателей. Данный законопроект направлен на создание прозрачной и четкой процедуры для совместного распоряжения исключительными правами, что, в свою очередь, должно способствовать добросовестному поведению участников правоотношений. Определение ключевых аспектов распоряжения исключительными правами позволит предотвратить возможные споры между соправообладателями и обеспечит защиту как их интересов, так и интересов лицензиатов и других третьих лиц, взаимодействующих с правообладателями.

Список литературы

1. Гражданско-правовой метод регулирования общественных отношений / В. Ф. Яковлев. – 3-е изд., доп. – М.: Статут, 2022. – С. 210–227.

2. Дождев Д. В. Понятие справедливости (aequitas) в римской правовой традиции // Европейская традиция частного права: исследования по римскому и сравнительному праву: в 2 т. Исслед. центр част. права им. С. С. Алексеева при Президенте Рос. Федерации, Рос. шк. част. права. – М.: Статут, 2021. – С. 8–27.

3. Новицкий И. Б. Принцип добросовестности в проекте обязательственного права // Вестник гражданского права. – 2006. – № 1. – С. 129.

4. Карапетов А. Г., Савельев А. И. Свобода договора и ее пределы. Т. 1: Теоретические, исторические и политико-правовые основания принципа свободы договора и его ограничений. – М.: Статут, 2012. – С. 307.

5. Синицын С. А. Абсолютные и относительные субъективные гражданские права: проблемы теории // Журнал российского права. – 2016. – № 2(230).

6. Sohm R. Der Gegenstand. Ein Grundbegriff des Bürgerlichen Gesetzbuches. – Leipzig: Verlag von Duncker und Humblot, 1905. – Pp. 61–62.

7. Калятин В. О. Проблемы определения системы правообладателей результатов интеллектуальной деятельности // ИС. Авторское право и смежные права. – 2020. – № 8. – С. 35–48.

8. Постановление президиума СИП от 17.04.2017 по делу № СИП-289/2016 // СПС «Консультант плюс».

9. Решение СИП по делу № СИП-796/2022 от 27.03.2023 // СПС «Консультант плюс».

10. Пункт 8 Обзора судебной практики Верховного Суда Российской Федерации № 1 (2023) (утв. Президиумом ВС РФ 26.04.2023).

11. Справка о некоторых спорных вопросах соправообладания исключительным правом на результат интеллектуальной деятельности и средство индивидуализации (подготовлена к обсуждению на заседании Научно-консультативного совета при Суде по интеллектуальным правам от 30 ноября 2018 года). С. 7. – URL: https://ipc.arbitr.ru/files/pdf/spravka_po_sopravo.pdf (дата обращения: 01.06.2024).

12. Постановление СИП от 15.02.2018 по делу № А32-36047/2016, от 24.12.2020 по делу № А40-29771/2019 // СПС «Консультант плюс».

13. Определение ВС РФ от 27.09.2019 № 305-ЭС19-15824 по делу № А40-151454/2017 // СПС «Консультант плюс».

14. Решение СИП от 30.08.2018 по делу № СИП-188/2018, постановление Девятого арбитражного апелляционного суда от 11.04.2012 по делу № А40-100964/11 // СПС «Консультант плюс».

15. Пункт 99 Постановления Пленума ВС РФ от 23.06.2015 № 25 «О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации» // СПС «Консультант плюс».

Е. Д. Борулёва,
магистрант,
Московский государственный юридический университет
имени О. Е. Кутафина (МГЮА)

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ «ДИПФЕЙК» ВО ВЗАИМОСВЯЗИ С ПРАВОМ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ: РОССИЙСКАЯ И ЗАРУБЕЖНАЯ ПРАКТИКА

Аннотация. Технологии «дипфейк» используются в коммерческой деятельности для снижения затрат, однако возникает множество рисков, связанных с нарушением прав интеллектуальной собственности и прав личности. В частности, не решен вопрос определения правовой природы дипфейка и объектов интеллектуальной собственности, созданных с применением дипфейка. Целью научной работы является определение пределов законного использования дипфейков и поиск способов предупреждения правонарушений в этой сфере. В статье описаны подходы к определению дипфейков, риски использования данной ИИ-технологии и способы их минимизации. Анализируется судебная практика России и зарубежных юрисдикций по вопросам нарушения авторских прав на произведения и прав

личности в цифровом пространстве в связи с применением технологии «дипфейк».

Ключевые слова: дипфейк, искусственный интеллект, цифровое пространство, право интеллектуальной собственности, авторское право, объекты интеллектуальной собственности, нарушение авторских прав, нарушение прав на товарные знаки

USAGE OF DEEPFAKE IN RELATIONSHIP WITH INTELLECTUAL PROPERTY LAW: RUSSIAN AND FOREIGN PRACTICE

Abstract. Deepfakes are used in commercial activities to reduce costs, but there are many risks associated with the violation of intellectual property rights and individual rights. In particular, the issue of determining the legal nature of deepfakes and intellectual property objects created with the use of deepfake has not been resolved. The purpose of the scientific work is to determine the limits of legitimate use of deepfake and to find ways to prevent offenses in this area. The article describes approaches to the definition of deepfakes, risks of using this AI-technology and ways to minimize them. The author analyzes the judicial practice of Russia and foreign jurisdictions on the issues of infringement of copyright for works and individual rights in digital space in connection with the use of deepfake technology.

Keywords: deepfake, artificial intelligence, digital space, intellectual property law, copyright, objects of intellectual property, copyright infringement, personal non-property rights

Введение. Технология «дипфейк» (в оригинале – deepfake) активно используется в различных сферах жизнедеятельности, но чаще всего применяется в коммерческой деятельности, например, для создания роликов, рекламы и даже фильмов. Применяя дипфейк, создатели видеопродукта в первую очередь стремятся уменьшить затраты на актерскую игру, поскольку такая ИИ-технология позволяет воссоздать любую личность в цифровом пространстве, однако не задумываются о влиянии на право интеллектуальной собственности.

Основная часть. Так, феноменом последних лет стали дипфейки знаменитостей в фильмах, рекламах, видео с церемоний, роликах в TikTok – самыми известными примерами такого «участия» были сцены фильмов с Николасом Кейджем, комедийные вирусные ролики с Томом Крузом, последние фильмы «Форсажа» с Полом Уокером.

Последние новости из мира шоу-бизнеса описывают ситуации расширения возможностей ИИ-технологий и использование дипфейка в голосовых помощниках, например, подобный случай произошел с актрисой Скарлетт Йоханссон и компанией OpenAI, которые урегулировали конфликт в досудебном порядке.

С одной стороны, применение технологии дипфейка позитивно отражается на технологическом развитии, развитии киноиндустрии, но с другой – злоупотребление данной ИИ-технологии приводит к нарушению прав интеллектуальной собственности, в частности, авторских прав, и к уголовным преступлениям посредством создания незаконного контента, такого как порнографические материалы.

В то же время возможные проблемы неограниченного использования дипфейка обсуждаются юридическим сообществом, и на сегодняшний день рассмотрено немало споров, связанных с нарушением авторских прав в связи с использованием технологии «дипфейк».

Для того чтобы погрузиться в проблематику, необходимо дать определение правовой природы данной технологии.

Дипфейк представляет собой технологию, основанную на использовании генеративно-самостоятельных нейросетей (GAN), которые позволяют частично преобразовывать исходный видео- или аудиоряд с помощью компьютерных алгоритмов.

Законодательное регулирование данной ИИ-технологии в большинстве юрисдикций отсутствует в связи с ее новизной, однако суды стран создают прецеденты и отвечают на вопрос, что такое дипфейк.

Так, в нашумевшем деле «Рефейс Технолоджис» арбитражный суд города Москвы в решении, устоявшем в апелляционной и кассационной инстанциях, подчеркнул, что «технология дипфейк – дополнительный инструмент обработки видеоматериалов» [1. С. 4].

Согласно Закону об искусственном интеллекте Европейского союза (далее – Евросоюз), дипфейк – изображения, аудио- и видеоконтент, созданные технологией искусственного интеллекта, неотличимые от существующих людей, предметов, мест и событий, которые ложно кажутся подлинными и правдивыми [6. С. 459].

Также сложившееся мнение научного юридического сообщества и законодателя о дипфейке сводится к аудио- или видеоманипуляции искусственным интеллектом для создания контента. Например, профессор Калифорнийского университета Хани Фарид определил дипфейк как изображение или текст, аудио или видео, созданные с помощью искусственного интеллекта и методов машинного обучения [5. С. 1–33]. Более того, в поставленной повестке заседания Комитета по доказыванию США указано, что дипфейк представляет собой неподлинную аудиовизуальную демонстрацию, созданную с использованием искусственного интеллекта, сложную для распознавания [2. С. 358].

В связи с вышеуказанным стоит отметить, что преобразование изображения или голоса человека в цифровом пространстве не исключает факт наличия творческого труда человека при создании исходного объекта интеллектуальной собственности, в большинстве случаев речь идет об аудиовизуальных произведениях. А исключительное право на произведение, созданное с применением технологии дипфейка, должно принадлежать лицу, которое использовало в творческой деятельности данную ИИ-технологию для создания произведения, поскольку интеллектуальная собственность используется для стимулирования творческой деятельности по всему миру.

Таким образом, с точки зрения логического рассмотрения вопроса правовой природы дипфейка технология «дипфейк» является инструментом искусственного интеллекта преобразования аудио- и видеоконтента для создания и демонстрации реалистичного, но неподлинного образа, а следовательно, отдельно взятый дипфейк не может быть признан самостоятельным охраняемым объектом интеллектуальной собственности, поскольку отсутствует творческий характер.

В то же время дипфейк как самостоятельный объект может быть признан незаконно созданным и нарушать права интеллектуальной собственности и личные неимущественные права.

Нарушение интеллектуальной собственности путем злоупотребления технологией «дипфейк». Незаконное использование изображения или голоса человека в дипфейк может быть признано существенным нарушением прав интеллектуальной собственности, в частности, авторских прав и прав на товарные знаки.

Законодательство об интеллектуальной собственности большинства стран охраняют права личности на образ – в частности, на личные черты внешности, на голос и иные характеристики, таким образом, легализуется коммерческое использование человека.

Использование дипфейка не только ставит под сомнение подлинность внешности лица, но и его голоса, в связи с чем интеллектуальная собственность и права личности тесно связаны в контексте использования технологии дипфейка.

Например, в Индии применяются режимы авторского права или охраны товарного знака при условии нарушения прав личности в цифровом пространстве.

Интересным кажется недавно рассмотренное дело в Индии по иску Ариджит Сингх и принятый в связи с массовым рассмотрением подобных дел в Болливуде приказ, в котором прослеживается связь личных и публичных прав и права интеллектуальной собственности, в частности, авторское право. А именно ответчикам выдали временный судебный запрет на использование образа Истца путем «использования его имени, голоса/вокального стиля и техники вокальных аранжировок, манеры пения, фотографии, изображения или его подобия, подписи, персоны или любые другие атрибуты личности в любой форме, для любой коммерческой или иной выгоды, без согласия Истца, включая, но не ограничиваясь использованием любых черт личности в любой форме или СМИ, включая онлайн-платформы, публикации, рекламные материалы, доменные имена или использование искусственного интеллекта…» [3. С. 32]. Таким образом, Высший Суд в Бомбее признал нарушение неимущественных прав на образ певца, а именно на имя, голос и вокальный стиль, изображение и фотографии и на подпись путем преобразования технологией дипфейк и использование «конечного персонажа» в видео.

Похожее дело по нарушению прав на голос путем использования дипфейка было рассмотрено в Пекине, но в отличие от правовой практики Индии, согласно законодательству Китая, голос является неотъемлемой частью естественных прав человека. Так, Пекинский онлайн-суд 26 апреля 2024 г. постановил, что компания разработчик программного обеспечения нарушила права человека, после того как использовала технологию дипфейка для воспроизведения голоса без согласия этого человека и после продала его иным платформам, не уведомив о незаконном использовании нематериального блага, т. е. голоса [7].

Более того, Пекинский суд указал в решении, что голос естественного человека идентифицируется по тембру и частоте голоса, обладая уникальными и стабильными характеристиками, которые могут вызывать мысли или эмоции, связанные с конкретным человеком. Хотя естественный голос человека может стать менее узнаваемым после синтеза с искусственным интеллектом, это не означает, что

он не подлежит правовой защите, в связи с чем технология не всегда разрывает связь с естественными человеческими голосами.

Таким образом, судебная практика зарубежных стран приходит к выводу о том, что к личным правам человека, помимо его изображения, относится голос, который также может подпадать под режим охраны авторским правом.

В связи с признанием личных прав и права на публичность, особенно если речь идет о знаменитостях, получение согласия от таких лиц на создание дипфейка является обязательным для использования их образа и характеристик личности в коммерческих целях.

Также права личности сильно взаимосвязаны с коммерческим использованием атрибутов своей личности в Соединенных Штатах Америки (далее – США), несмотря на некоторые различия в зависимости от штата, права личности охраняют имя, образ и изображение человека. В связи с тем, что в основе прав личности в США лежит коммерческая эксплуатация ее атрибутов, правовые вопросы, связанные со сходством при злоупотреблении технологией дипфейка, разрешается в институте неимущественных прав личности.

Однако проблема нарушения авторских прав при использовании технологии дипфейка стоит остро в США, поскольку, согласно Закону об авторском праве, произведение может подлежать охране авторским правом при условии, если оно является оригинальным авторским произведением, зафиксированным на материальном носителе [5. С. 83], т. е. «авторское произведение» должно быть создано человеком.

В связи с чем объекты авторского права, созданные с помощью технологии дипфейка, в США не подпадают под режим охраны авторским правом и не относятся к произведениям.

Стоит отметить, что в вопросах использования и распространения контента с дипфейком применима концепция авторского права fair use, согласно которой допустимо правомерное использование объекта авторского права с учетом принципа разумности и выявленных на практике факторов (цель и характер использования, характер произведения, объем и существенность заимствования, влияние использования произведения на рынок). Следовательно, регулирование дипфейков в США в рамках авторского права неоднозначно из-за возможности подпадание под режим добросовестного использования. Аргументом в пользу подпадания под добросовестное использование исходного произведения может служить тот факт, что характер работы отличается от оригинального произведения, поэтому вероятность причинения ущерба потенциальному рынку крайне мала.

В то же время иная ситуация возникает при наличии в контенте, созданном с дипфейком, порочащих и клеветнических сведений, поскольку такие вопросы регулируются в большей степени уголовным законодательством.

Возвращаясь к ранее указанному российскому делу о дипфейке по иску ООО «Рефейс технолоджис», стоит отметить также интересную формулировку арбитражного суда в решении: «…тот факт, что моушн-дизайнер по заказу осуществил технический монтаж исходных материалов видеоролика посредством технологии deepfake, сам по себе не свидетельствует о том, что видеоролик доступен для свободного использования (без согласия правообладателя), или о том, что группа лиц, обеспечившая написание сценария видеоролика, видеосъемку, его

аудиосопровождение, не внесли личный творческий вклад в создание видеоролика и не признаются его авторами» [1. С. 4]. Таким выводом суд пресек возможные дальнейшие споры о свободном использовании подобных произведений, созданных с помощью ИИ-технологий, и еще раз подчеркнул наличие творческого вклада человека в создание видеоролика.

Следовательно, при желании использования произведение с дипфейком или его части необходимо заключить договор об отчуждении исключительного права или договор о предоставлении права использования с правообладателем произведения, а также получить согласие от лица, которого «использовали» для дипфейка.

Аналогичный подход можно применять к использованию дипфейков в товарных знаках, а именно получить согласие лица на создание дипфейка по его образу и регистрации полученного обозначения в качестве товарного знака. В случае отсутствия письменного согласия лица на создание дипфейка и регистрации товарного знака патентные ведомства, скорее всего, откажут в регистрации такого обозначения либо данное лицо пойдет в суд с исковым заявлением о нарушении прав на изображение или о введении потребителя в заблуждение.

Минимизация рисков использования технологии дипфейк. Правовые системы в связи с быстрым развитием ИИ-технологий обновляют законодательную базу и пытаются создать способы технической защиты от злоупотребления технологии дипфейк, в частности, принимаются отдельные законы о регулировании искусственного интеллекта.

Законодатели иностранных юрисдикций в целях минимизации рисков использования технологии дипфейка приняли во внимание инструменты проверки подлинности информации в цифровом пространстве, используемые, в частности, в уголовном процессе, а также принимаются меры предоставления цифровой информации. Например, в США используется стандарт Дауберта в отношении идентификации дипфейков.

Во многих юрисдикциях приняли законы об обязательной маркировке цифрового контента, созданного с помощью ИИ-технологии, в частности, такие законодательные акты действуют в КНР, США и Евросоюзе.

В США, как было сказано ранее, с учетом возможности применения концепции fair use как аргументации законного использования технологии дипфейк, государственным институтам трудно регулировать пределы использования такой ИИ-технологии, что также приводит к проблемам с уведомлениями и удалением соответствующего контента в соответствии с законодательством о коммуникации [4].

Согласно ст. 52 (3) Закона об искусственном интеллекте Евросоюза, от создателей цифрового контента с дипфейком требуется прозрачность в раскрытии информации о способе создания цифрового контента, а именно создатель должен предоставить информацию об использованных методах [6. С. 459]. Данная норма направлена на информирование потребителей относительно цифрового контента и на распознавание ими изображений, созданных с помощью манипуляций. В то же время эффективность закрепленных требований о раскрытии информации зависит от надежных сильных механизмов правоприменения, а именно вопрос привлечения к ответственности за неисполнение обязательства.

Кроме того, законодателям необходимо тщательно продумать и закрепить баланс публичных и частных интересов – прозрачности сведений и подавляющий эффект на художественное самовыражение и развитие творческой деятельности.

Однако применение инструмента принудительной маркировки цифрового контента с дипфейком открывает вопрос, кто будет нести ответственность, в частности, обсуждается объем ответственности онлайн-платформ. Предполагаю, что государства, в которых вносятся соответствующие поправки в законы (например, США, Китай), обяжут онлайн-платформы запрашивать информацию о контенте у пользователей до публикации и мониторинга платформы на предмет дипфейков: в этом случае будет вставать вопрос о возможном нарушении исключительных прав третьих лиц. В свою очередь, подобный мониторинг требует дополнительных технических средств, которые должны будут разработать либо сами онлайн-платформы, либо по заказу государства специализированная компания.

Существуют иные подходы к рассмотрению ответственности за распространение объектов, созданных с помощью технологии дипфейк, но с нарушением прав третьих лиц.

Так, законодательство об авторском праве Индии содержит исчерпывающий перечень нарушений авторских прав, однако дипфейк не включен в данный перечень, в связи с чем в случае возникновения посягательств на исключительные права (в частности, право на создание производных произведений, защита произведения от искажения) ответственность возлагается на создателя спорного произведения или на информационного посредника. Такую правовую позицию высказал суд в решении по делу Myspace Inc. против Super Cassettes Industries Ltd. [8].

В связи с вышесказанным законодательства об авторском праве разных юрисдикций могут использоваться в качестве эффективного инструмента государственного регулирования в отношении использования технологии дипфейк при условии законодательной модернизации к современным условиям.

В то же время существует техническая необходимость создания компьютерной технологии для своевременного обнаружения дипфейка, последующих уведомлений посреднику и владельцу контента и уничтожению такого произведения, созданного путем злоупотребления данной ИИ-технологии.

Кроме того, как ранее было отмечено, и заключение договоров об отчуждении лицензионных соглашений, и получение согласий от соответствующих лиц на использование дипфейка станут эффективным способом минимизации нарушений исключительных прав и личных неимущественных прав, например, на изображение и голос человека.

Заключение. Применение технологий «дипфейк» все в больших масштабах ставит законодателя в непростую ситуацию: с одной стороны, сдерживание масштабов использования такой ИИ-технологии в целях минимизации нарушений в сфере права интеллектуальной собственности и посягательств на личные неимущественные права, с противоположной – поддержание технологического развития и творческой деятельности.

В то же время государствам необходимо применять активные подходы к борьбе с незаконно созданными и распространенными объектами интеллектуальной собственности с дипфейком.

Технология «дипфейк», как вид искусственного интеллекта, должна рассматриваться как дополнительный технический инструмент для создания объекта интеллектуальной собственности, в связи с этим дипфейк не может быть признан самостоятельным объектом и охраняться правом интеллектуальной собственности отдельно. Но вхождение дипфейка в иной объект делает его составной частью, и такой объект охраняется правом интеллектуальной собственности как единое произведение или товарный знак.

Более того, в связи с активным развитием технологии дипфейк, а именно расширением возможностей не только на манипуляцию изображения и мимики человека, но и его голоса и интонации, необходимо предоставить голосу человека правовую охрану как нематериального блага наряду с изображением человека.

В частности, изменить ст. 152.1 Гражданского кодекса РФ следующим образом:

«ст. 152.1 ГК РФ “Охрана изображения и голоса гражданина”

в п. 1 добавить “…изображения и голоса гражданина (в том числе его фотографии, а также видеозаписи, аудиозаписи или произведения изобразительного и кинематографического искусства, в которых он изображен) допускаются только с согласия этого гражданина…”

добавить подп. 4 п. 1 “гражданин записывал голос за плату”

в п. 2 добавить “…содержащих изображение или голос гражданина…”

в п. 3 добавить “если изображение или голос гражданина… гражданин вправе требовать удаления этого изображения или аудиозаписи…”»

Таким образом, российской юрисдикцией приравняются по правовой защите два неотъемлемых блага человека: изображение и голос, более того, музыкальные произведения и аудиовизуальные произведения будут взаимосвязаны с материальными благами, в связи с чем упростится судебное разбирательство по нарушению одного лица на объект авторского права.

Также кажется приемлемым и необходимым ввести на государственном уровне обязательную маркировку контента, создаваемого ИИ-технологиями, таким образом, государственный регулятор создаст базу таких произведений и увеличит возможность пресечения нарушений исключительных прав и личных неимущественных прав.

Список литературы

1. Решение Арбитражного суда города Москвы от 30.11.2023 по делу № А40-200471/2023 // Электронное правосудие [Электронный ресурс]. – URL: arbitr.ru/A40-200471/2023 (arbitr.ru) (дата обращения: 01.09.2024).

2. Agenda for Advisory committee on evidence rules meeting Washington, D.C. April 19, 2024. – URL: 2024-04_agenda_book_for_evidence_rules_meeting_final.pdf (uscourts.gov) (дата обращения: 01.09.2024).

3. Arijit Singh v. Codible Ventures LLP and Ors. Interim Application (L) No. 23560 of 2024 in com ipr suit (l) No. 23443 of 2024. In the high court of judicature at bombay ordinary original civil jurisdiction in its commercial division – 2024. – URL: https://www.livelaw.in/pdf_upload/arijit-singh-vs-codible-ventures-llp-552701.pdf (дата обращения: 02.09.2024).

4. Communications Decency Act of 1996 (CDA) S.314 – 1995–1996. – URL: Text – S. 314–104th Congress (1995-1996): Communications Decency Act of 1995. Congress.gov. Library of Congress (дата обращения: 02.09.2024).

5. Copyright Law of 1976 United States Code Title 17 – Copyrights (Public Law 94-553 of October 19, 1976), as last amended by Public Law 104-39 of November 1, 1995). – URL: US001: Copyright, Code, 19/10/1976, Title 17 USC Ch. 1 to 11 (derechosautor.com) (дата обращения: 02.09.2024).

6. European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) / P9_TA(2024)0138 – 2024. – URL: TA (europa.eu) (дата обращения: 01.09.2024).

7. Hany Farid Creating, Using, Misusing, and Detecting Deep Fakes Journal of Online Trust & Safety 1:4 – 2022 – September. – URL: (PDF) Creating, Using, Misusing, and Detecting Deep Fakes (researchgate.net) (дата обращения: 01.09.2024).

8. Myspace Inc. v. Super Cassettes Industries Ltd. (2017) 236 DLT 478 (DB). In the High Court of Delhi FAO (OS) 540/2011 and C.M. Appl. 20174/2011, 13919 & 17996/2015 – 2021 – December 12. – URL: Myspace Inc. v. Super Cassettes Industries Ltd. - The Cyber Blog India (дата обращения: 02.09.2024).

9. 全国首例 AI 生成声音人格权侵权案一审宣判北京互联网法院 2024 年 04 月 23 日 [Первое в стране дело о нарушении прав личности, созданное с помощью искусственного интеллекта, было рассмотрено в первой инстанции, Пекинский онлайн-суд, 23 апреля 2024)]. – URL: https://mp.weixin.qq.com/s/_GxGaG6Q2NYHJWQuOtMyrQ?from=industrynews&version=4.1.20.6024&platform=win (дата обращения: 02.09.2024).

Е. А. Губаева,
юридическая фирма Semenov & Pevzner

ОТВЕТСТВЕННОСТЬ ОПЕРАТОРА ЦИФРОВОЙ ПЛАТФОРМЫ ПРИ НАРУШЕНИИ НА ПЛАТФОРМЕ ИСКЛЮЧИТЕЛЬНЫХ ПРАВ НА ТОВАРНЫЕ ЗНАКИ

Аннотация. В статье рассматривается ответственность оператора (владельца) цифровой платформы при нарушении исключительных прав на средство индивидуализации. Сделан вывод о том, что признание оператора платформы информационным посредником зависит от активности и степени участия платформы в отношениях между продавцом и покупателем. Кроме того, поскольку законодателем не установлен надлежащий период рассмотрения заявлений о нарушении исключительных прав на товарные знаки на цифровых платформах, автором предлагается указать срок в семь дней с учетом ст. 314 ГК РФ, предусматривающей подобный срок для исполнения обязательств, срок исполнения которых сторонами не был определен.

Ключевые слова: цифровая платформа, оператор цифровой платформы, товарный знак, цифровая экономика, информационный посредник, маркетплейс, средство индивидуализации

LIABILITY OF THE DIGITAL PLATFORM OPERATOR IN CASE OF INFRINGEMENT OF EXCLUSIVE RIGHTS TO TRADEMARKS ON THE PLATFORM

Abstract. The article considers the liability of the operator (owner) of a digital platform in case of infringement of exclusive rights to a means of individualization. It is concluded that the possibility of recognizing the platform operator as an information intermediary directly depends on the degree of participation of the platform in the relationship between the seller and the buyer. In addition, since the legislator has not established a proper period for consideration of applications for infringement of exclusive rights to trademarks on digital platforms, the author proposes to specify a period of seven days, taking into account Article 314 of the Civil Code of the Russian Federation, which provides for a similar period for the fulfillment of obligations, the term of performance of which was not determined by the parties.

Keywords: digital platform, digital platform operator, trademark, digital economy, information intermediary, marketplace, means of individualization

Введение. На сегодняшний день процессы цифровой трансформации экономики стремительно развиваются, а цифровые технологии оказывают огромное влияние на экономическое развитие общества. Как отмечает В. А. Вайпан, цифровая экономика строится на трех уровнях, которые влияют на жизнь и развитие общества. Первым уровнем выступают рынок и отрасли экономики, в которых происходит непосредственное взаимодействие субъектов предпринимательской деятельности. На втором уровне расположены платформы и технологии, где появляются необходимые компетенции для развития сфер деятельности. Наконец, третий уровень обуславливает существование среды, создающей условия для развития цифровых платформ и технологий [5. С. 6].

Основная часть. Что понимается под цифровой платформой? В Федеральном законе от 26 июля 2006 г. № 135-ФЗ «О защите конкуренции» (далее – Закон о защите конкуренции) цифровая платформа определяется как «программа (совокупность программ) для электронных вычислительных машин в информационно-телекоммуникационных сетях, в том числе в сети Интернет, обеспечивающую совершение сделок между продавцами и покупателями определенных товаров».

Цифровые платформы являются неотъемлемой частью современной экономики, без которых невозможно представить деятельность субъектов предпринимательской деятельности в современном мире [2. С. 1]. Однако в настоящее время существуют определенные пробелы в законодательстве, а также и в правоприменительной практике в отношении правового регулирования осуществления деятельности с помощью цифровых платформ.

В ходе осуществления предпринимательской деятельности на многих цифровых платформах используются определенные средства индивидуализации, в основном товарные знаки. Известно, что товарные знаки выполняют важные функции:

– идентификационную – благодаря чему товары (услуги) способны выделяться на фоне конкурентных товаров и запоминаться потребителям;

– информационную – потребители могут сделать вывод относительно характеристик товара (услуги) и осуществить выбор;

– создания конкурентных правоотношений между предпринимателями, посредством чего хозяйствующие субъекты стремятся повышать качество продаваемых ими товаров (услуг) [3. С. 13].

Тем не менее нередки ситуации, когда предприниматель или, к примеру, владелец платформы может осознанно или по ошибке нарушить исключительные права лиц на средства индивидуализации. В таком случае возникнет проблема нарушения обеспечения потребительского интереса. Клиент будет приобретать на платформе товар, не соответствующий его ожиданиям. Пострадают и конкуренты: ведь, используя товарный знак, вызывающий неправдоподобные представления и ассоциации о товаре (услуге), нарушитель создаст себе преимущество на цифровой платформе. Но это преимущество неправомерно и должно пресекаться.

Стоит отметить, что нарушения исключительных прав на товарные знаки на платформах не являются единичными случаями. Скорее наоборот, это можно назвать частым явлением. Лишь в 2023 году, по данным Федеральной антимонопольной службы, на маркетплейсах по жалобам правообладателей было заблокировано более 2,4 млн карточек товаров [4].

В результате случающихся нарушений исключительных прав на платформах возникает насущный вопрос: несет ли владелец (оператор) цифровой платформы какую-либо ответственность за необнаружение контрафакта на платформе или за задержку в удалении информации, которая содержит в себе нарушение исключительных прав?

В случае нарушения исключительных прав на товарные знаки на платформах неминуемо может возникнуть риск судебных разбирательств. Поэтому необходимо определить правовой статус владельца или оператора цифровой платформы и проанализировать, может и должен ли данный субъект нести ответственность за нарушение прав в отношении средств индивидуализации, совершенное на цифровой платформе.

В законодательстве России предусмотрена категория информационного посредника; согласно ст. 1253.1 ГК РФ оператор платформы признается информационным посредником и освобождается от несения ответственности, если его деятельность удовлетворяет следующим условиям:

1) он не знал и не должен был знать о том, что использование соответствующих результатов интеллектуальной деятельности или средств индивидуализации, содержащихся в таком материале, является неправомерным;

2) в случае получения в письменной форме заявления правообладателя о нарушении интеллектуальных прав с указанием страницы сайта и (или) сетевого адреса в сети Интернет, на которых размещен такой материал, он своевременно принял необходимые и достаточные меры для прекращения нарушения интеллектуальных прав.

Однако можно ли признать владельца или оператора цифровой платформы информационным посредником, если на платформе было совершено нарушение исключительных прав на товарные знаки?

В российской практике, связанной с защитой исключительных прав на товарные знаки, сложилось два подхода к определению статуса лица, владеющего цифровой платформой. Согласно первому подходу, владелец цифровой платформы признается информационным посредником, поскольку сам не вводит

контрафактный товар в гражданский оборот и оказывает лишь посреднические услуги между продавцом и потребителем.

Второй подход основан на том, что владелец цифровой платформы также участвует в реализации контрафактных товаров, поскольку без содействия продавца никаких гражданско-правовых отношений между потребителем и продавцом не сложилось бы. Например, Суд по интеллектуальным правам в деле № А41-85375/2020 сделал вывод о том, что «общество “Вайлдберриз” выступает в качестве получателя денежных средств за реализацию и доставку заказанного товара, а также осведомлено о содержании размещаемой на его сайте информации о контрафактном товаре».

Представляется, что для определения статуса владельца информационной платформы анализ будет производиться в каждом конкретном деле в зависимости от набора тех или иных обстоятельств, установленных законодательством (в частности, ст. 1253.1 ГК РФ). Кроме того, на признание лица информационным посредником влияют требования, установленные в п. 78 Постановлении Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации»:

– какую роль занимает лицо в формировании размещаемого на платформе материала;

– получает ли лицо прибыль от размещения материала, являющегося неправомерным, на цифровой платформе.

Исследователи также делают вывод о том, что решение о статусе лица, владеющего цифровой платформой, должно приниматься в зависимости от формы участия лица в отношениях между продавцом и потребителем. Так, А. С. Ворожевич выделяет следующие формы взаимодействия цифровой платформы с другими участниками предпринимательских отношений:

– маркетплейс совершает реализацию товара от имени и за счет продавца. Потребитель оплачивает товар напрямую маркетплейсу, а продавец получает вырученную сумму только после удержания платформой процента;

– маркетплейс оказывает услуги, связанные с транспортировкой и хранением на складах товара, однако не принимает участия в продаже товаров и получает оплату от продавцов только за оказываемые сопутствующие услуги [1. С. 133–141].

В оферте ООО «Вайлдберриз» (цифровая платформа Wildberries) можно заметить, что платформа работает именно по первому сценарию: согласно п. 4.11 оферты, «Вайлдберриз удерживает вознаграждение, сумму подлежащих возмещению издержек, стоимость услуг Вайлдберриз и цену хранения товара из денежных средств, подлежащих перечислению продавцу за реализованный товар». Это значит, что маркетплейс, во-первых, взымает плату с продавцов за такие услуги как хранение, доставка, маркировка, упаковка товара, а во-вторых, удерживает также и процент с реализации товара, то есть получает денежные средства за продажу контрафактного товара, а не за предоставление возможности размещать товар на площадке.

Согласно сформировавшейся судебной практике, именно платформа Wildberries выступает продавцом в отношениях с потребителями. Например, в од-

ном из дел было установлено, что при покупке маркетплейс выдает чеки, где указывается непосредственно продавцом товара. Более того, в случае брака или иных проблем с товаром сама платформа в качестве продавца возмещает потребителям убытки и замену неисправного продукта. Так, в деле, рассмотренном Первым кассационным судом общей юрисдикции, судом было установлено, что ООО «Вайлдберриз» посредством дистанционного способа продажи товаров осуществило продажу физическому лицу наручных часов Romanoff 6302 G3B2. По истечении гарантийного срока гражданин обратился к платформе с претензиями к качеству товара, которые оставлены без удовлетворения. В ходе производства по делу ООО «Вайлдберриз» не оспаривало, что в сложившихся правоотношениях является продавцом товара, что привело к удовлетворению исковых требований и возложению на платформу обязанности компенсировать истцу убытки и моральный вред. В таком случае, разумеется, стоит признать, что платформа не отвечает критериям, предъявляемым к информационному посреднику, и должна нести ответственность при реализации контрафактного товара.

В то же время оферта ООО «ЯндексМаркет» содержит следующие положения: предметом договора между маркетплейсом и продавцом является оказание услуг «ЯндексМаркетом», куда включается размещение товаров продавца на вебсайте. Кроме того, оплата оказанных услуг осуществляется в форме отдельного платежа, а не посредством удержания маркетплейсом процента от вырученной суммы от покупателя. То есть можно сделать вывод, что данный маркетплейс работает по второй модели, описанной А. С. Ворожевич, и, соответственно, можно предположить, что действительно является информационным посредником.

Анализ зарубежной практики показывает, что иностранные подходы к определению статуса и, следовательно, ответственности владельца цифровой платформы довольно похожи на национальный. Например, в деле Tiffany против eBay, рассмотренном в США, истец просил привлечь к ответственности владельцев маркетплейса eBay за то, что платформа способствовала продаже контрафактных товаров на своем сайте. Суд отказал в удовлетворении исковых требований, подчеркнув необходимость высокого уровня доказательства того факта, что компания знала или должна была знать о нарушении. По мнению суда, владелец цифровой платформы предпринял разумную меру для предотвращения нарушений, воспользовавшись программой VeRO (Verified Rights Owner Program), которая удаляет незаконный контент в течение 12 часов после обращения правообладателей.

В ином же деле, рассмотренном судом Европейского союза, компания Coty, являющаяся правообладателем товарного знака DAVIDOFF, обратилась в суд против владельца цифровой платформы Amazon. Истец утверждал, что на платформе предлагаются к продаже духи с названием, содержащим в себе товарный знак истца. Лицензионных договоров между истцом и ответчиком не заключалось, разрешения на использование средства индивидуализации платформой Amazon получено не было. Суд отказал в удовлетворении иска, отметив, что маркетплейс выполняет функцию исключительно технического посредника в отношениях продавца и покупателя на платформе. Платформа Amazon осуществляет лишь хранение товаров продавцов на своих складах и предоставляет онлайн-площадку для реализации товаров.

Получается, что суды других правопорядков при выяснении ответственности цифровых платформ также отталкиваются от степени участия платформы в отношениях между продавцом и покупателем, а также выявляют, мог ли маркетплейс знать о размещениях контента на платформе с нарушением прав третьих лиц.

Статья 1253 ГК РФ предусматривает, что «лицо для признания его информационным посредником не только не должно знать о том, что использование объектов интеллектуальной собственности, содержащихся в материале на цифровой платформе, является неправомерным, но и обязано своевременно принимать меры для прекращения нарушения исключительных прав».

Отметим, что в законодательстве предусмотрен четкий срок удаления неправомерного материала лишь в отношении объектов авторского права. Согласно ст. 15.7 Закона об информации, правообладатель вправе направить владельцу сайта заявление о нарушении авторских и (или) смежных прав, если на сайте им будет обнаружена информация, размещенная без каких-либо законных оснований. Владелец сайта, в соответствии с действующим законодательством, обязан удалить неправомерно размещенные материалы в течение 24 часов с момента получения заявления от правообладателя.

В отношении средств индивидуализации срок удаления ссылок, контента на платформе, содержащей в себе контрафактные товары, законом не установлен. Данный пробел в законодательстве влечет злоупотребления со стороны владельцев цифровых платформ, в результате чего неправомерно размещенная информация на сайте не удаляется, нарушители продолжают получать выгоду от продажи контрафактного товара, права владельцев исключительных прав продолжают нарушаться.

К сожалению, судами также не выведены критерии для определения разумного срока прекращения нарушения прав. Например, в решении по делу № А41-8904/2022 суд не признал ООО «Вайлдберриз» информационным посредником, поскольку «с момента получения ответчиком претензии истца до принятия им соответствующих мер по удалению информации прошло около 3 месяцев, и более того, спорная информация в отношении спорных товаров после удаления размещается заново». В то же время в ином деле, напротив, суд пришел к выводу о том, что ответчик – владелец цифровой платформы – предпринял меры и удалил информацию в разумные сроки: исковое заявление было направлено в декабре 2013 года, а удаление контента произошло в конце февраля 2014 года.

По мнению автора, отсутствие четко регламентированного срока удаления с цифровой платформы материалов, содержащих в себе чужие объекты интеллектуальной собственности, влечет серьезные экономические последствия для всех участников предпринимательских отношений. Таким образом, видится правильным внесение изменений в действующее законодательство и установление разумного срока, при выполнении которого владелец цифровой платформы может быть признан информационным посредником.

Автор полагает, что разумным сроком может быть определен срок в двадцать четыре часа, как закреплено Законом об информации. Однако с учетом специфики работы маркетплейсов, необходимости запроса от правообладателей документов, подтверждающих их исключительные права, срок удаления может быть

продлен до семи дней, поскольку, к примеру, ст. 314 ГК РФ определяет именно такой срок для исполнения должником обязательства со дня предъявления кредитором требования об его исполнении (если срок исполнения обязательства сторонами был не определен).

Таким образом, если деятельность цифровой платформы не удовлетворяет установленным в законе критериям и не позволяет признать ее владельца информационным посредником, наступает гражданско-правовая ответственность. Однако Правительством Российской Федерации был также разработан проект постановления, согласно которому с 1 марта 2023 года маркетплейсы должны были нести ответственность за распространение контрафактной продукции, а также немаркированного товара. Как следует из анализа документа, ответственность маркетплейсов должна была наступать именно за сокрытие сведений и неуказание их в системе обязательной электронной маркировки. Тем не менее данный документ не вступил в законную силу, хотя, по мнению автора настоящей работы, его принятие обеспечило бы защиту потребителей от некачественной продукции и правообладателей от нарушения их исключительных прав.

Заключение. В статье были рассмотрены разные подходы к ответственности владельцев цифровых платформ за предложение к продаже и продажу на маркетплейсах товаров, маркированных средствами индивидуализации без получения на то разрешения правообладателей. Автором сделан вывод, что владелец (оператор) цифровой платформы признается информационным посредником только в случае, если маркетплейс выступает лишь техническим посредником в отношениях между продавцом и покупателем. Если же маркетплейс принимает денежные средства за покупку контрафактного товара, не удаляет в разумные сроки контент, содержащий нарушение исключительных прав, владелец платформы должен выступать ответчиком и привлекаться к ответственности наряду с продавцом контрафактного товара.

Список литературы

1. Ворожевич А. С. Споры по нарушениям исключительных прав на товарные знаки в маркетплейсах // Журнал Суда по интеллектуальным правам. – 2021. – № 2. – С. 133–141.

2. Губин Е. П., Харитонова Ю. С. Цифровые платформы в Европе, Китае и России: основные подходы и тенденции правового регулирования // Право и экономика. – 2020. – № 8(340).

3. Ворожевич А. С. Защита брендов: стратегии, системы, методы: учебное пособие для магистров. – М.: Проспект, 2017. – 141 с.

4. Маркетплейсы заблокировали 2,4 млн карточек контрафакта в 2023 году // ПравоРу [Электронный ресурс]. – URL: https://pravo.ru/news/251180/ (дата обращения: 16.07.2024).

5. Правовое регулирование экономических отношений в современных условиях развития цифровой экономики: монография / отв. ред. В. А. Вайпан, М. А. Егорова. – М.: Юстицинформ, 2019. – 376 с.

Е. М. Косьяненко,
кандидат юридических наук, доцент,
Уральский государственный юридический университет
имени В. Ф. Яковлева

АКТУАЛЬНЫЕ ПРАВОВЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ПРОИЗВЕДЕНИЙ АРХИТЕКТУРЫ И ДИЗАЙНА В СЕТИ ИНТЕРНЕТ

Аннотация. Развитие цифровых технологий способствует увеличению скорости распространения результатов интеллектуальной деятельности. Одновременно с легальным использованием развивается и незаконное копирование цифровых произведений. Однако произведения архитектуры и дизайна не являются классическими информационными произведениями. Статья посвящена исследованию взаимосвязи способов использования объектов архитектуры и дизайна в сети Интернет и мер ответственности за нарушения интеллектуальных прав на такие объекты. Нормы материального права, посвященные регулированию объектов архитектуры и дизайна, предопределяют специфику использования этих объектов. Эскизы, проекты, чертежи, файлы визуализации, фотографии и прочие результаты интеллектуальной деятельности архитекторов и дизайнеров защищаются от нелегального копирования и распространения в сети Интернет. Однако в правовое понятие «произведение архитектуры» входит также материальный архитектурный объект. В статье соотносятся правила и нормы IV части российского Гражданского кодекса в отношении произведения с правами архитекторов на реализацию их дизайн-проектов в материально-вещественной форме, а также порядок расчета компенсации за незаконное использование «экземпляров» с реальными произведениями архитектуры и дизайна при предложении товаров, работ или услуг в сети Интернет.

Ключевые слова: право, цифровые технологии, интеллектуальная собственность, произведение архитектуры, дизайн-проект, реализация проекта, компенсация

CURRENT LEGAL ISSUES OF USING ARCHITECTURE AND DESIGN WORKS ON THE INTERNET

Abstract. The development of digital technologies contributes to the increase in the speed of distribution of the results of intellectual activity. Along with legal use, illegal copying of digital works is also developing. However, works of architecture and design are not classic information works. The article is devoted to the study of the relationship between the methods of using architectural and design objects on the Internet and measures of liability for violation of intellectual property rights to such objects. The norms of substantive law devoted to the regulation of architectural and design objects predetermine the specifics of the use of these objects. Sketches, projects, drawings, visualization files, photographs and other results of intellectual activity of architects and designers are protected from illegal copying and distribution on the Internet. However, the legal concept of "work of architecture" also includes a tangible architectural object. The author of the article correlates the rules and norms of Part IV of the Russian Civil Code in relation to the work with the rights of architects

to implement their design projects in real form, as well as the procedure for calculating compensation for the illegal use of “copies” with real works of architecture and design when offering goods, works or services on the Internet.

Keywords: law, digital technologies, intellectual property, architectural work, design project, project implementation, compensation

Введение. Согласно п. 1 ст. 1229 Гражданского кодекса РФ (далее – ГК РФ), физическое лицо или организация, обладающие исключительным (имущественным) правом на результат интеллектуальной деятельности (правообладатель), вправе использовать такой результат по своему усмотрению любым не противоречащим закону способом. Правообладатель может разрешать или запрещать третьим лицам использование результата интеллектуальной деятельности своей волей и по своему желанию. Отсутствие запрета правообладателя не считается его согласием или разрешением.

Современное законодательство определяет информационно-телекоммуникационную сеть Интернет как «технологическую систему, предназначенную для передачи информации, доступ к которой осуществляется с использованием специальных технических средств». Поэтому, размышляя об использовании произведений архитектуры и дизайна в Сети, необходимо учитывать технологически-информационную специфику системы, понимать, что телекоммуникационная сеть позволяет распространять только информационные и нематериальные блага, определяя особый характер использования результатов интеллектуальной деятельности, свойственный цифровым объектам.

Основная часть. В действующем гражданском законодательстве отсутствует точная дефиниция понятий «произведение архитектуры» и «произведение дизайна». Обращаясь к регулированию подобных объектов до 2006 года, можно отметить, что ранее под объектами авторского права в сфере архитектуры понимались: архитектурный проект, разработанная на его основе документация для строительства и сам архитектурный объект [14].

В современной научной литературе и судебной практике [17] под «произведением архитектуры» понимается в первую очередь *архитектурный проект*, т. е. та часть проектной документации, в которой выражено *архитектурное решение*. Возведение здания, сооружения или конструкции на основе оригинального авторского архитектурного проекта, по смыслу п. 1 ст. 1294 ГК РФ, является не созданием произведения архитектуры, как было ранее, а использованием произведения архитектуры путем реализации проекта. Вместе с тем судебная практика подчеркивает важность специфики архитектурной деятельности, предусматривающей две формы бытия объекта права: как в форме произведения архитектуры, градостроительства и садово-паркового искусства, так и в форме проектов, чертежей, изображений и макетов, охраняемых авторским правом. Рассмотрим терминологию обозначенных объектов подробнее.

Действующее законодательство устанавливает повышенные требования к проектной документации, а также к лицам, их разрабатывающим, в том числе определяет некоторые обязательные условия договора о подготовке данной документации, закрепляет условия привлечения профессиональных субъектов, формулирует порядок разработки проектной документации, регламентирует процессы

оценки соответствия документации требованиям законодательства, закрепляет ответственность за нарушение требований.

Например, в гл. VI Градостроительного кодекса РФ упоминаются типовые и нетиповые «архитектурные решения» как составные части проектной документации. Они могут содержать документацию, состоящую из материалов в текстовой форме либо в виде карт, схем, фигур и определяющую архитектурные, функционально-технологические, конструктивные и инженерно-технические решения для обеспечения реконструкции, ремонта или создания новых объектов капитального строительства, если при этом затрагиваются конструктивные и другие характеристики надежности и безопасности.

Совершенно верно уважаемый нами ученый В. С. Витко выделял в процессе создания архитектурного произведения такие этапы, как: «1) возникновение замысла (идеи) архитектурного объекта; 2) создание архитектурного решения (форма изложения замысла); 3) выражение архитектурного решения в объективной форме путем закрепления воображаемой формы изложения замысла на материальном носителе в виде изображения или в объемно-пространственной форме непосредственно в материале» [1. С. 105]. Ключевым является некое оригинальное творческое авторское «архитектурное решение», которое для целей установления факта наличия или отсутствия неправомерного использования архитектурного произведения необходимо выявить и обособить. Только после этого становится возможным проследить взаимосвязь индивидуального нетипового творческого решения с реализованным объектом.

Подобный эскиз или чертеж может быть выполнен как в обычном классическом виде, так и в 3D-формате, как от руки, так и с помощью компьютерной графики, в том числе в виде визуализации будущего архитектурного объекта. Именно такие чертежи и рисунки обычно именуются авторами «дизайн-проект» или «произведение архитектурного дизайна». Во-вторых, «произведение архитектуры», как объект охраны, включает в себя реализованный в пространстве материальный объект (объект недвижимости либо не относящийся к недвижимости объект архитектуры и дизайна).

Однако реализация проекта в пространстве связана не только с созданием «произведения архитектуры и искусства», но и с использованием такого объекта. Неисчерпывающий перечень способов использования произведений закреплен в ст. 1270 ГК РФ. В соответствии с подп. 10 п. 2 ст. 1270 ГК РФ использованием произведения независимо от того, совершаются ли соответствующие действия в целях извлечения прибыли или без такой цели, считается, в частности, практическая реализация архитектурного, дизайнерского и иных проектов. Возникает несколько вопросов: 1) что такое «практическая реализация» объекта? Можно ли реализовать архитектурный или дизайнерский проект в сети Интернет? Каким способом можно использовать данный объект в сети Интернет?

В настоящее время авторы и правообладатели произведений архитектуры и так называемых архитектурных дизайн-проектов активно формируют судебную практику в общих и арбитражных судах в свою пользу [16]. По статистике, суды в 80 % случаях удовлетворяют требования правообладателей о взыскании компенсаций за незаконное размещение в сети Интернет изображений в виде рисунков, эскизов, 3D-визуализаций или фотографий произведений архитектуры [8].

При этом свои требования истцы (правообладатели) формулируют, основываясь на фактах незаконного использования в сети Интернет чертежей, эскизов и рисунков, фотографий, а расчет компенсации производят на основании неправомерного использования реализованных архитектурных объектов (по п. 2 ст. 1301 ГК РФ) в размере двукратной цены «контрафактного экземпляра произведения», указывая в качестве таковых готовые дома, бани, завершенные интерьеры квартир, реконструированные коммерческие помещения и т. д. У ответчиков такие подходы вызывают недоумение и сомнение в добросовестности и соразмерности.

Описывая возможности использования произведений, М. А. Рожкова поясняет, что «использование результата интеллектуальной деятельности допускает три разновидности действий в отношении этого результата, а именно: его обнародование – совершение определенных действий, которые позволяют сделать этот объект интеллектуальной деятельности доступным для всеобщего ознакомления с ним публики, не подразумевающее материальное воплощение этого результата; его воплощение в материальном носителе (иначе говоря, воспроизведение), с тем чтобы выпустить этот материальный носитель в гражданский оборот, что подразумевает изготовление материального носителя, в котором применен, использован, воссоздан результат интеллектуальной деятельности и который будет продан или иным образом отчужден, передан в прокат, на хранение, ввезен на территорию Российской Федерации или вывезен с территории и т. п.; и его интегрирование, охватывающее переработку…» [12. С. 6]. Следовательно, по мнению эксперта, изготовление материального носителя с целью внедрения в гражданский оборот приравнивается в первую очередь к воспроизведению.

Особенности использования исследуемого объекта уточняются в п. 1 ст. 1294 ГК РФ, где предусмотрено, что автор произведения архитектуры, градостроительства или садово-паркового искусства имеет исключительное право использовать свое произведение в соответствии с п. 2 и п. 3 ст. 1270 ГК РФ, в том числе путем *разработки документации* для строительства и путем *реализации* архитектурного, градостроительного или садово-паркового *проекта*. Использование архитектурного или аналогичного проекта для реализации допускается, по общему правилу, только однократно. Таким образом, закон связывает использование произведения архитектуры с фактом его практической непосредственной реализации любым способом [10], но ничего не говорит о воспроизведении проекта или изготовлении экземпляра чертежа, эскиза, рисунка или фотографии (о распечатке фотографии или копировании рисунка и др.).

Указанные нормы не распространяются на «произведения дизайна». Если пострадавшая сторона (правообладатель) в исковом заявлении опирается на положения ст. 1294, п. 2 и п. 3 ст. 1270 ГК РФ, то необходимо соотнести идею автора дизайна с «архитектурным решением» или «архитектурным проектом». В целом использование дизайна может производиться как путем воспроизведения, так и с помощью распространения экземпляров дизайна, переработки дизайна, публичного показа дизайнерской модели и т. д. При этом в случае предложения к продаже и продажи контрафактного материального носителя произведения дизайна отсутствует использование несколькими способами [13, 15].

Также правообладателю следует учитывать принцип исчерпания права и положения ст. 1272 ГК РФ, когда *оригинал или экземпляры произведения дизайна*

правомерно введены в гражданский оборот на территории нашей страны *путем их продажи или иного отчуждения*, дальнейшее распространение оригинала или экземпляров произведения допускается без согласия правообладателя и без выплаты ему вознаграждения, за исключением случая, предусмотренного ст. 1293 ГК РФ.

В качестве примера некорректного, на наш взгляд, расчета компенсации можно привести судебное дело № А60-23052/2023, где за неправомерное использование фотографий модульных домов и за реализацию проекта модульного дома компенсацию рассчитывали на основании п. 1, 2 ст. 1301 ГК РФ. При этом компенсация за незаконное использование на сайте фотографических снимков домов не была обоснована истцом ни стоимостью изготовления одной фотографии, ни стоимостью использования права на фотографию либо соразмерными убытками правообладателя. Общая стоимость исключительных прав на фотографии, созданные по договору авторского заказа, составляла 15 тыс. рублей за 103 фотографии домов (около 145 рублей за одну фотографию), договор авторского заказа не содержал какого-либо сложного технического задания либо требований к фотографическим объектам. Правообладатель потребовал взыскать компенсацию из расчета 20 тыс. рублей за одну фотографию, и суд удовлетворил требование правообладателя в полном размере.

В этом же деле истец просил взыскать компенсацию за нарушение исключительных прав на дизайн-проект путем использования его на сайте на основании п. 2 ст. 1301 ГК РФ в двукратном размере стоимости «контрафактных экземпляров произведения» (т. е. дизайн-проекта модульного дома), рассчитывая размер компенсации на основании стоимости самого модульного дома, указанной в договоре подряда. Следует заметить, что модульный дом не был построен, а был оформлен только договор на строительство дома. Суд удовлетворил требование истца и взыскал компенсацию за незаконное использование дизайн-проекта в размере почти 1,5 млн рублей [18]. Суд рассматривал дом как экземпляр дизайн-проекта, а договор на строительство – как распространение контрафактного экземпляра дизайн-проекта.

Исследуя компенсацию как меру ответственности, ученые пишут, что «разновидностью контрафактных экземпляров, обладающей некоторыми особенностями, являются материальные копии с произведений изобразительного, декоративно-прикладного искусства, практическая реализация произведений архитектуры. В таких случаях возможен расчет компенсации по стоимости права либо в виде процента от стоимости оригинальной работы, если она известна в связи с тем, что работа была ранее приобретена у автора. Возможно также взыскание компенсации в твердой сумме. Факторами, влияющими на размер компенсации, могут служить количество копий, неоднократность подобных действий, коммерческий характер такой деятельности. Имеет значение также известность автора и/или произведения» [7. С. 132].

Если речь идет о расчете компенсации за использование объекта архитектуры (реализацию объекта архитектуры), то так называемым «контрафактным экземпляром» должна выступать материальная копия оригинального экземпляра, т. е. непосредственно самого объекта архитектуры (возведенный дом, построенная баня, реконструированное сооружение, готовый интерьер помещения и т. д.).

Однако в судебной практике мы видим стабильную подмену понятий, и вместо объекта архитектуры стороны предъявляют фотографии, рисунки, эскизы, чертежи и прочие архитектурные проекты и решения.

На наш взгляд, если речь идет о незаконной практической реализации произведения дизайна и архитектуры, то правообладателю необходимо доказать, что в материализованном объекте использовались уникальные решения произведений архитектуры и дизайна, созданные специально для правообладателя на основе технического задания. Кроме того, контрафактные «экземпляры архитектурных произведений» или реализованные на основании проектной документации сооружения должны существовать реально в момент нарушения исключительного права [6]. В противном случае расчет компенсации, основанный на несуществующих в действительности копиях зданий и сооружений, нарушает как минимум принципы добросовестности и справедливости.

Заключение. Таким образом, использование (в виде обнародования, воспроизведения, распространения, переработки и т. д.) «произведения архитектуры» и «произведения дизайна» в сети Интернет может ассоциироваться только с использованием архитектурного решения или проекта (а именно чертежа, эскиза, рисунка, визуализации, фотографии, графического файла и т. д.), т. е. частью проектной документации, имеющей *информационное* значение, в которой выражен самостоятельный уникальный творческий авторский замысел. Однако использовать в сети Интернет материальный архитектурный объект (построенный дом, здание, сооружение) не представляется возможным. Материальный объект можно сфотографировать и перенести в цифровую форму, тогда появится производный объект в виде цифровой фотографии дома. Любой документ или договор на строительство дома, ремонт помещения, реконструкцию какого-либо архитектурного объекта также может рассматриваться как материальный носитель (экземпляр), но подтверждать он будет только способ использования таких произведений, как рисунки, чертежи, схемы (воспроизведение, переработка) в том случае, если в тексте договора или в приложениях используются аналогичные объекты (рисунок, чертеж, схема), охраняемые авторским правом. Однако договор подряда на создание архитектурного объекта, в том числе размещенный в сети Интернет, не является доказательством реализации архитектурного или дизайнерского проекта, равно как договор на создание натюрморта или портрета не является картиной. Реализация возможна только путем строительства архитектурных и дизайнерских объектов. Поэтому расчет компенсации за незаконное использование в виде реализации архитектурного объекта, основанный на фактически не реализованном объекте либо на подмене объекта (фотография или рисунок вместо построенного дома), не отвечает требованиям соразмерности, справедливости, законности и не способствует развитию нормальной конкурентной среды в области архитектуры и дизайна.

Список литературы

1. Витко В. С. К вопросу о понятии «произведение архитектуры»: анализ правовой позиции, выработанной судебной практикой // Копирайт (Вестник Академии интеллектуальной собственности) – 2021. – № 1. – С. 96–107.

2. Градостроительный кодекс Российской Федерации от 29.12.2004 № 190-ФЗ // Собрание законодательства РФ. – 2005. – № 1 (часть I). – Ст. 16.

3. Гражданский кодекс Российской Федерации (часть четвертая): Федеральный закон от 18.12.2006 № 230-ФЗ // Собрание законодательства РФ. –2006. – № 52 (часть I). – Ст. 5496.

4. О составе разделов проектной документации и требованиях к их содержанию: Постановление Правительства РФ от 16 февраля 2008 г. № 87 // Собрание законодательства РФ. – 2008. – № 8 – Ст. 744.

5. Об архитектурной деятельности в Российской Федерации: Федеральный закон от 17.11.1995 № 169-ФЗ // Собрание законодательства РФ. – 1995. – № 47. – Ст. 4473.

6. Постановление Суда по интеллектуальным правам от 14.06.2023 по делу № А40-17129/2022.

7. Павлова Е. А., Калятин В. О., Корнеев В. А и др. Компенсация как мера ответственности за нарушение исключительных прав. Часть 2 // Журнал Суда по интеллектуальным правам. – 2022. – № 3(37). – С. 118–211.

8. Аналитическая система «Сутяжник» (версия 1.17), разработанная ООО «НПП «Гарант-Сервис-Университет» 2017–2024 гг.

9. Постановление Пленума Верховного Суда РФ от 23.04.2019 № 10 // СПС «Гарант» [Электронный ресурс]. – URL: https://internet.garant.ru/#%2Fdocument%2F72230696%2Fparagraph%2F340%3A0 (дата обращения: 08.09.2024).

10. Постановление Суда по интеллектуальным правам от 07.07.2014 № С01-547/2014 по делу № А70-6510/2013.

11. Рекомендации Научно-консультативного совета при Суде по интеллектуальным правам по вопросам, возникающим при рассмотрении требований о пресечении нарушений исключительных прав // Журнал Суда по интеллектуальным правам. – 2024. – № 2(44). – С. 11–20. [Электронный ресурс]. – URL: http://ipcmagazine.ru/files/ipcmagazine/0/2/1744020/jornal_062024_new.pdf (дата обращения: 08.09.2024).

12. Рожкова М. А. О некоторых вопросах оборота исключительных прав и материальных носителей объектов интеллектуальной собственности // Журнал российского права. – 2014. – № 9. – С. 5–11. [Электронный ресурс]. – URL: https://rozhkova.com/pdf/Oborotmatenositeley-2014.pdf (дата обращения: 07.09.2024).

13. Постановление Суда по интеллектуальным правам от 18.12.2020 по делу № А40-203904/2019, которое вошло в Обзор судебной практики рассмотрения гражданских дел, связанных с нарушением авторских и смежных прав в информационно-телекоммуникационной сети «Интернет», утв. Президиумом Верховного Суда Российской Федерации 29 мая 2024 г. // СПС «Гарант» [Электронный ресурс].

14. Гл. IV Федерального закона от 17.11.1995 № 169-ФЗ «Об архитектурной деятельности в Российской Федерации» // СПС «Гарант» [Электронный ресурс].

15. П. 56 Постановления Пленума Верховного Суда РФ от 23.04.2019 № 10 // СПС «Гарант» [Электронный ресурс].

16. Решение Коптевского районного суда г. Москвы от 31 июля 2023 г. по делу № 02-0029/2023; Решение Арбитражного суда Свердловской области и Постановление Семнадцатого Арбитражного Апелляционного суда № 17-АП-2255/2024 по делу А60-23052/2023; Решение Арбитражного суда г. Москвы и Постановление Суда по интеллектуальным правам № С01-2840/2023 по делу № А40-21631/2023 и др.

17. Постановление Президиума ВАС РФ от 27.09.2011 № 5816/11, от 06.11.2012 г. № 7697/12, Определение ВС РФ от 24.04.2017г. № 305-ЭС17-3662, а также ряд постановлений Суда по интеллектуальным правам: от 24.01.2017 по делу № А40-214554/2015; от 16.05.2018 № 310-ЭС18-13107 по делу № А62-6028/2016; от 07.06.2018 № С01-334/2018 по делу № А05-9375/2017; от 19.02.2019 № С01-21/2019 по делу № А48-9019/2017; от 20.05.2019 № С01-189/2019 по делу № А60-10375/2018; от 24.09.2019 № С01-910/2019 по делу № А54-78/2018; от 17.10.2019 № С01-1068/2019 по делу № А41-76048/2018; от 20.11.2019 № С01-1043/2019 по делу № А62-2870/2018; от 26.08.2020 № С01-666/2020 по делу № А32-34035/2018 и др.

18. Решение Арбитражного суда Свердловской области от 25.01.2024 и Постановление Семнадцатого Арбитражного Апелляционного суда от 17.05.2024 г. №17-АП-2255/2024 по делу А60-23052/2023.

19. Справка «Вопросы, связанные с определением критериев творческой деятельности на примере фотографических произведений», вынесенная на обсуждение на заседании Научно-консультативного совета при Суде по интеллектуальным правам // Журнал Суда по интеллектуальным правам. – 2024. – № 2(44). – С. 21–34 [Электронный ресурс]. – URL: http://ipcmagazine.ru/files/ipcmagazine/0/2/1744020/jornal_062024_new.pdf (дата обращения: 08.09.2024).

20. Технический регламент о безопасности зданий и сооружений: Федеральный закон от 30.12.2009 № 384-ФЗ // Собрание законодательства РФ. – 2010. – № 1. – Ст. 5.

Е. А. Останина,
кандидат юридических наук, доцент,
Челябинский государственный университет

ИМЯ ФИЗИЧЕСКОГО ЛИЦА И ПСЕВДОНИМ КАК СРЕДСТВА ИНДИВИДУАЛИЗАЦИИ

Аннотация. В статье анализируются два средства индивидуализации гражданина – имя и псевдоним. В отечественной судебной практике уже высказан вывод о том, что при создании псевдонима требуется согласие носителя имени, если имя и псевдоним совпадают. Однако этот вывод не совсем корректен. Личное неимущественное право на имя, как и всякое право, не является безграничным, его пределы устанавливаются с учетом противостоящих интересов, а противостоящим интересом может быть свобода творчества. Поэтому если псевдоним больше известен, чем имя, нет нарушения права на имя.

Ключевые слова: имя, псевдоним, свобода творчества, авторское право

THE NAME OF A PERSON AND THE PSEUDONYM AS A MEANS OF INDIVIDUALIZATION

Abstract. The article analyzes two means of individualization of a person – a first name and a pseudonym. In modern judicial practice, it has been concluded that when creating a pseudonym, the consent of the bearer of the name is required if the name and the pseudonym coincide. The author believes that this conclusion is not entirely correct. The author believes, that the person's right to the name is a one among the natural rights, and the same is a right to the freedom of creativity. Therefore, if the pseudonym is more well-known than the name, there is no violation of the right to the name.

Keywords: name, pseudonym, freedom of creativity, copyright

Введение. Индивидуализация гражданина обеспечивается разными средствами, но в первую очередь индивидуализация гражданина осуществляется путем указания его имени [6. С. 174].

Основная часть. В ст. 19 ГК РФ имя гражданина прямо названо средством индивидуализации, а ст. 150 ГК РФ включает право на имя в открытый перечень личных нематериальных благ. Средства индивидуализации физического лица возникли исторически. В закрепленных ст. 19 и 20 ГК средствах индивидуализации до сих пор осталось очень много от римского права и от раннего Средневековья.

Имя человека – это средство индивидуализации, причем одно из наиболее старых и наиболее удобных средств; в период цифровизации право на имя должно получить определенные новые способы защиты, чтобы, с одной стороны, исключить произвольную эксплуатацию чужой популярности (какая была бы, например, в случае свободы использования чужого имени в наименовании героев видеоигр или мультфильмов), а с другой – нужно позволить гражданам, если они хотят и допускают это, на основании договора определенным образом «монетизировать» свою популярность, в том числе посредством разрешения использовать имя в качестве элемента товарных знаков, коммерческих обозначений.

В немецкой литературе отмечается, что имена, с одной стороны, служат упорядочению гражданского оборота, так как обозначают участников правоотношений, с другой – отражают индивидуальность личности, а также что имя выполняет функцию устойчивой идентификации личности [2. С. 26]. С этим можно согласиться. Нужно отметить, что 11.06.2024 в Германии принят Закон о перемене имени (Gesetz zur Änderung des Ehenamens- und Geburtsnamensrechts und des Internationalen Namensrechts), который вступает в силу 1 мая 2025 г. Закон направлен на расширение свободы в выборе имени; при этом фактором, ограничивающим свободу, остается соображение защиты прав носителя имени; особенно немецкий законодатель обращает внимание на защиту личных нематериальных прав несовершеннолетнего [1. S. 1–46]. В российском праве ст. 58 Семейного кодекса Российской Федерации [8] устанавливает границы права родителей свободно выбирать имя своему ребенку, можно обратить внимание на то, что основным ориентиром в осуществлении этого права является защита законных интересов несовершеннолетнего.

Право на имя существует в рамках абсолютного правоотношения. Нарушением права на имя является использование имени без согласия его носителя (п. 3

ст. 19 ГК); здесь имеется не до конца разрешенная проблема определения границ права на имя с учетом того, что совпадение имен может быть случайным. Обычно признается, что совпадение имен не представляет собой нарушения даже в том случае, если это совпадение не совсем случайно (например, если родители назвали своего ребенка по имени знаменитого дедушки или прадедушки, как в Риме, например, были Марк Порций Катон – старший и Марк Порций Катон – младший). Так, по замечанию М. М. Агаркова, право на имя не дает управомоченному лицу права исключительного пользования своим именем. Другие лица также могут им пользоваться вполне правомерно, когда они сами обладают тем же именем [4. С. 96].

Вместе с тем правила о регистрации товарных знаков обнаруживают, что возможна конкуренция граждан – носителей совпадающих имен. Согласно п. 9 ст. 1483 ГК, не могут быть зарегистрированы в качестве товарных знаков обозначения, тождественные имени или производному от них обозначению известного в Российской Федерации на дату подачи заявки лица, без согласия этого лица или его наследника. Конечно, это требование установлено потому, что товарный знак, в котором содержится указание на имя известного гражданина, распространил бы все позитивные ассоциации, которые у людей вызывает это имя, на товары, для которых зарегистрирован товарный знак. Безусловно, если мы допустим такое распространение без согласия гражданина, это будет в высшей степени несправедливо, поскольку это носитель имени добился, чтобы его имя так позитивно воспринималось обществом. В случае если заявитель сам обладает именем, тождественным имени гражданина, известного на день подачи заявки, совпадение имен заявителя и известно лица не должно освобождать заявителя от получения согласия гражданина, известного в Российской Федерации или в мире на день подачи заявки, от получения разрешения.

Ассоциации, связанные с тем или иным словом, могут меняться. Например, в известных спорах о товарных знаках «гагаринский» и «чкаловский» суд обратил внимание на устойчивые ассоциации, сложившиеся у потребителей. Поскольку организации, зарегистрировавшие за собой эти товарные знаки, десятилетиями находились на улицах с аналогичным названием, суд счел, что слова указывают скорее на место нахождения организации, но не на конкретных граждан, известных своими заслугами; таким образом, здесь слова утратили свою связь с личностью носителя имени, а это значит, что право на имя не было нарушено (Постановление Президиума СИП от 31.10.2016 по делу № СИП-238/2016; Решение СИП от 25.12.2014 по делу № СИП-734/2014).

Похожая проблема, связанная с установлением границ права на имя, возникает в случае использования другим гражданином псевдонима, совпадающего с именем. Такой казус рассматривался Верховным Судом РФ в деле Феликса Разумовского (определение СК ГД ВС РФ от 15.08.2017 № 5-КГ17-102), где требование состояло в запрете использовать псевдоним, аналогичный имени ответчика.

Несмотря на то, что имя истца и псевдоним ответчика не совпадали в части отчества, иск был удовлетворен, коллегия подчеркнула, что ответчик не получил согласия истца. Примечательно, что из обстоятельств дела даже неясно, знал ли ответчик, выбирая псевдоним, о существовании истца. Представляется, что правила о защите имени можно толковать несколько мягче, не требуя у того, кто хочет

создать псевдоним, максимально подробного поиска по миру для выяснения вопроса о том, не совпадает ли предполагаемый псевдоним с чьим-нибудь именем [7. С. 71–86]. Хотелось бы отметить социальную пользу псевдонима. Ее важно учитывать, поскольку защита личных неимущественных прав имеет важную особенность – требуется учитывать и социальную ценность охраняемого права, и социальную ценность права (или законного интереса), которое находится в конфликте с защищаемым субъективным правом истца. Можно согласиться с тем, что границы личного неимущественного права определяются в каждом конкретном случае с учетом противостоящих интересов, ценности противостоящего права [8. С. 164]. В области авторского права, в частности, значимый интерес состоит в охране свободы творчества. Псевдоним может использоваться как способ отграничить творчество от частной жизни, или как способ разграничить две сферы творчества, например, художественное и научное. Поэтому возможность аннулировать псевдоним, предоставленная каждому носителю сходного имени, даже если этот носитель менее известен, чем обладатель псевдонима, может несколько сузить свободу творчества (по крайней мере, придется творить под собственным именем или быть готовым в любой момент сменить свое имя в органе ЗАГС, превратив псевдоним в имя.

Предусмотренное ст. 19 ГК РФ правило следует толковать с учетом цели его установления. При таком толковании должна учитываться узнаваемость носителя псевдонима и носителя имени для круга потенциальных читателей, зрителей и иных лиц, которым адресовано творчество. Если псевдоним подражает известному и узнаваемому носителю имени, нарушается основная функция имен и псевдонимов – сделать личность узнаваемой. В таком случае это действие следует оценивать в качестве правонарушения. Если носитель имени не более известен, чем носитель псевдонима, можно сделать вывод о случайном совпадении имени и псевдонима. При таком случайном совпадении не следует требовать согласия носителя имени для использования псевдонима. Поэтому кажется слишком широким вывод, сделанный в Определении СКГД ВС РФ от 15.08.2017 № 5-КГ17-102.

Заключение. Представляется, что для удовлетворения иска, предъявленного обладателем имени к носителю псевдонима, недостаточно просто установить сходство имени с псевдонимом. Требуется еще установить признаки злоупотребления правом в действиях лица, использующего псевдоним.

Список литературы

1. Dutta A. Reform des deutschen Namensrechts. Berlin Juristische Gesellschaft zu Berlin, publiziert von Walter de Gruyter GmbH, 2020. S. 1–46.

2. Erman Bürgerliches Gesetzbuch. Kommentar mit Nebengesetzen / H. P. Westermann, B. Grunewald, G. Maier-Reimer. 17. Auflage. – Köln: Verlag Dr. Otto Schmidt KG, 2023.

3. Thieme W. Das Deutsche Personenrecht. – Berlin: Duncker & Humblot, 2003.

4. Агарков М. М. Избранные труды по гражданскому праву: в 2 т. – Т. 2. – М.: АО «Центр Юринфор», 2002. – 490 с.

5. Бойкова Т. А. Личное имя как объект языковой рефлексии (на материале метаязыковых высказываний русских и американцев): дис. … канд. филол. наук. – М., 2017.

6. Гонгало Б. М. Правовой статус гражданина в частном праве. Постатейный комментарий главы 3 Гражданского кодекса Российской Федерации // Избранное: сборник научных трудов: в 5 т. / Б. М. Гонгало. М.: Статут, 2021. Т. 2. Гражданское право. 2003–2014. – 720 с.

7. Останина Е. А. О защите имени и псевдонима. По мотивам Определения Судебной коллегии по гражданским делам ВС РФ от 15.08.2017 № 5-КГ17-102 // Вестник экономического правосудия Российской Федерации. – 2017. – № 11. – С. 71–86.

8. Ульбашев А. Х. Общее учение о личных правах. – М.: Статут, 2019.

М. Н. Чирагов,
ООО «ЛигалПикс»,
Высшая школа экономики,
магистр права
У. А. Алиев,
Институт права и национальной безопасности,
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации,
аспирант

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК УГРОЗА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Аннотация. В статье рассматривается влияние искусственного интеллекта (ИИ) на право интеллектуальной собственности в условиях цифровой эпохи. В центре внимания – правовые вызовы, связанные с использованием данных, защищенных авторским правом, для обучения ИИ, а также создание новых произведений на основе таких данных. Анализируются текущие судебные прецеденты, включая иски против компаний OpenAI и GitHub, которые поднимают вопросы этичности и законности использования таких данных. Также обсуждаются правовые аспекты лицензирования открытого программного обеспечения и проблемы защиты авторских прав в условиях активного применения ИИ. Делается вывод о необходимости разработки четких правовых рамок и обеспечения прозрачности использования данных для обучения ИИ, а также подчеркивает важность поиска компромиссов в вопросах лицензирования и защиты авторских прав в новых технологических реалиях.

Ключевые слова: искусственный интеллект (ИИ), интеллектуальная собственность, авторское право, обучение ИИ, лицензирование, судебные прецеденты, правовое регулирование

ARTIFICIAL INTELLIGENCE AS A THREAT TO INTELLECTUAL PROPERTY

Abstract. The article examines the impact of artificial intelligence (AI) on intellectual property law in the digital era. It focuses on the legal challenges related to the use of copyrighted data for AI training, as well as the creation of new works based

on such data. The author analyzes recent legal precedents, including lawsuits against companies like OpenAI and GitHub, which raise questions about the ethics and legality of using such data. The article also discusses the legal aspects of open-source software licensing and the challenges of protecting copyright in the context of active AI application. The author concludes that clear legal frameworks and transparency in data usage for AI training are necessary, emphasizing the importance of finding compromises in licensing and copyright protection in the new technological landscape.

Keywords: Artificial Intelligence (AI), Intellectual Property, Copyright, AI Training, Licensing, Judicial Precedents, Regulation

Введение. Инновации невозможны без защиты нематериального капитала. Внимание к интеллектуальной собственности последние десятилетия обоснованно повышалось, так как рост и диверсификация экономики сопряжены с новыми технологиями. Мы вошли в цифровую эпоху, включая искусственный интеллект (далее – ИИ), технологии прогнозирования, сложную автоматизацию и большие данные. Это неизбежно приводит к изменению существующих отраслей и возникновению новых. Есть опасения, что цифровизация может усугубить экономическое неравенство (Доклад о положении в области интеллектуальной собственности в мире за 2022 г. Вектор инновационной деятельности. Женева. ВОИС).

Обсуждение трансформации юридической профессии уходит корнями в появление пишущей машинки, копировальной бумаги, компьютера и т. д. Эта область (развитие юридической функции) не входит в предмет настоящей работы. Я хотел бы акцентировать внимание на ИИ, его влияние на право интеллектуальной собственности и рассмотреть зарождающееся правовое регулирование. Актуальность темы обусловлена правовым составляющим творчества, который считался уникальным актом человеческого гения. Уникальным и неповторимым. У человека была абсолютная монополия на искусственное создание нового. Вызовы для права заключались в фиксации этого творения, выявлении критериев уникальности, защите и охране, регламентации существования нематериальных активов в гражданском обороте. Генеративные сервисы появились не вчера, но созданные ими объекты были настолько примитивны, что никто всерьез не воспринимал их. Однако публичные сервисы последних лет поставили перед специалистами ряд вопросов:

– можно ли считать созданные ИИ объекты уникальным творением;

– как установить авторство;

– возможность их защиты и охраны;

– необходимость обозначить такие объекты;

– способы регулирования в существующем гражданско-правовом порядке (обобщая предыдущие вопросы).

Это далеко не полный перечень вопросов, которые актуальны для юристов в сфере интеллектуальной собственности. В рамках настоящей статьи мы не ставим задачу рассмотреть экономические аспекты темы ИИ, но в части аргументации иногда будем прибегать к этой составляющей вопроса.

В качестве основных методов в работе применены: метод аналогии, юридико-догматический, герменевтический, структурно-функциональный методы

и сравнительно-правовой метод (включающий в себя case-study и cross-study методы). Без последнего невозможно изучение новых предметов.

Основная часть. Регулирование ИИ. Для понимания влияния ИИ на интеллектуальную собственность необходимо рассмотреть способы и примеры регулирования в разных юрисдикциях. Под регулированием следует понимать в том числе и рамочные акты, концепции, стандарты, проекты. В связи с тем, что ИИ является новым вызовом для существующих правовых систем, следует шире трактовать регулирование.

Инструменты генеративного искусственного интеллекта могут создавать новый контент: текст, компьютерный код, изображение, аудио, видео. Результат создается на основе запроса пользователя (промта). Генеративный ИИ основан на машинном обучении с использованием огромного массива данных, который может содержать миллиарды страниц текста, изображений, кода, музыки и т. д. Убеждены, что в первую очередь юриспруденции нужно ответить на вопрос об авторстве материала, на основе которого обучается ИИ, а второстепенно рассматривать за программой право на объект творчества. При этом конкретное законодательное толкование этих объектов необязательно. Правоприменитель сам неплохо находит объекты интеллектуальной собственности в новых формах (произведениях). Например, дело о незаконном использовании результатов интеллектуальной собственности, а именно видео в формате reels [1]. Суд решил, что reels является аудиовизуальным произведением и «расщепил» его на составные объекты результатов интеллектуальной деятельности.

Помимо практики правоприменителя, развивается и специальное регулирование.

Одним из важных актов в сфере ИИ в Российской Федерации стал Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (с изменениями и дополнениями) [2]. В рамках этого указа была утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 года (далее – Стратегия). В 2024 году в него были внесены изменения [3]. Учитывая специфику направления, динамичность регулирования в области ИИ кажется закономерным. На наш взгляд, Указ Президента РФ от 15 февраля 2024 г. № 124 конкретизировал и актуализировал национальную стратегию. В Стратегии появилось понятие «большие генеративные модели» (п. 5, подп. «о»). Указом Президента РФ от 9 мая 2017 г. № 203 утверждена стратегия развития информационного общества в Российской Федерации на 2017–2030 годы [4]. Стратегия научно-технологического развития Российской Федерации среди приоритетов научно-технологического развития Российской Федерации в ближайшие 10–15 лет определяет «переход к передовым цифровым, интеллектуальным производственным технологиям, роботизированным системам, новым материалам и способам конструирования, создание систем обработки больших объемов данных, машинного обучения и ИИ; связанность территории Российской Федерации за счет создания интеллектуальных транспортных и телекоммуникационных систем». Понятие ИИ встречается и во многих других стратегиях. За последние годы национальные стратегии в области ИИ и продвижения ИИ-технологий вы-

пустили Канада, Китай, Дания, Комиссия ЕС, Финляндия, Франция, Индия, Италия, Япония, Мексика, Скандинаво-Балтийский регион, Сингапур, Южная Корея, Швеция, Тайвань, ОАЭ и Великобритания.

Важной вехой в части регулирования ИИ в России было принятие Федерального закона № 123-ФЗ [5]. Законом было установлено, что в Москве с 1 июля 2020 года на пять лет устанавливается экспериментальный правовой режим. Среди основных задач экспериментального режима указаны создание благоприятных правовых условий развития технологий ИИ и апробация технологий ИИ. Согласно подп. 2 п. 1 ст. 2 Закона, под искусственным интеллектом понимается комплекс технологических решений, позволяющий имитировать когнитивные функции человека и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека. Это определение нам кажется наиболее актуальным.

Как средство стимулирования ИИ были созданы и экономические предпосылки. Были внесены изменения в гл. 25 НК РФ «Налог на прибыль организаций» внесены федеральными законами от 14.07.2022 № 321-ФЗ и № 323-ФЗ «О внесении изменений в часть вторую Налогового кодекса Российской Федерации» [6]. Письмом ФНС России от 07.03.2023 № СД-4-3/2672 до налогоплательщиков доведены коды, которые используются при заполнении налоговой декларации по налогу на прибыль организаций при учете указанных расходов [7]. Так как ИИ используется во многих отраслях, создается специальное регулирование в форме распоряжений, приказов и т. п.

В 2021 году был принят Кодекс этики в сфере искусственного интеллекта («Кодекс»). В нем были установлены общие этические принципы и стандарты поведения, которыми следует руководствоваться участникам отношений в сфере ИИ. Кодекс содержит важные принципы и подходы в части использования ИИ, например:

– человеко-ориентированный и гуманистический подход;
– уважение автономии и свободы воли человека;
– недискриминация;
– оценка рисков и гуманитарного воздействия;
– рискориентированный подход;
– идентификация ИИ в общении с человеком;
– безопасность работы с данными и др.

На практике этические аспекты часто не принимаются во внимание основными акторами. Однако в Кодексе обозначены важные принципы и подходы, игнорирование которых может привести к правовым коллизиям. Можно с уверенностью заявить, что последние изменения в законодательство о персональных данных будут развивать безопасность работы с данными и рискориентированный подход. Опрос российского бизнеса демонстрирует, что в качестве основных рисков участники считают угрозу конфиденциальности данных, кибербезопасности и соблюдения нормативных и законодательных данных.

В середине 2025 года Минцифры рассчитывает представить первую версию цифрового кодекса для регулирования сферы связи и IT. Создание цифрового ко-

декса для регулирования отношений в сфере связи и информационно-коммуникационных технологий (далее – ИКТ) вошло в Стратегию развития отрасли связи до 2035 года [8].

Тренд на создание регулирования ИИ прослеживается и в других юрисдикциях. В **Китае** в конце 2023 года были опубликованы 24 правила («Правила») регулирования ИИ [9]. Правила содержат интересные аспекты регулирования и в части интеллектуальной собственности. Созданные генеративными технологиями материалы (включая видео и аудио) должны быть соответствующим образом помечены. Подобная мера является хорошим шагом в сторону борьбы и с дипфейками. Кроме того, компании, занимающиеся разработкой технологий ИИ, должны будут использовать только «законные данные» для обучения своих моделей. Предусматривается создание четких механизмов рассмотрения жалоб от пользователей.

В октябре 2023 года в **США** был подписан Указ о мерах безопасности, связанных с развитием ИИ [10]. В документах выделены основные риски, среди которых крупные генеративные модели, содержащие миллиарды параметров. Документ также подчеркивает важность идентификации материала, созданного ИИ (водяным знаком/маркировкой). Отмечается, что без гарантий ИИ может поставить под угрозу конфиденциальность американцев. ИИ не только облегчает извлечение, идентификацию и использование персональных данных, но и повышает стимулы для этого, так как компании используют данные для обучения систем ИИ. В указе три основных акцента: безопасность/оборона США, конфиденциальность данных и идентификация материалов, созданных ИИ.

Также в 2023 году Закон об ИИ был принят в **ЕС** [11]. Ключевая особенность закона – рискориентированный подход. В Законе системы ИИ разделены на группы в зависимости от риска, который они несут:

– Запрещенные ИИ (например, системы, которые классифицируют лиц, создают социальный рейтинг, собирают и анализируют фото с камер наблюдения и т. п.). Оговоримся, что запрещены они скорее для выхода на рынок, но в исключительных случаях их использование допустимо (правоохранительные органы).

– ИИ с высоким уровнем риска. Для таких продуктов обязательна регистрация в специальном реестре с общим доступом, проведение оценки воздействия на права человека, создание специальных систем управления и контроля над ИИ и иные требования.

– ИИ с умеренным риском или без риска. Такие системы/продукты должны отвечать базовым принципам прозрачности.

Основной акцент регулирования сделан на этическую сторону. В целом развитие регулирования в сфере ИИ в разных юрисдикциях основано на схожих принципах: безопасность, рискориентированный подход, создание условий для прогресса, защита прав человека.

Искусственный интеллект и интеллектуальная собственность. Данные являются тем топливом, которое необходимо для работы генеративных систем. В погоне за созданием новых продуктов предприниматели зачастую используют информацию, получение которой не всегда оформлено должным образом с правовой точки зрения. Обучение генеративного ИИ возможно по двум сценариям:

– компания/субъект самостоятельно предоставляет системе данные;

– компания/субъект обращается в специализированные организации, которые занимаются обучением генеративного ИИ.

Во всех сценариях есть ряд схожих рисков, а именно: способ получения данных, достоверность содержания, юридическое оформление получения и дальнейшей передачи. Кроме того, часть сервисов обучаются на основе материалов из Интернета, где много произведений, защищенных авторским правом. Все актуальнее становится проблема использования для обучения систем персональных и биометрических данных граждан.

Среди рисков ИИ для интеллектуальной собственности WIPO дополнительно отмечает утечку конфиденциальной/коммерческой информации. При разработке продуктов для бизнеса для обучения зачастую используется конфиденциальная информация, представляющая коммерческую ценность. Если должным образам не контролировать этот процесс, также возможна утечка данных.

В связи с юридической неопределенностью в отношении регулирования интеллектуальной собственности во многих юрисдикциях возникают судебные споры. Традиционно правоприменитель быстрее законодателя сталкивается с новыми вопросами права, что приковывает внимание к разбирательствам, где еще не сформировано специальное регулирование. Не исключение и споры, связанные с законностью использования материалов для обучения ИИ. Например, в 2023 году Getty Images подала иск против Stability AI, утверждая, что их изображения были использованы для обучения ИИ без разрешения. Истец утверждал, что ответчик использовал более 12 млн изображений из фотобанка истца без разрешения и финансовой компенсации, построив на этом свой бизнес. Важность дела связана не только с прецедентом правового обличия использования интеллектуальной собственности в обучении, но со стимулированием законодателя в создании соответствующего регулирования. В том же 2023 году гильдия авторов и семнадцать всемирно известных писателей подали судебный иск в Южный округ Нью-Йорка против компании OpenAI, разработавшей ChatGPT, обвиняя ее в нарушении авторских прав.

Еще одним заметным делом, касающимся авторского права и использования генеративного ИИ, был кейс авторов против OpenAI. В сентябре 2023 года группа авторов во главе с Гильдией авторов подала коллективный иск против компании OpenAI в США. В число истцов входят такие известные авторы, как Джордж Р. Р. Мартин, Джон Гришэм, Джоди Пиколт и др. Всего в иске участвуют более десяти известных писателей. Авторы утверждали, что OpenAI использовала их произведения без разрешения для обучения своих языковых моделей, таких как GPT-3.5 и GPT-4. Кроме того, истцы заявили, что их работы были загружены с пиратских электронных библиотек при обучении ИИ, что привело к созданию текстов, имитирующих их стиль. По мнению авторов, это нарушает их авторские права и угрожает их доходам. Иск также содержал обвинения в создании производных работ на основе оригинальных произведений. Например, среди заявлений содержится указание на попытки генерации новых томов популярного цикла «Песнь Льда и Огня» Джорджа Р. Р. Мартина с помощью ИИ. Это также рассматривается как нарушение прав на оригинальные произведения. На сегодняшний день были проведены предварительные судебные заседания, и сбор доказательств начался в ноябре 2023 года [12].

Также небезынтересным кажется дело 2022 года разработчиков против GitHub, Microsoft и OpenAI. Иск был направлен в первую очередь против GitHub Copilot. В своем иске истцы указали, что фрагменты их кода были скопированы без указания авторства оригинальных разработчиков. Истцы также сослались на положения Закона об авторском праве в цифровую эпоху (DMCA), в частности раздел 1202 (b)(2), который регулирует защиту информации, связанной с управлением авторскими правами. Они обвинили GitHub в нарушении DMCA, утверждая, что компания удалила важную информацию о происхождении кода из его фрагментов, что привело к нарушению авторских прав. В ходе судебного разбирательства многие из предъявленных исков были отклонены. Позже суд отклонил еще три иска, что стало значительной победой для ответчиков. Судья пришел к выводу, что представленных доказательств в материалах дела недостаточно для установления сходства между сгенерированным кодом и GitHub и кодом с открытыми лицензиями, которое использовалось для обучения системы. Суд не счел, что есть нарушения DMCA. Однако нужно учесть, что на решение суда сильно повлияли изменения, внесенные в ходе разбирательства в GitHub. Именно эти обновления позволили сервису предлагать на выходе предоставлять отдельные и измененные фрагменты кода, а не копировать исходный материал. В свою очередь, для демонстрации вероятности повторного использования кода привели в качестве доказательства исследование в области ИИ [13]. Суд отказал в приобщении данного доказательства. Указанное исследование посвящено запоминанию данных в нейронных языковых моделях, а также аспектам запоминания, влияющих на приватность/полезность/справедливость работы подобных моделей.

Несмотря на отклонение судом большинства претензий, два основных вопроса остаются спорными, а именно:

– Нарушение лицензии на открытый исходный код. Заявители утверждают, что GitHub нарушил условия лицензии.

– «Нарушение доверия». Заявители также обвиняют ответчика в нарушении доверительных отношений между GitHub и сообществом разработчиков. По сути, разработчики, загружая свой код, не предполагали, что он будет использован для обучения модели. Кроме того, разработчики не были указаны в качестве авторов.

Небезынтересным кажется дело Thomson Reuters Enterprise Center против ROSS Intelligence Inc. В 2020 году Thomson Reuters Enterprise Center и ее дочерняя компания West Publishing Corporation подали иск против ROSS Intelligence Inc. Основные претензии истцов были сфокусированы на незаконном использовании материалов для разработки продукта (инструмент для поиска юридической информации с использованием ИИ). Это одно из наиболее релевантных дел, связанных со столкновением ИИ с авторским правом, при использовании проприетарных баз данных. Кроме того, ROSS Intelligence Inc. использовал бота для скачивания контента, а затем использовал в целях обучения своей ИИ-модели. Истец заявил, что эти материалы (например, заголовки и ключевые номера) защищены авторским правом и их использование без лицензии нарушает интересы истца. Исход дела может существенно повлиять на практику в части «добросовестного использования» для разработчиков ИИ-сервисов/моделей.

Заключение. В условиях стремительного развития ИИ проблема защиты интеллектуальной собственности становится все более актуальной. Существует

опасность крайних позиций. Так, излишнее регулирование затормозит технологический рост, что приведет к отставанию. Обратное может привести к ситуации, когда случится массовое нарушение интеллектуальной собственности. Кроме того, важно обсуждение правомерности использования материалов, защищенных авторским правом, для обучения ИИ, а также регулирование возникновения производных произведений в сфере ИИ.

Безусловно, главная угроза для интеллектуальной собственности – это незаконное использование объектов для обучения ИИ. Речь не только о текстовых материалах, но и о музыкальных произведениях, изображениях и т. д. Нельзя согласиться с позицией, что подобная ситуация связана с отсутствием четкого правового регулирования, так как существующее законодательство в большинстве юрисдикций дает вполне понятный ответ о необходимости получения соответствующей лицензии.

Для обеспечения справедливого использования интеллектуальной собственности при взаимодействии с ИИ необходимо:

– Совершенствование законодательства. На фундаментальном уровне правовое регулирование дает ответы на существующие вопросы в части ИИ, однако необходимо дополнение специальными нормами.

– Обеспечение прозрачности. Необходимо обеспечить доступ к информации о том, какие данные используются для обучения ИИ. Кроме того, авторам необходимо предоставить возможность контролировать в полной мере использование их произведений.

– Коммерческая основа. Важно дать авторам возможность получать отчисления за использование их произведений для обучения ИИ.

Указанные меры помогут найти баланс между инновациями в области ИИ и защитой интеллектуальной собственности, что будет способствовать развитию технологий и обеспечению соблюдения прав авторов.

Список литературы

1. Решение Арбитражного суда Московской области от 26 апреля 2024 г. по делу № А41-101804/23 // СПС «ГАРАНТ» [Электронный ресурс]. – URL: www.garant.ru (дата обращения: 01.09.2024).

2. Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (с изменениями и дополнениями)» // СПС «ГАРАНТ» [Электронный ресурс]. – URL: www.garant.ru (дата обращения: 01.09.2024).

3. Указ Президента Российской Федерации от 15 февраля 2024 г. № 124 «О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» и в Национальную стратегию, утвержденную этим Указом» // СПС «ГАРАНТ» [Электронный ресурс]. – URL: www.garant.ru (дата обращения: 01.09.2024).

4. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «ГАРАНТ» [Электронный ресурс]. – URL: www.garant.ru (дата обращения: 01.09.2024).

5. Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // СПС «ГАРАНТ» [Электронный ресурс]. – URL: www.garant.ru (дата обращения: 01.09.2024).

6. Федеральный закон от 14 июля 2022 г. № 323-ФЗ «О внесении изменений в часть вторую Налогового кодекса Российской Федерации» (с изменениями и дополнениями) // СПС «ГАРАНТ» [Электронный ресурс]. – URL: www.garant.ru (дата обращения: 01.09.2024).

7. Письмо Федеральной налоговой службы от 7 марта 2023 г. № СД-4-3/2672@ «О кодах для декларации по налогу на прибыль» // СПС «ГАРАНТ» [Электронный ресурс]. – URL: www.garant.ru (дата обращения: 01.09.2024).

8. Распоряжение Правительства Российской Федерации от 24 ноября 2023 г. № 3339-р // СПС «ГАРАНТ» [Электронный ресурс]. – URL: www.garant.ru (дата обращения: 01.09.2024).

9. China Takes Friendlier Approach to AI in Finalized Guidelines // Bloomberg [Электронный ресурс]. – URL: https://www.bloomberg.com/news/articles/2023-07-13/china-unveils-final-version-of-generative-ai-rules (дата обращения: 12.05.2024).

10. FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence // The White House [Электронный ресурс]. – URL: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/ (дата обращения: 19.05.2024).

11. Artificial intelligence act [Электронный ресурс] // EU Artificial intelligence act [Электронный ресурс]. – URL: https://artificialintelligenceact.eu/the-act (дата обращения: 25.05.2024).

12. Guild v. OpenAI Inc. // Leagle [Электронный ресурс]. – URL: https://www.leagle.com/decision/infdco20231205626 (дата обращения: 21.06.2024).

13. Carlini N., Lee K., Ippolito D., Tramèr F., Jagielski M., Zhang C. Quantifying Memorization Across Neural Language Models. ICLR, Google Research, University of Pennsylvania, Cornell University, 2023. – URL: https://arxiv.org/pdf/2202.07646 (дата обращения: 01.09.2024).

А. Ю. Чурилов,
кандидат юридических наук,
Национальный исследовательский Томский государственный университет

ДЕПОНИРОВАНИЕ ОБЪЕКТОВ АВТОРСКОГО ПРАВА: ТЕОРИЯ И ПРАКТИКА

Аннотация. В статье рассматриваются вопросы депонирования объектов авторского права с использованием традиционных баз данных и блокчейн-технологий. Особое внимание уделено преимуществам и недостаткам каждого метода, а также правовым и техническим проблемам, которые могут возникнуть при их применении. Исследуется вопрос фиксации существования объекта авторского

права без депонирования и его влияние на защиту интеллектуальной собственности. Работа направлена на выявление практических проблем и поиск оптимальных решений для эффективного управления правами на объекты авторского права.

Ключевые слова: право, цифровые технологии, авторское право, депонирование, блокчейн, база данных, интеллектуальная собственность, фиксация, правовая защита

DEPOSITING COPYRIGHT OBJECTS: THEORY AND PRACTICE

Abstract. The article examines the issues of depositing copyright objects using traditional databases and blockchain technology. Special attention is given to the advantages and disadvantages of each method, as well as the legal and technical challenges that may arise. The study also explores the concept of registering the existence of copyright objects without depositing them and its impact on intellectual property protection. The work aims to identify practical problems and find optimal solutions for effective copyright management.

Keywords: law, digital technologies, copyright, depositing, blockchain, database, intellectual property, registration, legal protection

Введение. Вопрос фиксации факта существования объектов авторского права в настоящее время стоит довольно остро. Это связано со все более возрастающей ролью интеллектуальной собственности в капитализации юридических лиц, а также теми преимуществами, которые предоставляют хозяйствующим субъектам эти результаты интеллектуальной деятельности.

Ранее нами уже обсуждались теоретические проблемы, связанные с реализацией депонирования объектов авторского права для дальнейшего управления права на соответствующие объекты [3, 5], поэтому целью данной работы является освещение практических проблем, которые могут возникнуть при реализации подобного рода проектов.

Основная часть. Подчеркнем, что использование технологии блокчейн для депонирования не является безусловным преимуществом перед традиционными базами данных и системами хранения. Вряд ли можно согласиться с исследователями, отмечающими, что традиционное централизованное хранение объектов авторского права в связи с высокой скорость передачи, простотой копирования делает цифровые публикации чрезвычайно уязвимыми для плагиата, и права интеллектуальной собственности авторов – пользователей подобных систем не могут быть гарантированы [8]. Этот тезис представляется сомнительным, поскольку он создает впечатление о некой «неуязвимости» объектов, которые депонируются с использованием системы блокчейн.

Фиксация факта существования объекта авторского права может осуществляться двумя способами – с депонированием объекта и без такового.

Следует также отметить, что традиционные блокчейн-системы требуют больших вычислительных мощностей, что увеличивает стоимость транзакций и поддержания всей системы в целом с каждым новым депонируемым объектом, и тем самым делает использование технологии блокчейн для депонирования и фиксации прав довольно дорогой услугой. Разумеется, системы нового поколе-

ния, использующие технологии Proof-of-Stake, снижают энергозатраты на поддержание. Однако внедрение этих решений требует значительных инвестиций и обновления существующих инфраструктур, что может быть труднодостижимо для небольших организаций и правообладателей.

Кроме того, в настоящее время существует множество разных блокчейн-платформ (Ethereum, Binance Smart Chain и др.), каждая из которых имеет свои стандарты и протоколы. Это создает проблему совместимости как при обороте прав на депонируемые объекты, так и при переходе с одной системы на другую. Разумеется, для создания единой экосистемы представляется возможным разработать единые стандарты, которые позволят интегрировать различные блокчейн-системы. Согласование стандартов между платформами требует времени и усилий, а также соответствующего надлежащего и тщательно выверенного правового регулирования для обеспечения интероперабельности соответствующих систем. Однако внедрение единых стандартов, хотя и кажется привлекательным, вряд ли будет способствовать дальнейшему развитию технологии блокчейн. Также следует отметить, что блокчейн и смарт-контракты часто используются в международных отношениях, где действуют разные юридические механизмы охраны и защиты интеллектуальной собственности. Это может вызвать правовые конфликты, особенно в ситуациях, когда разные страны по-разному регулируют блокчейн.

Одной из ключевых особенностей блокчейн-систем является необратимость (окончательность) транзакций [4]. С точки зрения перспектив в процессе доказывания это, безусловно, является преимуществом – такая неизменность позволит с гораздо большей убежденностью утверждать, что депонированный объект оставался неизменным как по форме, так и по содержанию [7]. Вместе с тем это означает в том числе и то, что, если транзакция была совершена с ошибкой или в результате мошенничества, отменить ее невозможно. В области авторского права это может привести к серьезным проблемам, если, к примеру, исключительное право на произведения будет передано по ошибке.

Также в этой связи встает вопрос договорных отношений, возникающих в связи с оказанием услуги депонирования, особенно если депонирование осуществляется не в традиционных базах данных, а в блокчейн-системах. Допустим, правообладатель заключил договор с лицом, осуществляющим депонирование, и в дальнейшем договор был расторгнут. С учетом неизменности транзакций в сети блокчейн и невозможности их удаления, возникает вопрос, что в дальнейшем делать с депонированным объектом, поскольку договорные основания для его хранения отпали с прекращением договора, а удалить это невозможно. С одной стороны, как отмечал Верховный Суд РФ, 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 [2], с другой – отсутствие договорного основания хранения (оказания услуги) делает такое хранение нецелесообразным, и дорогостоящим – при этом с депонированным объектом фактически ничего сделать не получится.

Заключение. Подводя итог, можно отметить, что депонирование объектов авторского права является важным инструментом защиты интеллектуальной собственности в условиях цифровой экономики. Использование технологии блокчейн или традиционные базы данных для фиксации объектов авторского права имеют

свои преимущества и недостатки. Блокчейн предлагает неизменность данных и прозрачность транзакций, что делает его привлекательным для депонирования, однако высокая стоимость, энергозатраты и правовые риски, связанные с необратимостью операций в сети блокчейн, представляют перспективы его использования туманными. Традиционные базы данных, хотя и обеспечивают простоту реализации депонирования и меньшие затраты, не гарантируют полной безопасности данных и подвержены рискам изменения или удаления информации, что снижает их надежность и достоверность и, как следствие, доказательственную силу выдаваемых свидетельств.

Также важным аспектом является выбор подходящего способа фиксации факта существования объекта авторского права, будь то депонирование с хранением объекта или фиксация факта существования без хранения. Первый метод обеспечивает более высокую степень надежности и пригодности для большинства правовых ситуаций, но сопряжен с техническими и юридическими сложностями. Фиксация без депонирования, хотя и является наименее затратной для всех сторон, может быть недостаточной для эффективной защиты прав в случае споров.

Список литературы

1. Новоселова Л. А. Государственная регистрация программ для ЭВМ: модель будущего авторского права? // Вестник экономического правосудия Российской Федерации. – 2021. – № 1. – С. 62–71.

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. Чурилов А. Ю. К вопросу о возможности оборота интеллектуальных прав с использованием технологии блокчейн // Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции: в 6 т., Казань, 22 сентября 2023 года. – Казань: Познание, 2023. – С. 414–417.

4. Чурилов, А. Ю. Правовое регулирование применения технологии блокчейн. – М.: Юридический дом «Юстицинформ», 2021. – 152 с. – ISBN 978-5-7205-1739-7.

5. Чурилов, А. Ю. Фиксация и оборот исключительных прав на объекты авторского права с помощью смарт-контрактов: миф или реальность? // Актуальные проблемы российского права. – 2024. – Т. 19, № 3(160). – С. 89–99. – DOI: https://doi.org/10.17803/1994-1471.2024.160.3.089-099

6. Taherdoost H. Innovation Through Research and Development: Strategies for Success (Signals and Communication Technology). – Springer, 2024. – 331 p.

7. Qu K., Wang L. Blockchain Deposition and Copyright Protection Method for Self-Published Content Infringement // IEIS 2022. ICIEIS 2022. Lecture Notes in Operations Research / M. Li, G. Hua, X. Fu, A. Huang, D. Chang (Eds.). – Springer, Singapore. – DOI: https://doi.org/10.1007/978-981-99-3618-2_3

8. Zheng H., Xue Y., Xie W., Shi Z. A Blockchain Based Documentation Sharing Framework for Copyright Protection // Computational and Experimental Simulations in Engineering. ICCES 2023. Mechanisms and Machine Science / S. Li (Eds). Vol. 145. – Springer, Cham, 2024. – DOI: https://doi.org/10.1007/978-3-031-42987-3_80

ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Э. М. Гильманов,
старший преподаватель,
Казанский инновационный университет имени В. Г. Тимирясова
А. М. Бабаева,
студент,
Казанский инновационный университет имени В. Г. Тимирясова

ИСПОЛЬЗОВАНИЕ КРИМИНАЛИСТИЧЕСКИХ МЕТОДИК ДЛЯ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ В ЦИФРОВОЙ СФЕРЕ

Аннотация. В связи с тенденциями развития общества в целом криминалистика должна «идти в ногу» и применять все более современные инструменты и методики как для разработки, так и для применения научных достижений во имя предотвращения нетривиальных преступлений, доселе невиданных. Указом Президента РФ от 10 октября 2019 года № 490 «О развитии искусственного интеллекта в Российской Федерации» были провозглашены положения о возможном внедрении мощностей искусственного интеллекта в деятельность государственных органов. Анализу данного подзаконного нормативного положения и возможных путей его применения посвящено данное исследование.

Ключевые слова: искусственный интеллект, криминалистика, методы, преступление, цифровизация, киберпреступность, расследование

THE USE OF FORENSIC TECHNIQUES TO SOLVE CRIMES IN THE DIGITAL SPHERE

Abstract. Due to the trends in the development of society as a whole, criminology must keep up and apply more and more modern tools and techniques both for the development and application of scientific achievements in the name of preventing non-trivial crimes hitherto unseen.

Decree of the President of the Russian Federation on October 10, 2019 № 490 "On the development of artificial intelligence in the Russian Federation" announced provisions on the possible introduction of the capacities of artificial intelligence in the activities of state bodies. This study is devoted to the analysis of this subordinate regulatory provision and possible ways of its application.

Keywords: artificial intelligence, criminology, methods, crime, digitalization, cybercrime, investigation

Введение. В соответствии с современными положениями российского законодательства о развитии искусственного интеллекта, это технология, позволяющая использовать мощности компьютерного устройства для анализа большого объема данных. И это, в силу его природы, превосходит скорость и качество работы, обусловленные отсутствием эмоций (человеческого фактора).

Перспектива синтеза искусственного интеллекта с работой органов предварительного следствия и разработки новых методик представляется весьма успешной в силу титанических размеров баз данных, применяемых в ходе уголовного судопроизводства. Ведь, как известно, разнообразие способов совершения преступлений в цифровой сфере оставляет за собой и обуславливает возникновение цифровых следов [2. С. 130].

Основная часть. Преступление в парадигме компьютерных технологий (далее – киберпреступление) представляет из себя активное действие, наносящее обществу вред путем изъятия и незаконного присвоения сведений, составляющих информационную безопасность как личности, так и государства; информация о праве собственности на объекты, регулируемые гражданским законодательством, и многие другие правовые институты, связанные с информацией в информационно-телекоммуникационных сетях (Интернет).

Как и у каждой группы преступлений, у киберпреступлений есть своя специфика. Ей являются многочисленные и разноплановые инструменты, используемые при их осуществлении. В этой связи уникальная правовая природа киберпреступлений определяет и особенности криминалистических методов по противодействию им [1. С. 170–171].

С одной стороны, криминалистические методы борьбы имеют свои подходы к толкованию киберпреступлений: большой объем информационных данных, потенциально обладающий признаками противообщественной направленности. Стоит отметить, что из всех настолько проработанная возможность совершения деяния при помощи компьютерных технологий обозначена только при мошенничестве. С другой стороны, этому правовому субинституту присущи и общие черты расследования: способ совершения преступления, особенности оставления следов и следовой информации, личностные характеристики преступника [3. С. 36].

Проведение так называемой компьютерной криминалистики, исходя из названия, предполагает использование в ходе расследования навыков по использованию цифровых и технологических достижений науки. Это будет способствовать разработке новых методов по сбору, анализу, сохранению и регистрации доказательств. Например, после получения результатов судебной экспертизы следователи по борьбе с киберпреступностью связываются с компаниями, обеспечивающими подключение к информационно-телекоммуникационным сетям. Это происходит с целью выяснения, какие ресурсы или протоколы подключения использовались для совершения преступления [4. С. 30–31].

Также еще не до конца изученными являются возможности искусственного интеллекта к самообучению: его пределы, скоростные лимиты, количество используемого трафика (данный вопрос создает дополнительный мотив к призыву компаний, обеспечивающих соединение искусственного интеллекта с информационно-телекоммуникационной сетью Интернет к сотрудничеству с органами уголовного розыска). Что напрямую коррелирует с потенциальными возможностями методологии и инструментария криминалистики по отношению к расследованию киберпреступлений.

Заключение. Подводя итог, основополагающим отличием киберпреступлений является применение компьютеров в качестве «орудия» преступления. Соответственно, и методы криминалистической борьбы и противодействия им должны быть обеспечены новейшими достижениями компьютерной техники.

В частности, самым базовым применением искусственного интеллекта в борьбе с киберпреступлениями может послужить его использование в качестве инструмента более качественного анализа данных по определенной категории преступлений (например, преступлений против половой свободы и половой неприкосновенности или преступлений против экономики), включая в нее запись камер видеонаблюдения, точные координаты места совершения преступления и т. д.

Однако это упирается в нарушение конституционных прав и свобод человека и гражданина в плане сбора и применения личных данных преступника. Данная казуистика и будет являться камнем преткновения для законодателя, если искусственный интеллект как инструмент криминалиста найдет дальнейшее применение.

Список литературы

1. Болтенкова Ю. В. Особенности расследования преступлений, совершаемых с использованием IT-технологий в сфере компьютерной информации // Поколение будущего: Взгляд молодых ученых – 2022: сборник научных статей 11-й Международной молодежной научной конференции, Курск, 10–11 ноября 2022 г. Т. 2. – Курск: Юго-Западный государственный университет, 2022. – С. 170–174. – EDN: YZQBVM

2. Климова Я. А. Цифровая криминалистика: перспективы развития // Вестник Волгоградской академии МВД России. – 2020. – № 4(55). – URL: https://cyberleninka.ru/article/n/tsifrovaya-kriminalistika-perspektivy-razvitiya (дата обращения: 05.09.2024).

3. Сарычев А. В., Архипцев И. Н. Современное состояние раскрытия и расследования преступлений, совершаемых с использованием информационных технологий // Проблемы правоохранительной деятельности. – 2020. – № 1. – URL: https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-raskrytiya-i-rassledovaniya-prestupleniy-sovershaemyh-s-ispolzovaniem-informatsionnyh-tehnologiy.

4. Шевченко Е. С. О криминалистической трактовке понятия «киберпреступность» // Информационное право. – 2014. – № 3. – С. 29–32.

Е. С. Зиновьева,
адъюнкт,
Нижегородская академия Министерства внутренних дел
Российской Федерации

ДОВЕРИТЕЛЬНЫЙ АСПЕКТ ИНСТИТУТА ПОРУЧИТЕЛЬСТВА

Аннотация. В статье рассматривается вопрос доверия в институте поручительства, опираясь на субъективный аспект данного явления, а также на положения Уголовно-процессуального кодекса РФ. Данный вопрос имеет важное значение при выборе меры пресечения, содержащей аспекты поручительства как со сто-

роны правоохранительных органов, так и непосредственно со стороны подозреваемого/обвиняемого, однако принятие данного решения в настоящее время имеет ряд сложностей субъективного характера.

Ключевые слова: доверие, вред, выбор меры пресечения, следователь, поручительство, подозреваемый, закон

THE CONFIDENTIAL ASPECT OF THE INSTITUTION OF SURETY

Abstract. In the article, the author examines the issue of trust in the institution of surety, based on the subjective aspect of this phenomenon, as well as on the provisions of the Criminal Procedure Code of the Russian Federation. This issue is important when choosing a preventive measure containing aspects of surety, both on the part of law enforcement agencies and directly on the part of the suspect/accused, however, making this decision currently has a number of subjective difficulties.

Keywords: trust, harm, choice of preventive measure, investigator, surety, suspect, law

Введение. Понимание института поручительства отражается предположением, что межличностная ответственность лица, в отношении которого избирается личное поручительство, к самому поручителю, является первостепенной по отношению к ретроспективным мерам, предусмотренным ч. 4 ст. 103 УПК РФ, поскольку они служат лишь гарантом, подкрепляющим указанную ответственность.

Основная часть. Для избрания исследуемой меры пресечения следователю необходимо найти подтверждение оснований для доверия. Вместе с тем личное поручительство означает своего рода неоспоримое доверие к поручителю.

Точным можно считать предположение, что «факт доверия должен носить двойственный характер» [1. С. 35]. «Доверие к поручителю» предполагает под собой наличие следующих факторов:

– доверие следователя к поручителю;

– доверие следователя к подозреваемому (обвиняемому);

– доверие между поручителем и подозреваемым (обвиняемым).

При этом доверие между следователем и лицом, которому дается поручительство, ст. 103 УПК РФ не закрепляется в качестве обязательного условия, но само собой подразумевается в практике избрания этой меры. Предлагаем подробнее рассмотреть суть термина «доверие» как требование к личности самого поручителя:

1. потенциальный поручитель должен находиться в доверительных отношениях с обществом (заслуживать доверия со стороны системы правосудия);

– доверие со стороны общества в лице следователя или иного должностного лица, разрешающего вопрос об избрании меры пресечения по конкретному делу, устанавливается на предварительном (подготовительном) этапе, в ходе которого стороной защиты предоставляются необходимые документы, содержащие сведения, характеризующие личность ходатайствующего о роли поручителя гражданина [2];

2. потенциальный поручитель должен находиться в доверительных отношениях с подозреваемым или обвиняемым [3. С. 99];

– Объясняя вышеуказанный пункт, мы безусловно соглашаемся с точкой зрения М. А. Чельцова, согласно которой предусмотренная ст. 103 УПК РФ мера пресечения с подкрепляющей ее ответственностью, в своей сущности зиждется на том, что уклонение приводит к негативным последствиям для третьего лица, из чего можно заключить, что воздействие на обвиняемого (подозреваемого) носит опосредованный характер [4. С. 11], что также можно отнести к черте, определяющей сущность личного поручительства.

В то же время из нее вытекает и другая немаловажная сущностная черта, которую можно упрощенно именовать «принцип разделенной ответственности». Так, ретроспективные последствия в случае нарушения условий личного поручительства будут претерпевать как подозреваемый (обвиняемый), так и поручившееся лицо. Отсюда следует, что оба этих лица имеют стимул по обеспечению надлежащей реализации анализируемой меры.

Установление данного межличностного доверия просто необходимо. Как мы указали выше, ответственность подозреваемого/обвиняемого перед поручителем является первостепенной. К примеру, Е. Г. Васильевой указано, что эффективность этой меры пресечения находится в зависимости не только от доверия лица, избравшего меру, но и от доверия к поручителю со стороны того, кому дается поручение [5. С. 86]. Соответственно, следующее за избранием данной меры воздействие отчасти носит опосредованный характер, поскольку предполагает воздействие на психику одного путем помещения другого в зависимость от его поведения. Тем не менее смущает тот факт, что законодателем не определены критерии, по которым правоохранитель оценивает такое доверие. Видимо, смысл, заложенный в ст. 103 УПК РФ, предполагает, что, к примеру, следователь в каждом конкретном случае при определении степени доверия между поручителем и подозреваемым (обвиняемым) будет полагаться на свой жизненный опыт, что опять возвращает нас к проблеме излишней субъективности, способной вылиться в чрезмерную неоднородность следственно-судебной практики, в произвольную интерпретацию, имеющую явно неблагоприятное влияние на юридическую технику. Тем не менее описывать в самом УПК РФ все факторы, свидетельствующие о подобном межличностном доверии, нецелесообразно, поскольку это способно привести к излишнему перенасыщению нормы и, как следствие, ее усложнению, что, в свою очередь, опять повлекло бы неверное ее применение. С оглядкой на все описанные выше проблемы считается разумным рекомендовать суду высшей инстанции создать отдельное разъяснение по вопросам толкования положений ст. 103 УПК РФ. Такое разъяснение можно было бы поместить в уже существующий акт судебного толкования, касающийся мер пресечения: в Постановление Пленума Верховного Суда РФ от 19.12.2013 № 41 [6. С. 211], распространив его действие в том числе и на личное поручительство, которое существенно сложнее толковать однородно, нежели тот же залог, которому в данном документе уделено отдельное внимание. Хотелось бы предположить, что о действительности такой доверительной связи или обоснованности ее презумпции могут говорить обстоятельства, свидетельствующие о том, что подозреваемый или обвиняемый заинтересован в благополучии поручителя и, соответственно, чтобы он не был подвергнут ответственности по ч. 4 ст. 103 УПК РФ. Например, родственная связь между гражданином и потенциальным поручителем, профессиональная (трудовая) связь.

Заключение. Таким образом, два рассмотренных аспекта доверия тесно связаны друг с другом, поскольку оба необходимы для продуктивной реализации исследуемой процессуальной меры.

Список литературы

1. О практике применения судами законодательства о мерах пресечения в виде заключения под стражу, домашнего ареста и залога: Постановление Пленума Верховного Суда Российской Федерации от 19.12.2013 № 41 // Российская газета. – 2013. – № 294.

2. Баландюк О. В. О правовом положении личного поручителя в уголовном судопроизводстве // Российский следователь. – 2019. – № 13.

3. Васильева Е. Г. Меры уголовно-процессуального принуждения: монография / науч. ред. З. Д. Еникеев. – Уфа: РИО БашГУ, 2003.

4. Закомолдин А. В. Личное поручительство в системе мер пресечения: проблемы правоприменения // Вестник Самарской гуманитарной академии. Серия: Право. – 2018. – № 1(20).

5. Чельцов М. А. Советский уголовный процесс. – М.: Госюриздат, 1951.

6. Уголовный процесс: учебник для бакалавриата юридических вузов / О. И. Андреева [и др.]; под ред. О. И. Андреевой, А. Д. Назарова, Н. Г. Стойко, А. Г. Тузова. – Ростов н/Д: Феникс, 2018.

Э. Ю. Латыпова,
кандидат юридических наук, доцент,
Казанский инновационный университет имени В. Г. Тимирясова
Р. Р. Бадрутдинов,
магистрант,
Казанский инновационный университет имени В. Г. Тимирясова

ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ В СФЕРЕ КОМПЬЮТЕРНЫХ ИГР И ИХ ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

Аннотация. Мы живем в постоянно развивающемся мире, в мире различных изобретений и новых открытий. За последние десятилетия человечество начало активно внедрять в свою жизнь средства информатизации в различных видах деятельности, стало использовать информационные технологии в таких сферах жизни, как работа, учеба, развлечение, общение и многих других. Компьютерные игры можно отнести к одному из видов развлечений, в них играют для того, чтобы отвлечься, занять свободное время, именно поэтому в целом и можно сделать вывод о том, что они носят развлекательный характер. Особенный интерес со стороны правоохранительных органов вызывает факт того, что компьютерные игры сами по себе становятся пространством для совершения преступлений, таких как читерство, кибербуллинг, кража аккаунтов, фишинг-атаки. Совершение таких преступлений имеет высокий уровень общественной опасности в силу того, что сейчас к данным человека, которые могут украсть у него злоумышленники, подвязана почти вся его жизнь, и они представляют особенную для него ценность.

При совершении таких преступлений страдают многие аспекты жизни человека, например, кибербуллинг может негативно сказаться на эмоциональном состоянии тех людей, для которых игра становится не просто игрой, а чем-то намного большим.

Ключевые слова: информационные технологии, сеть Интернет, компьютерные игры, хакерство, читерство, кибербуллинг, кража аккаунтов, фишинг-атаки

CRIMES COMMITTED IN THE FIELD OF COMPUTER GAMES AND THEIR MAIN CHARACTERISTICS

Abstract. We live in a constantly evolving world, in a world of various inventions and new discoveries. Over the past decades, humanity has begun to actively introduce informatization tools into its life in various types of activities, began to use information technology in such areas of life as work, study, entertainment, communication and many others. Computer games can be attributed to one of the types of entertainment, they are played in order to distract themselves, to occupy their free time, which is why, in general, we can conclude that they are entertaining in nature. Particular interest from law enforcement agencies is the fact that computer games themselves become a space for committing crimes such as cheating, cyberbullying, account theft, phishing attacks. The commission of such crimes has a high level of public danger due to the fact that now almost his entire life is tied to a person's data, which can be stolen from him by intruders, and they are of particular value to him. When committing such crimes, many aspects of human life suffer, for example, cyberbullying can negatively affect the emotional state of those people for whom the game becomes not just a game, but something much more.

Keywords: information technology, Internet, computer games, hacking, cheating, cyberbullying, account theft, phishing attacks

Введение. Нельзя точно сказать, когда появилась первая компьютерная игра, однако же в некоторых источниках можно найти информацию о том, что первая видеоигра, в которую можно было играть на компьютере, была создана в 1958 году ученым-физиком Уильямом Хигинботом и носила название Tenis for two, что в переводе на русский означает «теннис для двоих». Ее особенность заключалась в том, что в нее могли играть сразу два человека, при помощи двух специальных ручек. Игра вызвала ошеломительный успех и стала прототипом многих современных офлайн-игр. Это значит, что компьютерные игры были придуманы уже более полувека назад, что является хоть и не слишком большим временным периодом, но достаточным для того, чтобы в мире компьютерных игр произошли различные изменения, преобразовавшие его в лучшую сторону.

Сейчас компьютерные игры вышли на новый уровень развития, в них играют как дети, так и взрослые. Но, конечно, большую популярность они имеют среди подрастающего поколения. Игра заменяет многим людям общение, благодаря тому, что человек, играющий в нее, уходит в вымышленный мир с головой и полностью погружается в него. Да, раньше компьютерные игры представляли из себя в основном симуляцию именно какой-либо игры, например, как в случае с теннисом для двоих. Но сейчас в них создаются не только миры, но и целые вселенные, различные сюжеты и их вариации, в общем, все то, чтобы человек мог

полностью уйти от реальности и проникнуться видеоигрой. При создании компьютерных игр может быть использован и искусственный интеллект [2. С. 88].

Актуальность данной работы обусловлена тем, что преступления в сфере компьютерных игр в настоящее время являются довольно серьезной проблемой как для самих игроков, так и для создателей компьютерных игр. С развитием новых технологий мир игровой индустрии приобретает все большее значение, привлекает внимание сотни тысяч игроков по всему миру. Однако вместе с активным ростом популярности компьютерных игр растет и количество преступлений, совершаемых в них, начиная от самого распространенного мошенничества до серьезных кибератак. Именно поэтому важно следить за пространством видеоигр и принимать меры по защите и предотвращению совершения различных преступлений, которые наносят вред не только отдельно взятому игроку, но и игровым компаниям.

Основная часть. Перед тем как разбирать основные характеристики данного явления, стоит разобраться в том, что представляют из себя преступления, совершаемые в пространстве компьютерных игр. Как уже было отмечено ранее, изучаемый вид преступления начал проявлять себя относительно недавно, в силу того, что сам по себе мир компьютерных игр достаточно молод, именно поэтому точного определения преступлениям, совершаемым в сфере компьютерных игр, законодатель не дает. Данный вид преступлений имеет свою специфику и особенности, отличающие его от иных видов общественно опасных деяний. Таким образом, преступлениями в сфере компьютерных игр являются действия, нарушающие установленные в той или иной игре правила, а иногда и законы, связанные с неправомерным доступом к конфиденциальной информации, завладением чужим аккаунтом, кражей банковских реквизитов в корыстных целях и др. Главной отличительной чертой изучаемого явления является то, что совершается оно в виртуальном пространстве, а это в свою очередь делает его довольно трудно раскрываемым, имеющим высокий уровень латентности и создающим угрозу кибербезопасности.

Основными характеристиками преступлений, совершаемых в сфере компьютерных игр, являются следующие:

– совершение преступного деяния в виртуальном пространстве;

– отсутствие отдельного состава за данный вид преступления;

– использование различных современных технологий, как инструмента совершения преступления;

– глобализация преступлений в сфере компьютерных игр.

Разберем каждую из них более подробно.

Итак, как уже было отмечено, главной отличительной чертой изучаемого вида преступлений является то, что совершается оно в виртуальном пространстве. Наличие факторов, связанных с тем, что в виртуальном пространстве не действуют законы физики и по-другому течет время, характеризует виртуальное пространство как особенную среду, в которой довольно тяжелым представляется проследить за тем или иным правонарушением. В данной среде игроки могут создавать аватаров и посредством управления ими играть в те или иные игры как самостоятельно, так и совместно с другими участниками. Именно то, что преступное

деяние совершается в раскрываемом киберпространстве, и вызывает определенные трудности при определении характера совершенного преступления, а также при попытке раскрыть его [3. С. 211]. В отличие от реального мира, в котором намного легче выявить факт совершения преступления.

Если рассматривать преступные деяния, совершаемые в компьютерных играх со стороны уголовно-правовой ответственности, стоит отметить тот факт, что в уголовном законодательстве нашей страны не существует конкретной нормы, предусматривающей наказание за данный вид преступления, что способно вызывать определенные трудности при квалификации совершенных пользователями компьютерных игр, общественно опасных деяний.

Одним из самых распространенных видов «преступлений», которое можно совершить в компьютерной игре, является читерство, которое подразумевает использование различных технологий и кодов, например, для так называемой прокачки своего персонажа, приобретение преимущества в той или иной игровой вселенной. Читерство, являясь одним из видов использования сторонней аппаратуры и программного обеспечения, представляет опасность именно потому, что выявить и распознать данную технологию достаточно тяжело.

Еще одной характеристикой преступлений, совершаемых в сфере компьютерных игр, является их глобализация. С ростом различных способов совершения преступлений в киберпространстве, а также с учетом того, что в мире идет активная информатизация и внедрение в жизнь людей все новых и новых компьютерных игр, растет и количество преступлений, совершаемых в них.

В целом, исходя из всего вышеперечисленного, можно сделать вывод о том, что преступления, совершаемые в сфере компьютерных игр, носят серьезный уровень общественной опасности. Они отличаются своей латентностью, неизвестной природой и спецификой [4]. Также, например, по мнению Ю. М. Батурина и С. В. Полубинской, развитого права в играх нет. Там действуют нормы, установленные разработчиком, обычаи виртуального делового оборота, но применяются правовые нормы реального мира, хотя и достаточно неопределенные ввиду множественности правовых систем [5. С. 12]. Тем самым авторы подчеркивают, что единой правовой системы также, как и системы санкций за те или иные правонарушения, в киберпространстве пока не сложилось. Однако некоторые нормы права можно трактовать по отношению к данному явлению. И все это вызывает определенные трудности при попытке привлечь пользователя компьютерной игры к какому-либо виду ответственности.

Именно поэтому российское законодательство по отношению к преступлениям, совершаемым в сфере компьютерных игр, требует особого внимания и доработки. Хотя речь и идет об определенных поправках и смене нормативно-правовой базы, не стоит забывать о том, что мы живем в современном мире, в котором такое создание человечества, как компьютерная игра, будет активно развиваться еще не одно десятилетие.

Видами преступлений, совершаемых в сфере компьютерных игр, являются специфические разновидности нарушений и вреда, происходящих в пространстве виртуальной реальности. Такие виды преступлений, хоть и не способны нанести физический вред здоровью человека, но все равно являются опасными в силу того,

что могут повлиять на финансовое благополучие человека, на безопасность и конфиденциальность его данных [6. С. 38], а также на его моральное состояние. Существуют различные виды преступлений, в компьютерных играх, приведем самые популярные, которые имеют наиболее частое проявление в рассматриваемой среде, это такие как:

– читерство – пожалуй, одно из самых знаменитых преступлений в компьютерных играх, о котором слышал почти каждый [7. С. 293];

– кибербуллинг;

– кража аккаунтов и конфиденциальных данных [8. С. 294];

– фишинг-атаки.

Таким образом, на практике существует большое количество видов преступлений, совершаемых в сфере компьютерных игр. Их главной целью всегда является либо завладение чужим имуществом, либо желание унизить пользователя игры, либо иные мотивы, которые подчеркивают негативную сторону данных деяний. Все данные виды преступлений схожи между собой [9. С. 295], труднораспознаваемы, и способны нанести серьезный урон для пользователей.

Уголовное законодательство нашей страны не предусматривает отдельных норм ответственности за совершение преступлений в сфере компьютерных игр, что вызывает определенные трудности при квалификации преступных деяний в виртуальном пространстве.

Уголовное право имеет возможность действовать и применяться в сфере преступлений в компьютерных играх лишь в некоторых случаях. Главной проблемой остается то, что виртуальное имущество пока еще не признано объектом правоотношений, возникающих в рассматриваемой сфере, в отличие от безналичных средств платежа, которые Постановлением Правительства РФ «О судебной практике по делам о мошенничестве, присвоении и растрате» были признаны предметом хищения в уголовном праве [10]. Согласно данному Постановлению, если при мошенничестве объектом преступления являются безналичные денежные средства, то по смыслу положения п. 1 примечаний к ст. 158 Уголовного кодекса РФ, а также ст. 128 Гражданского кодекса РФ кража безналичных средств платежа должна рассматриваться как хищение имущества. Безналичные денежные средства связаны с компьютерными играми посредством того, что многие игроки при регистрации на сайте игры и создании своего личного кабинета вводят реквизиты банковских карт [11]. Именно эти реквизиты и становятся в будущем объектом совершения такого вида преступлений в киберпространстве, как кража конфиденциальных данных в корыстных целях. Таким образом, при совершении вышеприведенного преступления правонарушителя можно привлечь к ответственности по ст. 158 УК РФ. В ст. 128 Гражданского кодекса РФ говорится о том, что к объектам гражданских прав относятся не только имущество, имеющее материальное выражение, но и иное имущество, в том числе и безналичные платежные средства.

Преступления в сфере компьютерных игр можно квалифицировать по ряду статей, находящихся в гл. 28 «Преступления в сфере компьютерной информации» УК РФ, а именно ст. 272–274. Но стоит отметить, что прямое указание на компьютерные игры в них опять же отсутствует [12. С. 83], и суд при определении наказания должен ссылаться на то, что можно отнести к неправомерному доступу

к компьютерной информации, созданию, использованию и распространению вредоносных компьютерных программ, а также нарушению правил эксплуатации средств хранения компьютерной информации.

При уголовно-правовой характеристике преступлений в сфере компьютерной информации стоит отметить, что некоторые виды таких деяний преследуются именно по аналогии с существующими в реальном мире уголовными преступлениями. Например, кража или же предусмотренное ст. 159 УК мошенничество в игровом пространстве может быть расценено правоохранителем как «киберпреступление» [13]. Или, например вопрос о наказании за кибербуллинг может на практике квалифицироваться по составам клеветы или оскорбления, так как в первую очередь такое нарушение унижает честь и достоинство человека и гражданина.

Таким образом, можно сделать вывод о том, что система уголовной ответственности за преступления в сфере компьютерных игр сложна и находится на стадии разработки. При анализе преступлений в изучаемом виртуальном пространстве стоит учитывать особенности законодательства конкретной страны и то, как законодатель трактует нормы права.

Заключение. Преступления, которые совершаются в киберпространстве, направлены в первую очередь на получение выгоды пользователями. Они способны нанести вред как всему игровому сообществу в целом, так и отдельному пользователю. В свою очередь рассматриваемые преступления носят повышенный уровень общественной опасности за счет того, что являются трудно раскрываемыми, имеющими высокий уровень латентности, а также за счет своей малоизученности.

Стоит отметить тот факт, что в законодательстве нашей страны имеются пробелы в вопросах, возникающих при совершении лицами таких преступлений. Российское законодательство по отношению к преступлениям, совершаемым в сфере компьютерных игр, требует особого внимания и доработки. Хотя речь и идет об определенных поправках и смене нормативно-правовой базы, не стоит забывать о том, что мы живем в постоянно развивающемся современном мире, в котором такое создание человечества, как компьютерная игра, будет активно развиваться еще не одно десятилетие.

Система уголовно-правовой ответственности за преступления в сфере компьютерных игр сложна и находится на стадии разработки. При анализе преступлений в изучаемом виртуальном пространстве стоит учитывать особенности законодательства конкретной страны и то, как законодатель трактует нормы права. Характер таких преступлений способен меняться под влиянием развития технологий в играх [14. С. 305], изменения правил их использования, а также тенденций уровня заинтересованности общества в них. Именно поэтому в сфере применения уголовной ответственности к правонарушителям, совершающим преступления в компьютерных играх возникают различные проблемы.

Преступления в сфере киберпространства включают в себя различные виды деяний, таких как мошенничество, кибербуллинг, кража аккаунтов, хакерство, продажа фальшивых игровых предметов и иные виды. Данные преступления опасны тем, что могут нанести ущерб как игрокам, так и разработчикам игр. Важным является осознавать потенциальные риски и принимать меры предосторожности, чтобы защитить себя и свои данные в онлайн-играх, не допустить того,

чтобы кто-либо завладел ими в корыстных целях. Также важно соблюдать правила и этические нормы виртуального мира [15. С. 98], чтобы избежать участия и развития преступной деятельности в рассматриваемом пространстве.

Подрастающее поколение все больше и больше отдаляется от живого общения, преимущественно переходя к такому виду развлечения как виртуальные игры. Уже сейчас, с условием разнообразных форм и способов совершения преступлений в сфере компьютерных игр важно думать о безопасности и комфорте игроков. Стоит уделять особенное внимание и постоянно работать над системой ответственности в киберпространстве, и тогда возможно с течением времени законодательство нашей страны сможет привести киберпространство к защищенной, комфортной и устойчивой форме.

Список литературы

1. Латыпова Э. Ю., Гильманов Р. Э., Бадрутдинов Р. Р. Роль правоохранительных органов и специальных служб в борьбе с преступлениями, совершаемыми в сфере компьютерных игр, и технические решения для их предотвращения // Правопорядок: история, теория, практика. – 2024. – № 2(41). – С. 109–114. – DOI: 696X-2024-39-4-109-114

2. 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.

3. Бегишев И. Р. Культура информационной безопасности: психолого-правовой аспект // Психология и право. – 2021. – Т. 11, № 4. – С. 207–220.

4. Latypova E. Yu., Nechaeva E. V., Gilmanov E. M., Aleksandrova N. V. Infringements on Digital Information: Modern State of the Problem [Электронный ресурс]. – URL: https//www.shs-conferences.org/articles/shsconf/abc/2019/03/shsconf_pedtp2018_10004.html (дата обращения: 10.03.2024).

5. Батурин Ю. М., Полубинская С. В. Что делает виртуальные преступления реальными // Труды Института государства и права Российской академии наук. – 2018. – Т. 13, № 2. – С. 9–35.

6. Латыпова Э. Ю. Некоторые аспекты уголовной ответственности за деяния, посягающие на неприкосновенность частной жизни // Oeconomia et Jus. – 2019. – № 2. – С. 35–45.

7. Гильманов Т. Э., Гордеев М. А. Мошенничество в сфере компьютерных игр: постановка проблемы // Казанские научные чтения студентов и аспирантов имени В. Г. Тимирясова – 2022: материалы XII Международной научно-практической конференции студентов и аспирантов, 16 декабря 2022 г. В 3 т. Т. 3. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – С. 293–295.

8. Гильманов Т. Э., Гордеев М. А. Мошенничество в компьютерных играх путем создания фейкового аккаунта // Казанские научные чтения студентов и аспирантов имени В. Г. Тимирясова – 2022: материалы XII Международной научно-практической конференции студентов и аспирантов, 16 декабря 2022 г. В 3 т. Т. 3. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – С. 292–293.

9. Гильманов Т. Э., Гордеев М. А. Способы использования мошенниками бесплатных скриптов для компьютерных игр // Казанские научные чтения студентов и аспирантов имени В. Г. Тимирясова – 2022: материалы XII Международной научно-практической конференции студентов и аспирантов, 16 декабря 2022 г. В 3 т. Т. 3. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – С. 295–296.

10. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Российская газета. –2017, 11 декабря. – № 280.

11. Малахов М. Миллионы за пиксели: 7 самых дорогих покупок в играх // Портал BRODUDE. – 4 июля 2022 г. [Электронный ресурс]. – URL: https://brodude.ru/milliony-za-pikseli-7-samyh-dorogih-pokupok-v-igrah (дата обращения: 10.03.2024).

12. Нечаева Е. В., Латыпова Э. Ю., Гильманов Э. М. Посягательства на цифровую информацию: современное состояние проблемы // Человек: преступление и наказание. – 2019. – Т. 27, № 1. – С. 80–86.

13. Сотрудники уголовного розыска Нижегородской области раскрыли кражу аккаунта в онлайн-игре World of Tanks стоимостью 70 тыс. руб. // РБК Технологии и медиа. [Электронный ресурс]. – 2016, 2 марта. – URL: https://www.rbc.ru/technology_and_media/02/03/2016/56d7293d9a79473f782ed597 (дата обращения: 05.09.2024).

14. Зелепукин В. Ю. Программные средства защиты информации // Теория и практика современной науки. – 2017. – № 5(23). – С. 304–307.

15. Латыпова Э. Ю., Гильманов Э. М., Абдуллина А. Е., Гильманов Р. Э. Влияние нравственно-моральных норм на содержание уголовно-правовых норм в Уголовном кодексе России // Вестник экономики, права и социологии. – 2022. – № 1. – С. 93–99.

А. Ф. Мотолько,
сотрудник,
Следственный комитет Республики Беларусь

БЕЛОРУССКИЙ ОПЫТ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННОЙ СИСТЕМЫ «СЛЕД»

Аннотация. В статье обозначается важность принятия мер противодействия кибепреступности, использования информационных систем при расследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий, раскрываются возможности используемой в Следственном комитете Республики Беларусь информационно-аналитической системы «След».

Ключевые слова: киберпреступления, информационно-коммуникационные технологии, информационно-аналитические системы, криминалистически значимая информация, идентификаторы

BELARUSIAN EXPERIENCE IN INVESTIGATING CYBER CRIMES USING THE INFORMATION SYSTEM “SLED”

Abstract. The article outlines the importance of taking measures to combat cybercrime, using information systems in the investigation of crimes committed using information and communication technologies, and reveals the capabilities of the information and analytical system “Sled” used in the Investigative Committee of the Republic of Belarus.

Keywords: cybercrimes, information and communication technologies, information and analytical systems, forensically significant information, identifier.

Введение. В последние годы в Республике Беларусь отмечается значительное увеличение количества регистрируемых преступлений, совершаемых с использованием информационно-коммуникационных технологий. Складывающаяся динамика ежегодного роста киберпреступности требует принятия эффективных мер противодействия, в том числе технического и технологического характера.

Основная часть. В соответствии со ст. 14 Закона Республики Беларусь «Об информации, информатизации и защите информации» Следственный комитет Республики Беларусь, являясь государственным органом, осуществляющим в пределах своей компетенции государственное регулирование и управление в области информации, информатизации и защиты информации, участвует в реализации единой государственной технической и технологической политики в сфере цифрового развития, формирует и используют информационные ресурсы, создает и развивает информационные системы и информационные сети, обеспечивает их совместимость и взаимодействие в информационном пространстве Республики Беларусь [1].

В соответствии со ст. 4 Закона Республики Беларусь «О Следственном комитете Республики Беларусь» одной из задач ведомства является совершенствование следственной работы, внедрение в практику достижений науки и техники, положительного опыта, прогрессивных форм и методов организации предварительного следствия [2].

В этой связи Следственным комитетом Республики Беларусь на постоянной основе реализуются меры, направленные на разработку и внедрение эффективных высокотехнологичных инструментов борьбы с преступностью.

На сегодняшний день самой большой проблемой, с которой приходится сталкиваться следователям при расследовании преступлений, являются большие массивы информации. И это не только сведения о телефонных соединениях сотовых операторов, выгрузки с мобильных телефонов и иных гаджетов с помощью специальных программных продуктов, сведения по банковским счетам, электронным кошелькам, информация о доступах в сеть Интернет от провайдеров.

В качестве примера: по одному из расследуемых в центральном аппарате Следственного комитета Республики Беларусь уголовных дел следователю потребовалось проанализировать и извлечь значимую информацию из сотен тысяч электронных писем; свести в единый массив и проанализировать данные о 500 тыс. преступных криптообменных операций. При этом результаты такой

аналитической работы необходимо было визуализировать и представить в материалах уголовного дела в пригодном для восприятия виде.

Это вызывает необходимость поиска высокоэффективных средств и приемов анализа больших данных. Следователи должны уметь находить и извлекать значимую для уголовного дела информацию, анализировать ее, визуализировать и использовать в ходе выяснения обстоятельств преступления и сбора доказательств по уголовному уделу,

Для решения таких задач в Следственном комитете Республики Беларусь разработана и внедрена ведомственная автоматизированная информационная система «След» (АИС «След»), которая предназначена для накопления и хранения наиболее значимой цифровой информации по уголовным делам в целях последующего автоматизированного изучения и анализа такой информации, в том числе путем решения информационно логических задач построения цепочек связей по совокупности взаимосвязанных объектов учета, установления взаимосвязей отдельных эпизодов преступлений между собой, а также с целью установления лица, подлежащего привлечению в качестве обвиняемого.

Формирование и наполнение АИС «След» осуществляется непосредственно самими следователями при производстве по материалам проверок и уголовным делам, которые вносят учетную криминалистически значимую информацию.

Доступ сотрудников Следственного комитета к информационной системе осуществляется через свой личный кабинет посредством ведомственной сети передачи данных. Порядок помещения следователями сведений в АИС «СЛЕД» и алгоритм последующего их анализа закреплены ведомственными нормативными правовыми актами.

Принцип работы и преимущества использования АИС «След» можно продемонстрировать на следующем примере. Допустим, следователь по поступившему заявлению гражданина о хищении денежных средств с карт-счета устанавливает, что потерпевший стал жертвой «фишинга». Компрометация карт-счета произошла при вводе реквизитов доступа на подменной веб-странице, ссылку на которую ему переслал злоумышленник в ходе переписки в мессенджере Telegram.

Возбудив уголовное дело и проведя неотложные процессуальные действия, следователь авторизируется в АИС «След» и заполняет краткую информацию о новом преступлении: номер дела, квалификация деяния, краткая фабула. Затем вносит сведения по каждому выявленному идентификатору, который использовался преступником. В приведенном примере это: «юзернейм» и числовой идентификатор пользователя Telegram, переславшего потерпевшему фишинговую ссылку; доменное имя сайта, на котором размещена подменная веб-страница; реквизиты банковской платежной карты, на счет которой переведены денежные средства с карт-счета потерпевшего. С момента окончания ввода эта информация становится доступной всем следователям Следственного комитета Республики Беларусь, являющимся пользователям АИС «След», которые могут получить ее при осуществлении соответствующих поисковых запросов.

В ходе дальнейшего расследования по этому же уголовному делу следователь получает сведения по банковскому счету, на который преступник вывел денежные средства с карт-счета потерпевшего, а также узнает IP-адреса и UDID

устройства, с использованием которых преступник осуществлял удаленное управление этим счетом, номера электронных кошельков, на которые им были переведены похищенные денежные средства. Эти данные следователь дополнительно вносит в АИС «След».

И так далее, вплоть до окончания расследования, вся криминалистически значимая информация по уголовному делу аккумулируется в информационной системе, которая в режиме реального времени осуществляет сопоставление вносимых данных с уже имеющимися и выводит информацию о выявленных совпадениях.

При этом функционал системы предусматривает многоуровневый поиск совпадений. Допустим, если один следователь по своему уголовному делу выявил совпадение с уголовным делом своего коллеги из другого следственного подразделения по электронному кошельку, то уже по другому уголовному делу установлена связь по номеру банковской карточки, но уже с третьим уголовным делом, которое в свою очередь связано с рядом других уголовных дел по адресу криптокошелька и т. д.

В результате такого пересечения идентификаторов формируется «дерево совпадений», которое в удобной форме визуализации выводится с отображением цепочек связей между разными уголовными делами.

Заключение. Появилась возможность оперативного выявления и документирования фактов движения денежных средств в ходе осуществления преступной деятельности, связей между получателями денежных средств, источниками их происхождения, временем получения и местом хранения. Изучение полученных из АИС «След» сведений о совпадении идентификаторов позволяет также установить причастность привлекаемого к ответственности лица к другим совершенным аналогичным преступлениям, а также выявить соучастников преступления.

Список литературы

1. Об информации, информатизации и защите информации [Электронный ресурс]: Закон Республики Беларусь от 10 ноября 2008 г. № 455-З // Информационно-поисковая система «Эталон» / Национальный центр правовой информации Республики Беларусь.

2. О Следственном комитете Республики Беларусь [Электронный ресурс]: Закон Республики Беларусь от 13 июля 2012 г., № 403-З // Информационно-поисковая система «Эталон» / Национальный центр правовой информации Республики Беларусь.

К. Д. Муратов,
доктор юридических наук, доцент,
Казанский инновационный университет имени В. Г. Тимирясова;
Н. Э. Плачинта,
аспирант,
Казанский инновационный университет имени В. Г. Тимирясова

ЦИФРОВЫЕ ДОКАЗАТЕЛЬСТВА В СИСТЕМЕ МЕЖОТРАСЛЕВЫХ ВЕЩЕСТВЕННЫХ ДОКАЗАТЕЛЬСТВ

Аннотация. В исследовании обосновывается возможность создания единого информационного доказательственного поля вещественных доказательств, обеспечивающего универсальные процедуры при выявлении, изъятии, оценке и хранения вещественных доказательств в межотраслевых правоотношениях. Цифровая информация, существующая в виде видео-звуко-кино-интернет-файлов и сайтов, зафиксированная на электронных носителях информации, отражающая факты, сведения о предметах, документах, имуществе, о цифровом рубле виртуальных активах, денежных средствах, культурных ценностях, транснациональных хакерских группах, создает единое информационное поле цифровых вещественных доказательств расследуемого преступления – «цифровая криминалистическая модель преступления». Кроме того, установленные процессуальные правила применения электронной информации в отраслевом законодательстве обеспечивают единую нормативную цифровую модель доказательственного значения вещественных доказательств. Многофункциональная сущность цифровых вещественных доказательств и возможность их одновременного применения в доказывании по уголовному, гражданскому и административному делу позволит создать «единое межотраслевое цифровое информационное поле вещественных доказательств». Цель исследования состоит в обосновании актуальности и своевременности формирования цифрового доказательственного поля вещественных доказательств, и прежде всего четкого определения сущности, значения и правовых последствий применения цифровых технологий. Компьютерные атаки, компьютерный инцидент, криптовалюта, технология блокчейна, робототехника, аутентификация и идентификация персональных данных и их применения в правоприменительной практике требует создания нормативной основы. Результаты: показан зарубежный и национальный опыт применения цифровой терминологии при формулировании уголовно-правовых и процессуальных норм. Применение новых информационных технологий при доказывании обеспечит формирование цифровой криминалистической модели преступления при транснациональных расследованиях, преступлений в форме онлайн-технологий с применением технологий искусственного интеллекта. Предлагается многоуровневое и многофункциональное применение цифровых вещественных доказательств в их единстве и дифференциации в системе межотраслевых связей уголовного процесса, что позволит создать единое межотраслевое цифровое информационное поле вещественных доказательств.

Ключевые слова: цифровизация, информационные технологии, цифровые вещественные доказательства, межотраслевые связи, компьютерные и транснациональные виртуальные преступления

DIGITAL EVIDENCE IN THE SYSTEM OF INTER-INDUSTRIAL EVIDENCE

Abstract. The study substantiates the possibility of creating a single information evidentiary field of material evidence, providing universal procedures for the detection, seizure, evaluation and storage of material evidence in inter-branch legal relations. Digital information existing in the form of video-sound-film-Internet files and sites, recorded on electronic media, reflecting facts, information about objects, documents, property, about the digital ruble virtual assets, cash, cultural values, transnational hacker groups, creates a single information field of digital material evidence of the crime under investigation - "digital forensic model of crime". In addition, the established procedural rules for the use of electronic information in industry legislation provide a unified normative digital model of the evidentiary value of material evidence. The multifunctional nature of digital material evidence and the possibility of its simultaneous use in proving in criminal, civil and administrative cases will allow the creation of a "unified inter-industry digital information field of material evidence." The purpose of the study is to substantiate the relevance and timeliness of the formation of a digital evidentiary field of material evidence and, above all, a clear definition of the essence, meaning and legal consequences of the use of digital technologies. Computer attacks, computer incidents, cryptocurrency, blockchain technology, robotics, authentication and identification of personal data and their use in law enforcement practice require the creation of a regulatory framework. Conclusions: the foreign and national experience of using digital terminology in formulating criminal law and procedural norms is shown. The use of new information technologies in proving will ensure the formation of a digital forensic model of crime in transnational investigations, crimes in the form of Online technologies using artificial intelligence technologies. A multi-level and multifunctional use of digital material evidence in their unity and differentiation in the system of inter-branch connections of the criminal process is proposed, which will create a single inter-branch digital information field of material evidence.

Keywords: digitalization, information technology, digital evidence, intersectoral connections, computer and transnational virtual crimes

Введение. В современном законодательстве обновляется традиционная терминология и появляется новая, регламентируя новые общественные отношения: расширено понятие «имущественные права (включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права)» и как имущество определен цифровой рубль. Действительно, в ряде решений Верховного Суда РФ говорилось о новых возникающих на практике правоотношениях: получении доходов от использования бездокументарных ценных бумаг или цифровых прав, о виртуальных активах (криптовалюте) как предмете преступления.

Теория доказательств, объединяющая публично-правовые и гражданско-правовые отношения, как представляется, получила новый импульс для дальнейших исследований. «Цифровая» терминология, официально зафиксированная в отечественном и зарубежном законодательстве, должна быть исследована с позиций и уголовного права, и уголовного процесса, и криминалистики. Кроме того,

многочисленные дискуссии об информационном доказательственном поле при установлении фактических обстоятельств в правовом споре (публичном или частном), неизбежно приводит к общим и особенным выводам в этой сфере при анализе правоотношений субъектов права. Так, например, формулируются предложения по цифровизации нормотворчества и правоприменения: создать «электронные кодексы», генерировать типовые судебные решения при помощи искусственного интеллекта и создать автоматизированную систему контроля судебной практики.

В последние годы совершенствование уголовного, уголовно-процессуального законодательства и правоприменительной практики привело к многочисленным изменениям в уголовно-правовой терминологии, требующим разъяснений. Верховный Суд РФ практически полностью разъяснил весь терминологический ряд, который применяется при формулировании конструктивных и квалифицирующих признаков преступлений в сфере компьютерной информации и иных преступлений при использовании электронных и информационно-телекоммуникационных сетей, сети Интернет: «компьютерная информация», «персональные компьютеры», «встроенные вычислительные устройства», «средства и технологии сбора и передачи информации», «компьютерная программа с учетом положений статьи 1261 Гражданского кодекса Российской Федерации». Определены уголовно-правовые последствия вторжения в компьютерную информацию: «уничтожение», «блокирование», «модификация», «копирование», «нейтрализация средств защиты», «изменение пароля к учетной записи», «создание вредоносных компьютерных программ или иной вредоносной компьютерной информации», «нарушение установленного нормативными правовыми актами порядка уничтожения, блокирования, модифицирования, копирования компьютерной информации или нейтрализации средств ее защиты», «распространение вредоносных компьютерных программ», «использование вредоносных компьютерных программ». Все эти термины характеризуют «Цифровую модель преступления – corpus delikte (*тело преступления – Прим. автора*) в сфере уголовно-правовой охраны цифровой (электронной) информации и гарантирует ее безопасность: ст. 272, 273, 274, 274.1, 159.3, 159.6 УК РФ и др.

Постановка задачи. Таким образом, обоснованной целью настоящего исследования является аргументация единства и дифференциации применения доказательственной информации и выяснения современных межотраслевых последствий применения цифровой информации как сведений о фактах объективного мира на материальных носителях – межотраслевых вещественных доказательствах (жесткие диски-накопители, флеш-карты, диски, электронные устройства, компьютеры, телефоны, смартфоны, устройства с вычислительным устройствами (*терминология из указанного Постановления Верховного Суда РФ. – Прим. автора*). В связи с этим можно поддержать мнение о социальной значимости цифрового доказательства (цифровой документ, цифровая фотография, цифровое видео, носители цифровой информации).

Для достижения цели были сформулированы следующие задачи:

– показать дискуссию о цифровизации доказательственной деятельности субъектов права;

– показать значение информационного поля о предметах, документах, электронной информации и иного изъятого имущества в межотраслевых связях уголовного процесса;

– формирования информационного поля вещественных доказательств – «Цифровая модель преступления – corpus delikte»;

– доказать многоуровневое и многофункциональное применение цифровых вещественных доказательств в их единстве и дифференциации в системе межотраслевых связей уголовного процесса;

– предположить перспективу онлайн-расследований транснациональных преступлений.

Методика. В данном исследовании применена совокупность способов и приемов познания объективной реальности: теоретическая (диалектико-материалистический), общелогическая (анализ, синтез, дедукция) и эмпирическая (описание, наблюдение, сравнение).

Основная часть. Актуальные исследования применительно к фиксации, хранению и доказательственной электронной (цифровой) информации касаются самых современных проблем применения информационных технологий, в том числе с участием технологий искусственного интеллекта. Так, В. В. Глимейда обосновывает, что «цифровая технология представляет собой разработанные цифровые алгоритмы, выступающие в виде целостного программного продукта, результат применения которого в уголовном судопроизводстве может иметь процессуальное значение». А. В. Полякова, говорит, например, об «использовании “3D-моделей” объектов судебной экспертизы», под которой понимается «цифровой объект, создаваемый в трех измерениях с помощью специализированного программного обеспечения, который в процессе исследования воспроизводит объект-оригинал, обладая его существенными свойствами…» Д. В. Бахтеев предлагает интересную информационную систему, которая представляет собой «процесс криминалистического познания», позволяющий всю значимую криминалистическую информацию «трансформировать в совокупность доказательств по уголовному делу». И. Р. Бегишев исследует проблемы уголовно-правового регулирования робототехники: «…роботы являются крайне широкой категорией, под которую фактически подпадает любой материальный объект, способный к механическим манипуляциям в пространстве и обладающий достаточным уровнем развития программного обеспечения». Д. О. Буйнов анализирует способы совершения преступлений в сфере экономической деятельности с использованием цифровых технологий. А. И. Зазулин отмечает, что «эпоха цифры обернулась экспоненциальным ростом количества вероятных источников доказательств». А. А. Бессонов говорит о применении технологий поиска информации из открытых источников и алгоритмов искусственного интеллекта для поиска цифровых следов преступлений и анализа «больших данных». О. А. Зайцев и П. С. Пастухов обосновывают новую цифровую стратегию расследования преступлений. Можно поддержать идею формирования Концепции Единого цифрового уголовного дела. В литературе также говорится об «интернет-доказательствах», их значении и отмечают «процессуальные особенности».

Зарубежный опыт. Применение цифровых технологий затрагивает такую интересную проблематику, как создание инфомационно-справочного портала

«Шерлок», который разработан в целях содействия распространению информации о реализации Конвенции ООН против транснациональной организованной преступности, трех протоколов к ней и сведений о международно-правовой базе борьбы с терроризмом. В УПК Республики Казахстан была введена ст. 42-1 «Формат уголовного судопроизводства»: IT-система электронного уголовного дела (Е-уголовное дело – Единый реестр досудебных расследований (ЕРДР).

Заключение. Таким образом, существует обоснованная аргументация исследователей о цифровизации доказательственной деятельности субъектов права и о формировании информационного поля о предметах, документах, электронной информации и иного изъятого имущества в межотраслевых связях уголовного процесса. В связи с этим с целью многофункционального применения цифровых (вещественных) доказательств в их единстве и дифференциации в системе межотраслевых связей уголовного процесса необходимо: а) сформировать практико-ориентированную программу «Цифровая модель преступления – corpus delikte»; б) обосновать перспективу онлайн-расследований транснациональных преступлений; в) создать цифровые тематические платформы с использованием технологий искусственного интеллекта по законодательным видам вещественных доказательств (Единый репозиторий); г) создать Мониторинговый репозиторий вещественных доказательств по их видам в соответствии с конкретным составом преступления по уголовному делу.

Список литературы

1. Архипова Е. А., Додонов В. Н. Международно-правовые проблемы сотрудничества при выявлении, расследовании и предупреждении преступлений, совершенных с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации // Московский журнал международного права. – 2020. – № 2. – DOI: https://doi.org/10.24833/0869-0049-2020-2-77-87

2. Балгынтаев А. О. Электронное уголовное судопроизводство в Республике Казахстан // Сайт законодательства Казахстана. – URL: https://online.zakon.kz/Document/?doc_id=34878697&pos=6;-106#pos=6;-106 (дата обращения: 24.04.2023).

3. Бахтеев Д. В. Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений: автореф. … дис. д-ра юрид. наук: Екатеринбург, 2022. – С. 14.

4. Бегишев И. Р. Уголовно-правовое регулирование робототехники: монография. – М.: Блок-Принт, 2022. – С.44–45.

5. Бессонов А. А. К вопросу о цифровизации уголовного судопроизводства в Российской Федерации // Уголовный процесс и криминалистика: правовые основы, теория, практика, дидактика (к 75-летию со дня рождения профессора Б. Я. Гаврилова): сборник научных статей по материалам Международной научно-практической конференции (Москва, 3 ноября 2023 г.): в 2 ч. / под ред. Б. Я. Гаврилова, Ю. Е. Салеевой, Ю. В. Шпагиной, – М.: Академия управления МВД России, 2023. – Ч. 1. – С. 26–27.

6. Буйнов Д. О. Теория и практика собирания и экспертного исследования цифровых следов по уголовным делам в сфере экономической деятельности: автореф. … канд. юрид. наук. – М., 2024. – С. 5–7.

7. Глимейда В. В. Применение технических средств и цифровых технологий при производстве следственных действий: автореф. … канд. юрид. наук. – Краснодар, 2024. – С. 3–4.

8. Зазулин А. И. Уголовный процесс Германии в контексте национальных и международных тенденций по цифровизации права: монография. – М.: Проспект, 2022. – С. 3–4.

9. Зазулин А. И. Интернет-доказательства и перспективы их использования в доказывании по уголовным делам // Высокотехнологичный уголовный процесс: монография / под ред. д-ра юрид. наук С. В. Зуева, д-ра. юрид. наук. Л. Н. Масленниковой. – М.: Юрлитинформ, 2023. – С. 51–60.

10. Зайцев О. А., Пастухов П. С. Формирование новой стратегии расследования преступлений в эпоху цифровой трансформации // Вестник Пермского университета. Юридические науки. – Пермь, 2019.

11. Попов И. В 11 регионах России задержана группировка из 30 хакеров // Российская газета. – 2020, 24 марта. – URL: https://rg.ru/2020/03/24/v-11-regionah-rossii-zaderzhana-gruppirovka-iz-30-hakerov.html (дата обращения: 21.04.2023).

12. Кассационное определение третьего кассационного суда общей юрисдикции. Дело № 7У-3258/2022 [77-1578/2022] от 2 июня 2022 г. (г. Санкт-Петербург). – URL: https://xn--90afdbaav0bd1afy6eub5d.xn--p1ai/69166360 (дата обращения: 03.05.2023).

13. Крупные атаки хакеров в 2001–2016 годах: хронология // Информационное агентство ТАСС. – URL: https://tass.ru/info/1408961/amp (дата обращения: 22.10.2022).

14. Муратов К. Д. Хранение цифровой информации при формировании системы вещественных доказательств по уголовному делу // Санкт-Петербургский международный криминалистический форум: [Электронный ресурс]: материалы Международной научно-практической конференции. Санк-Петербург, 11 июня 2024 г. / сост. А. Р. Акиев, Т. А. Бадзгарадзе. – Электр. Дан (11,0 Мб). – СПб.: Санкт-Петербргский ун-т МВД России, 2024. – С. 349–353.

15. Муратова Н. Г. Цифровые учеты мониторинговых сведений по уголовным делам: или о Концепции единого цифрового уголовного дела (продолжение дискуссии) // Вестник Волгоградской академии МВД России. – № 1(68). – 2024. – С. 88–96.

16. Краснушкина Н., Райский А., Крючкова Е., Скоробогатько Д. // Коммерсантъ. 2017, 13 ноября. – № 210. – URL: kommersant.ru/doc/3466185 (дата обращения: 07.02.2020).

17. Новицкий В. А., Новицкая Л. Ю. Понятие и виды цифровых доказательств // Ленинградский юридический журнал. – 2019. – С. 213–220. – URL: https://cyberleninka.ru/article/n/ponyatie-i-vidy-tsifrovyh-dokazatelstv (дата обращения: 03.06.2024).

18. Подшибякин А. С. Правовое и криминалистическое обеспечение. – М.: ЦентрЮрИнфоР, 2011. – 352 с.

19. Полякова А. В. Формирование и развитие 3D технологий в судебно-экспертной деятельности: методологические и организационные аспекты: автореф. … канд. юрид. наук. – Уфа, 2023.

20. Постановление Пленума Верховного Суда Российской Федерации от 07.07.2015 № 32 (ред. от 26.02.2019) «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем». – URL: https://www.consultant.ru/document/cons_doc_LAW_182365 (дата обращения: 05.05.2023).

21. Постановление Пленума Верховного Суда РФ от 09.07.2013 № 24 (ред. от 24.12.2019) «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» // КонсультантПлюс. – URL: https://www.consultant.ru/document/cons_doc_LAW_149092 (дата обращения: 05.05.2023).

22. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также и иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей включая сеть «Интернет» // СПС «ГАРАНТ». – URL: https://www.garant.ru/hotlaw/federal/1591816 (дата обращения: 22.12.2022).

23. Юйпэн С. История и перспективы создания «умных судов» в КНР: проблемы применения технологии искусственного интеллекта // История государства и права. – 2023. – № 5. – С. 44–47.

24. Федеральный закон от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей ГК РФ». – URL: http://www.kremlin.ru/acts/bank/45766/page/1 (дата обращения: 05.05.2023).

25. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (в ред. ФЗ от 14.07.2022 № 331-ФЗ, с учетом ФЗ от 14.07.2022 № 292-ФЗ). – URL: http:// www.kremlin.ru/acts/bank/45766/page/1 (дата обращения: 05.05.2023).

26. Laptev V., Fedin V. Legal awareness in a Digital Society // Russian Law Journal. – 2020. – Vol. 8, № 1. – URL: https://www.russianlawjournal.org/jour/issue/view/28 (дата обращения: 01.09.2024).

27. Radvan M. Guest editor’s note on digitalization in law // BRICS Law Journal. – 2020. – Vol. VII, Iss. 2. –
URL: https://www.bricslawjournal.com/jour/article/view/330/168

28. Sharing Electronic Resources and Laws on Crime (SHERLOC). United Nations Office on Drugs and Crime (UNODC). – URL: https://sherloc.unodc.org/cld/ru/st/home.html (дата обращения: 14.06.2024).

Э. Г. Хомяков,
кандидат юридических наук, доцент,
Удмуртский государственный университет

АКТУАЛЬНЫЕ ВОПРОСЫ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация. В статье анализируются отдельные проблемы, связанные с расследованием киберпреступлений соответствующими подразделениями МВД России, среди которых называются недостаточная компетентность личного состава данных подразделений, их ограниченная техническая обеспеченность, а также слабое внедрение в практику их работы современных информационных и цифровых технологий. Обозначаются пути решения указанных проблем, оцениваются перспективы борьбы с киберпреступностью. В частности, говорится о необходимости совершенствования УПК РФ и более активном внедрении в практику работы правоохранительных органов России современных информационных и цифровых технологий.

Ключевые слова: киберпреступления, расследование, МВД России, следователь, специалист, цифровые следы, цифровые технологии, информация

TOPICAL ISSUES IN THE INVESTIGATION OF CYBERCRIMES

Abstract. The article analyzes individual problems related to the investigation of cybercrimes by the relevant units of the Ministry of Internal Affairs of Russia, including the insufficient competence of the personnel of these units, their limited technical support, as well as the weak implementation of modern information and digital technologies in their work. The ways to solve these problems are outlined, and the prospects for combating cybercrime are assessed. In particular, it discusses the need to improve the Criminal Procedure Code of the Russian Federation and more actively implement modern information and digital technologies in the work of law enforcement agencies of Russia.

Keywords: cybercrime, investigation, Russian Ministry of Internal Affairs, investigator, specialist, digital traces, digital technologies, information

Введение. Текущая криминогенная обстановка в России характеризуется прежде всего ростом количества киберпреступлений или согласно официальной статистике – преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Так, если в 2020 году (когда в отчетности МВД России появился указанный вид преступлений) было зарегистрировано 510 396 (24,97 % от общего количества зарегистрированных в России преступлений), то в 2021 году – 517 722 (25,83 %), в 2022 году – 522 065 (26,54 %), в 2023 году – 676 951 (34,77 %); раскрываемость данных преступлений по приведенным годам составила, соответственно: 20, 20, 23,4, 27,8 % [1]. По официальным данным, свыше 98 % подобных преступлений выявляются органами внутренних дел.

Основная часть. Осознавая значительную опасность киберпреступности, в 2022 году Президент России В. В. Путин издал Указ о создании в структуре МВД России Управления по организации борьбы с противоправным использованием

информационно-коммуникационных технологий [2]. Задачи данного управления, его функции и полномочия закреплены соответствующим приказом МВД России [3]; в частности, среди обозначенных задач стоит выделить: организацию предупреждения, выявления, пресечения и раскрытия преступлений, совершаемых с использованием (в сфере) информационно-коммуникационных технологий, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших; организацию пресечения распространения в информационно-телекоммуникационной сети Интернет информации, создающей угрозу причинения вреда жизни, здоровью и имуществу граждан, по вопросам деятельности Управления; организационно-методическое обеспечение деятельности подразделений центрального аппарата МВД России, территориальных органов МВД России, их структурных подразделений и оказание им практической помощи по вопросам деятельности Управления.

В настоящее время, возможно, еще рано говорить об эффективности работы данного подразделения и его достаточности в масштабах России.

Несомненно, что в ближайшие годы основная нагрузка в раскрытии и расследовании киберпреступлений будет лежать на следственных, оперативных и экспертно-криминалистических подразделениях территориальных органов МВД России. И в качестве основных проблем указанных подразделений следует рассматривать недостаточную компетентность личного состава указанных подразделений, их ограниченную техническую обеспеченность, а также слабое внедрение в практику их работы современных информационных и цифровых технологий.

Под компетентностью в данном случае следует понимать наличие у сотрудников как субъектов, задействованных в процессе выявления, раскрытия и расследования киберпреступлений знаний, умений и навыков в работе с цифровой информацией. Это связано с тем, что любое киберпреступление характеризуется гибридным следообразованием, когда преступник (или преступники) оставляет как физические, так и цифровые следы. Соответственно, сотрудники следственных и оперативных подразделений должны уметь в процессе расследования находить и фиксировать источники данных следов, например, различные электронные носители информации, а сотрудники экспертно-криминалистических подразделений – цифровые следы из представленных источников извлекать (фиксировать) и подвергать анализу в процессе соответствующего экспертного исследования.

В настоящее время в ч. 2 ст. 164.1 Уголовно-процессуального кодекса (далее – УПК) РФ закреплено требование о том, что «электронные носители информации изымаются в ходе производства следственных действий с участием специалиста». Также специалист привлекается «…к участию в процессуальных действиях… для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела» согласно ч. 1 ст. 58 УПК РФ. Подобным специалистом в области цифровых следов выступает, как правило, эксперт, имеющий право самостоятельного производства судебной компьютерной экспертизы. Следует отметить, что такие эксперты немногочисленны и, помимо участия в следственных действиях в качестве специалистов, их основной задачей является производство компьютерных экспертиз. При сохраняющейся тенденции роста киберпреступлений экспертно-

криминалистические подразделения МВД России задачу обеспечения специалистами необходимого «цифрового» профиля просто не вытянут.

В подобной ситуации при ежегодном росте числа киберпреступлений возникает необходимость в соответствующей подготовке следователей, оперативных сотрудников, возможно, сотрудников и иных подразделений, а также внесении изменений в УПК РФ, на что требуются время, необходимые ресурсы и законодательная инициатива от соответствующих субъектов. Возможно, требуется новая реформа МВД России либо отдельных его подразделений, в ходе которой сотрудники, продемонстрировавшие необходимую компетентность в борьбе с «цифровой» преступностью, получат соответствующие преференции.

В настоящее время практически все образовательные учреждения МВД и СК России, а также гражданские вузы, готовящие специалистов для правоохранительных органов, разработали и внесли в соответствующие образовательные программы либо новые дисциплины, либо отдельные темы, связанные с цифровизацией соответствующих направлений подготовки, например, с изучением современных цифровых технологий и их применением в юриспруденции. Однако не всегда подобные инициативы находят положительный отклик со стороны сотрудников правоохранительных органов.

Например, в рамках исследования Н. Б. Нечаевой [4] было проведено анкетирование следователей, которые отметили нежелание осваивать цифровые технологии и использовать их в следственной практике, так как это занимает много времени и замедляет основную работу.

В рамках другого исследования предлагается введение института IT-следователей, для эффективного функционирования которого необходима их соответствующая подготовка, которая «должна осуществляться по специальным образовательным программам, сочетающим как теоретические курсы, подготовленные ведущими учеными в сфере цифровизации уголовного процесса, так и практические занятия с экспертами-программистами, объясняющими, как работают и как могут применяться те или иные цифровые технологии» [5. С. 51].

С учетом цифровой трансформации уголовного судопроизводства, а также перспективами появления Цифрового (или Информационного) кодекса, призванного регулировать отношения в сфере связи и информационно-коммуникационных технологий [6–8], следует прогнозировать определенные изменения УПК РФ, вплоть до его новой редакции.

На отдельных интернет-площадках уже идут дискуссии о необходимости разработки цифрового УПК РФ; название «цифровой УПК» в данном случае условное и характеризует данный нормативно-правовой акт по способности регулировать уголовно-процессуальные отношения в цифровой среде [9].

В любом случае в УПК РФ необходимо закрепить все процедурные этапы «цифрового» расследования, а также все возможные процессуальные действия, связанные с цифровой информацией и ее носителями, четко определить все полномочия, которыми наделяются субъекты подобного расследования, а также их обязанности и ответственность.

Помимо нормативно-правового регулирования вопросов расследования киберпреступлений, необходимо более активное внедрение в практику работы правоохранительных органов России современных информационных и цифровых технологий.

В этой связи можно отметить, что в 2020 году Правительство Российской Федерации приняло решение о разработке программ цифровой трансформации в федеральных органах исполнительной власти [10].

В качестве примера подобных программ цифровой трансформации в области правоохранительной деятельности можно назвать Ведомственные программы цифровой трансформации МВД России [11–13].

К сожалению, в данных программах фактически отсутствуют мероприятия, направленные на техническое переоснащение подразделений, непосредственно задействованных в расследовании киберпреступлений. Вместе с тем такое переоснащение аппаратными и программными средствами отечественного производства жизненно необходимо.

Что касается низкой раскрываемости в России киберпреступлений, то для ее повышения необходима централизованная подготовка учебно-методических материалов, например, обучающих или предписывающих конкретные алгоритмы действий в различных ситуациях расследования киберпреступлений. При подготовке подобных материалов должен анализироваться и использоваться как практический опыт российских правоохранителей, так и зарубежный опыт, на что, в частности, нас нацеливает криминалистика как наука [14. С. 66].

Заключение. Необходимы новые методики расследования различных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, должны быть разработаны цифровые модели данных видов преступлений. Также, помимо методик расследования, необходимы методики выявления подобных преступлений, в том числе в режиме реального времени. А с учетом того, что преступники достаточно часто меняют способы совершения подобных преступлений, то соответствующие методики должны регулярно обновляться и при необходимости быть закрытыми. В разработке подобных методик видится одна из задач, возложенных на Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России. К решению данной задачи должно быть подключено и научное криминалистическое сообщество России.

Список литературы

1. Официальный сайт МВД Российской Федерации. – URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 07.09.2024).

2. Указ Президента Российской Федерации от 30.09.2022 № 688 «О внесении изменений в некоторые акты Президента Российской Федерации» // СПС «Консультант Плюс» [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_427884 (дата обращения: 07.09.2024).

3. Приказ Министерства внутренних дел России от 29.12.2022 № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации» // СПС «ГАРАНТ» [Электронный ресурс]. – URL: https://base.garant.ru/406374891 (дата обращения: 07.09.2024).

4. Нечаева Н. Б. Инновационная организационно–временная конструкция функционирования субъектов расследования // Пробелы в российском законодательстве. – 2016. – № 4. – С. 212–216.

5. Зуев С. В., Зазулин А. И. IT-следователь в цифровой среде уголовного судопроизводства // Правопорядок: история, теория, практика. – 2024. – № 2(41). – С. 48–53.

6. Распоряжение Правительства РФ от 24.11.2023 № 3339-р «Об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года» // СПС «Консультант Плюс» [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_463486 (дата обращения: 07.09.2024).

7. Фролова М. Единый документ: какие нормы будет описывать Цифровой кодекс РФ // Известия [Электронный ресурс]. – URL: https://iz.ru/1704035/mariia-frolova/edinyi-dokument-kakie-normy-budet-opisyvat-tcifrovoi-kodeks-rf (дата обращения: 07.09.2024).

8. Кузьменко А. Сенатор Рукавишникова призвала переименовать Цифровой кодекс [Электронный ресурс]. – URL: https://www.pnp.ru/social/senator-rukavishnikova-prizvala-pereimenovat-cifrovoy-kodeks.html (дата обращения: 07.09.2024).

9. Проект Цифрового УПК [Электронный ресурс]. – URL: https://t.me/c/2056342561/2728/2730 (дата обращения: 07.09.2024).

10. Постановление Правительства РФ от 10.10.2020 № 1646 «О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий в деятельности федеральных органов исполнительной власти и органов управления государственными внебюджетными фондами» (с изменениями и дополнениями) // СПС «ГАРАНТ» [Электронный ресурс]. – URL: https://base.garant.ru/74749576/#block_1000 (дата обращения: 07.09.2024).

11. Об утверждении Ведомственной программы цифровой трансформации МВД России на 2021–2023 годы: распоряжение МВД России от 29.12.2020 № 1/15065 (ред. от 08.09.2021) // СПС «ГАРАНТ» [Электронный ресурс]. – URL: https://base.garant.ru/402620866/#block_1000 (дата обращения: 07.09.2024).

12. Об утверждении Ведомственной программы цифровой трансформации МВД России на 2022–2024 годы: распоряжение МВД России от 11.01.2022 № 1/37 // СПС «ГАРАНТ» [Электронный ресурс]. – URL: https://base.garant.ru/404486678 (дата обращения: 07.09.2024).

13. Об утверждении Ведомственной программы цифровой трансформации МВД России на 2023–2025 годы: распоряжение МВД России от 25.01.2023 № 1/649 // СПС «ГАРАНТ» [Электронный ресурс]. – URL: https://base.garant.ru/406258675 (дата обращения: 07.09.2024).

14. Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р. Криминалистика: учебник. – 4-е изд., перераб. и доп. – М.: Норма: ИНФРА-М, 2023. – 928 с.

А. Д. Цветкова,
младший научный сотрудник,
Уральский государственный юридический университет имени В. Ф. Яковлева,
Центр содействия развитию криминалистики «КримЛиб»

ПОВЕДЕНЧЕСКАЯ БИОМЕТРИЯ В КРИМИНАЛИСТИКЕ

Аннотация. Современные цифровые технологии способствуют расширению сфер исследования и видов исследуемых биометрических характеристик, однако поведенческая биометрия недостаточно вовлекается в криминалистическую деятельность. Это связано с тем, что динамические характеристики менее стабильны и требуют больших вычислительных мощностей, времени для накопления и использования. Вместе с тем они позволяют решать уникальные криминалистические задачи и сложнее фальсифицируются, что делает их изучение весьма значимым и перспективным направлением криминалистики. Целью настоящей работы было подробно рассмотреть существующие ограничения и перспективы внедрения технологий обработки поведенческих биометрических характеристик в деятельность по раскрытию и расследованию преступлений.

Ключевые слова: биометрические технологии, биометрия, статические биометрические характеристики, физиологические биометрические характеристики, динамические биометрические характеристики, поведенческие биометрические характеристики, криминалистическая идентификация

Исследование выполнено за счет гранта Российского научного фонда № 23-78-10011, https://rscf.ru/project/23-78-10011

BEHAVIORAL BIOMETRICS IN FORENSIC SCIENCE

Abstract. Modern digital technologies contribute to the expansion of research areas and types of biometric characteristics under investigation, but behavioral biometrics is not sufficiently involved in forensic activities. This is because dynamic characteristics are less stable and require more computing power, time to accumulate and utilize. At the same time, they allow solving unique forensic problems and are more difficult to falsify, which makes their study a very significant and promising area of forensic science. The purpose of this paper was to examine in detail the existing limitations and prospects for the introduction of technologies for processing behavioral biometrics in crime detection and investigation.

Keywords: biometric technologies, biometrics, static biometric characteristics, physiological biometric characteristics, dynamic biometric characteristics, behavioral biometric characteristics, forensic identification

The research was funded by the Russian Science Foundation grant No. 23-78-10011, https://rscf.ru/project/23-78-10011

Введение. Развитие цифровых технологий в последние годы привело к стремительному расширению рынка биометрических технологий [6. С. 152], что проявилось и в правоохранительной сфере: так, в частности методики установления личности правонарушителя посредством автоматизированного распознавания

его лица по цифровому изображению активно обсуждаются учеными [7, 9] и применяются на практике.

Основная часть. При этом важно заметить, что все биометрические характеристики традиционно делятся на две группы: статические (физиологические) и динамические (поведенческие). В первую группу входят изображение лица, рисунки радужной оболочки глаза, ушной раковины, вен, папиллярных линий. К поведенческой биометрии (данный термин представляется более точным, если учитывать словарные определения эпитетов, и репрезентативнее представлен в исследованиях, поэтому в работе мы будем использовать в основном его) относятся: походка, голос, модель выполнения рукописной подписи, клавиатурный почерк [8. С. 209]. В то время как физиологические биометрические технологии широко внедряются в различные сферы практической деятельности, поведенческая биометрия используется, на наш взгляд, весьма ограниченно, хотя в конце прошлого века отдельным ее направлениям в науке отдавался явный приоритет [5. С. 64]. Описанная ситуация может быть связана с несколькими причинами:

1. Поведенческая биометрия проявляется лишь при определенных условиях, то есть не может быть получена и обработана в любой момент времени. Так, если, например, лицо с характеризующими конкретную личность чертами может наблюдаться постоянно, то походка – только если человек начнет передвигаться в пространстве без вспомогательных технических (в частности, транспортных) средств.

2. Биометрические технологии поведенческой идентификации требуют более длительной настройки; для автоматизированной обработки данных необходимо собрать больший объем «базовой информации», которая составит динамический стереотип. Так, для успешной регулярной идентификации по отпечатку пальца достаточно единоразово пройти процедуру дактилоскопической регистрации или отсканировать палец встроенным в телефон датчиком. Напротив, если создается система аутентификации, учитывающая клавиатурный почерк пользователя, требуется предварительно напечатать определенные объемы текстового материала [3. С. 144], чтобы система сформировала и запомнила профиль пользователя.

3. Поведенческая биометрия характеризуется большей вариационностью признаков: тогда как радужная оболочка глаза остается неизменной на протяжении почти всей жизни человека, подпись человека, а следовательно, и характер движений при ее исполнении, в которых задействуется около 20 мышц руки [4. С. 96], меняется при выполнении каждого очередного реквизита так, что и другие люди, и системы искусственного интеллекта склонны распознавать некоторые оригинальные подписи в качестве подложных [1. С. 519].

Также существует проблема, которая не является специфичной для поведенческой биометрии, а характерна для отдельных видов соответствующих признаков в общем. Она связана с недостаточной научной разработанностью аспектов использования конкретных биометрических данных и отсутствием технических средств для их фиксации, хранения, обработки. Сегодня данная проблема свойственна для исследований узоров ушной раковины, рисунка вен, походки, клавиатурного почерка и некоторых других направлений. Однако она носит субъективный характер и преодолима при наличии научного и практического интереса

к этому, тогда как описанные выше трудности более фундаментальны и проистекают непосредственно из природы динамических характеристик личности.

Вместе с тем поведенческая биометрия обладает рядом неоспоримых преимуществ:

1. Ее сложнее фальсифицировать (как третьему лицу, так и действительному носителю). Так, например, весьма значительной сегодня является проблема дипфейков [2], а сам человек может использовать специальную сетку-маску, которая блокирует работу видеокамеры, что не позволяет распознать его внешность. В свою очередь, поведенческие характеристики не наблюдаются в статическом положении и являются более комплексными, в связи с чем подделать или сознательно исказить их так, чтобы исключить возможность правильной идентификации, весьма затруднительно.

2. Для обработки поведенческой биометрии часто не требуется какого-либо специализированного оборудования. Распознавание папиллярных узоров, радужной оболочки глаз невозможно осуществить без точных микросканеров, тогда как клавиатурный почерк может быть исследован по информации, сохраняющейся в операционной системе компьютерного устройства, на котором осуществлялась печать.

3. Именно поведенческая биометрия позволяет решать уникальные экспертно-криминалистические задачи. Так, все статические характеристики обеспечивают идентификацию лица, которое присутствовало в определенном месте (возможно, в определенное время). Однако поведенческая биометрия дает возможность ответить на большее число специфических вопросов, связанных с характером противоправного деяния: по клавиатурному почерку можно определить, кто является исполнителем напечатанного текста (иного специального метода решения этой задачи не существует); по подписи – установить ее исполнителя в рамках почерковедческой экспертизы; по походке – сформулировать ряд диагностических выводов о человеке и т. д.

Заключение. В связи с этим считаем, что более широкое внедрение поведенческой биометрии в практику раскрытия и расследования преступлений может существенно повысить эффективность правоохранительной деятельности, особенно в части решения специфических задач. Требуется совершенствовать методы работы с традиционными характеристиками и имплементировать из наук компьютерно-технического профиля способы исследования новых цифровых явлений. Современные достижения научно-технического прогресса способны вооружить правоохранительную сферу всеми ресурсами, необходимыми для минимизации недостатков динамической биометрии и максимизации ее положительных сторон.

Список литературы

1. Бахтеев Д. В. Особенности распознавания подлога подписи человеком как первичные критерии для разработки системы искусственного интеллекта // Сибирское юридическое обозрение. – 2020. – Т. 17, № 4. – С. 514–522. – DOI: 10.19073/2658-7602-2020-17-4-514-522

2. Бодров Н. Ф., Лебедева А. К. Понятие дипфейка (deepfake) в российском праве, его классификация и проблемы правового регулирования // Юридический

вестник Дагестанского государственного университета. – 2023. – Т. 48, № 4. – С. 173–181. – DOI: 10.21779/2224-0241-2023-48-4-173-181

3. Брюхомицкий Ю. А. Текстонезависимая идентификация личности по динамическим биометрическим параметрам на основе иммунной модели клональной селекции // Известия ЮФУ. Технические науки. – 2018. – № 5(199). – С. 142–151. – DOI: 10.23683/2311-3103-2018-5-142-151

4. Иванов А. И. Биометрическая идентификация личности по динамике подсознательных движений: монография. – Пенза: Изд-во Пенз. гос. ун-та, 2000. – 186 с.

5. Расторгуев С. П. Программные методы защиты информации в компьютерах и сетях. – М.: Изд-во Аг-ва «Яхтсмен», 1993. – 187 с.

6. Шангина И. Ю. Технологии биометрической идентификации: мировая и российская практики // Инновации. Наука. Образование. – 2020. – № 18. – С. 151–156.

7. Шатов Д. В., Барсуков С. С., Шипанов И. Н. Лицевая биометрия и нейронные сети в криминалистике: современные возможности и проблемы применения // Юристъ-Правоведъ. – 2023. – № 1(104). – С. 155–163.

8. Guo J., Mu H., Liu X., Ren H., Han Ch. Federated learning for biometric recognition: a survey // Artificial Intelligence Review. – 2024. – Vol. 57. – Pp. 208–247. – DOI: 10.1007/s10462-024-10847-7

9. Yang M., Li Sh., Zeng J. The Effects of AI-Driven Face Restoration on Forensic Face Recognition // Applied Sciences. – 2024. – Vol. 14. – Article ID 3783. – DOI: 10.3390/app14093783

К. В. Шевелева,
старший преподаватель,
Российский технологический университет – МИРЭА

О КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ ПРИ РАССЛЕДОВАНИИ НЕЗАКОННЫХ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ АЗАРТНЫХ ИГР, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»

Аннотация. Статья посвящена исследованию криминалистически значимой информации при совершении преступления, предусмотренного ст. 171.2 УК РФ, посредством сети Интернет. При написании статьи использованы следующие научные методы: метод анализа, системно-структурный, эмпирический. Содержание исследования: в работе, на основе судебной и следственной практики, отмечаются важные с точки зрения криминалистики отображения действий преступников в Сети, а также иные элементы криминалистической характеристики незаконной организации и проведения азартных игр. В результате: автор приходит к выводу, что в целях эффективного расследования исследуемого преступления необходима комплексная разработка методики расследования с учетом ее криминалистической характеристики. Констатируется необходимость использования подобных сведений в следственной деятельности.

Ключевые слова: криминалистическая характеристика, незаконные организация и проведение азартных игр, следовая картина, криминалистическая информация

ON FORENSICALLY SIGNIFICANT INFORMATION IN THE INVESTIGATION OF ILLEGAL ORGANIZATIONS AND CONDUCTING GAMBLING CARRIED OUT USING THE INTERNET

Abstract. The article is devoted to the study of forensically significant information when committing a crime under Article 171.2 of the Criminal Code of the Russian Federation via the Internet. The following scientific methods were used in writing the article: analysis method, system-structural, empirical. Contents of the study: in the work, based on judicial and investigative practice, important from the point of view of forensic displays of criminals' actions on the network are noted, as well as other elements of the forensic characteristics of the illegal organization and conduct of gambling. As a result: the author comes to the conclusion that in order to effectively investigate the crime under study, it is necessary to comprehensively develop an investigation methodology taking into account its forensic characteristics. The need to use such information in investigative activities is stated.

Keywords: forensic characteristics, illegal organization and conduct of gambling, trace picture, forensic information

Введение. С 2016 года в Российской Федерации установлен специальный правовой режим, регламентирующий законную игорную деятельность. В соответствии с ним игорная деятельность разрешена в так называемых разрешенных зонах на территориях субъектов Российской Федерации (Алтайский край, Краснодарский край, Приморский край, Калининградская область, Республика Крым). Однако, несмотря на довольно-таки обширную область, где допускается организовывать и проводить различного рода азартные игры, незаконная деятельность в данной сфере продолжает функционировать. При этом ввиду активного распространения информационно-телекоммуникационных технологий и реализующих их компьютерных систем, преступность в данной сфере существенно реформировалась в онлайн-среду. И если чуть более 10 лет назад, такого рода деяния совершались путем открытия «подпольных» помещений, где были организованы игорные зоны, то в последние годы наблюдается тенденция к замене реальной площадки на ее цифровые аналоги, в виде интернет-сайтов и онлайн-кабинетов, в рамках которых лица могут удовлетворить свои игорные потребности.

Основная часть. Следует уточнить, что в Российской Федерации установлена ответственность за организацию и проведение азартных игр вне разрешенных зон (за исключением букмекерских контор, пунктов приема ставок и тотализаторов). Отдельные положения отражены в Федеральном законе «Об информации, информационных технологиях и защите информации» (ст. 15.1), в Кодексе об административных правонарушениях РФ (ст. 14.1.1). Особо отметим, что с 2011 года введена в действие статья 171.2 Уголовного кодекса Российской Федерации (далее – УК РФ) «Незаконные организация и проведение азартных игр», устанавливающая в том числе прямой запрет на организацию и(или) проведение

азартных игр с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, или средств связи, в том числе подвижной связи.

Данные следственной практики показали существенный рост зарегистрированных преступлений в период установления разрешенных игорных зон. Так, по данным Главного информационно-аналитического центра Министерства внутренних дел России по ст. 171.2 УК РФ «Незаконные организация и проведение азартных игр» в 2012 г. было зарегистрировано 96 преступлений, в 2013 г. – 106, в 2014 г. – 145, в 2015 г. – 1421, в 2016 г. – 2113 преступлений, в 2017 г. – 1492, в 2018 г. – 1249, в 2019 г. – 975, в 2020 г. – 924, в 2021 г. – 1235, в 2022 г. – 1457, в 2023 г. – 1489. В 2012 г. направлено в суд 33 уголовных дела по обвинению в незаконных организации и проведении азартных игр, в 2013 г. – 47, в 2014 г. – 73, в 2015 г. – 543, в 2016 г. – 1079, в 2017 г. – 9 17, в 2018 г. – 710, в 2019 г. – 498, в 2020 г. – 449, в 2021, 2022 и 2023 гг. – 476, 522, 367 (соответственно) уголовных дел с обвинительным заключением.

В то же время статистика показала снижение числа расследованных уголовных дел, что, по нашему мнению, связано с устойчивой тенденцией перехода азартных игр d виртуальную форму. Как отметила О. Ю. Веденская, «в 2020 г. лидирующие позиции в сегменте игрового рынка заняли онлайн-приложения для мобильных устройств ($63,2 млрд – 47 %) и программное обеспечение для ПК ($38,3 млрд – 38 %)» [1. С. 265].

Снижение числа расследованных уголовных дел, на наш взгляд, обусловлено спецификой совершения данного преступления в виртуальном пространстве, которому присущи такие признаки, как трансграничность, анонимность, высокая степень сокрытия действий в Сети, большое количество потерпевших, быстрота транзакций, которые затруднительно отследить и другие.

Очевидно, что такого рода преступная деятельность посредством влияния и распространения информационных технологий только усложняется, в связи с чем особую актуальность приобретают вопросы обнаружения, изъятия и исследования криминалистически значимой информации и дальнейшее ее использование в доказательственных целях.

Характеристика важной с точки зрения криминалистики информации незаконных организаций и проведения азартных игр через сеть Интернет включает в себя анализ цифровых следов, техническую экспертизу оборудования, изучение методов сокрытия и маскировки деятельности, а также выявление участников и организаторов подпольных азартных операций в Сети. Важным аспектом является также исследование финансовых потоков и транзакций, связанных с незаконными азартными играми в онлайн-среде [6. С. 98].

Одним из ключевых криминалистически значимых признаков являются данные об обстановке совершения преступления. Ученые-криминалисты рассматривают обстановку совершения преступления как совокупность внешних и внутренних условий, влияющих на преступление, и включает в нее различные факторы, воздейцствующие на вероятностную модель преступления [3. С. 206].

При этом киберсреда, в области которой осуществляется преступная деятельность в сфере организации и проведения незаконных азартных игр, обладает рядом специфических черт, позволяющих осуществлять деяние в различных формах.

Например, «на веб-сайте “***” размещена информация, обличающая заключение сделки между лицами, действующими по предварительному сговору или в рамках организованной преступной группы и игроком» [4]. Как видим, такое взаимодействие весьма прозрачно, и такой способ не популярен ни среди организаторов, ни среди игроков. При этом количество криминалистически значимой информации достаточно для установления всех фактов произошедшего события.

Сложнее ситуация обстоит с преступлениями, где не предполагается непосредственный контакт между участниками преступного действия. Такие преступления связаны с высоким уровнем подготовки, совершения и скрытия преступления. «Так, лица С.О.В., К.О.В. и К.П.С., действуя сообща, организовывали и проводили азартные игры через Интернет. С.О.В. разработал план преступления, приобрел необходимое оборудование и программное обеспечение, снял помещение, создав там условия для проведения игр и обеспечивая конспирацию» [5]. К.О.В. и К.П.С., в соответствии с их ролями, привлекали игроков, осуществляли контроль за игрой, выдавали выигрыши и вели учет финансов. Криминалистически значимые сведения об организации и проведении азартных игр в Интернете, осуществляемых непосредственно, более разнообразны.

Наряду с этим, обстановка, в которой совершенны преступления, предусмотренные ст. 171.2 УК РФ традиционным способом (офлайн), отличается большей информативностью. Такого рода преступления совершаются, как правило, в крупных городах либо в городах, имеющих туристических статус, что позволяет привлекать азартных игроков массово. Для этих целей арендуются помещения, которые маскируются под развлекательные учреждения и игровое оборудование в которых тщательно законспирировано. Например, на входе в игровое заведение устанавливается завлекающая вывеска иного содержания, отличного от реальной (о благотворительной деятельности и прочее). Формируется база клиентов, где администратор, при входе нового игрока, передает его номер организатору для допуска. Здесь же отметим, что имеют место случаи использования коррумпированных связей в правоохранительных органах, предоставляющих информацию о предстоящих проверках игровых заведений.

Когда преступление осуществляется посредством информационно-телекоммуникационных технологий, обстановка не играет существенной роли с точки зрения криминалистической информации ввиду того, что такие действия преступник может осуществлять с любой точки мира, используя только компьютерную технику либо смартфон. Как показала практика, для этих целей злоумышленники выбирают места с общедоступным выходом в сеть Интернет. С целью сокрытия своих деяний преступниками не используются личные помещения и помещения друзей и родственников с доступом к Сети. В результате «связать» место, откуда осуществлены преступные действия, и личность преступника представляется затруднительным.

В то же время злоумышленниками приобретаются на этапе подготовки технические средства, такие как компьютерные устройства, планшеты, телефоны, игровое оборудование, специализированное программное обеспечение.

В рамках расследования преступлений в сфере организации и проведения азартных онлайн-игр, такая информация может быть использована для идентифи-

кации пользователя, местоположения его технического устройства, подготовленность к совершению преступления, самого механизма преступления и использована в ориентирующих и доказательственных целях.

Таким образом, исследованный комплекс информации о ситуации, в которой действует незаконная группировка, занимающаяся азартными играми, позволит объединить все аспекты модели вероятности, выявить их взаимосвязи и разработать эффективные меры по борьбе с данным видом преступлений.

Заключение. Криминалистически важная информация при организации и проведении азартных игр в сети Интернет возникает с момента подготовки преступника к совершению данного преступления. Кроме того, нами подчеркивается важность экспертных исследований для успешного расследования подобных преступлений. Судебная экспертиза, включающая компьютерно-техническую, почерковедческую и бухгалтерскую экспертизу, играет ключевую роль в установлении фактов и доказательств, необходимых для привлечения к ответственности лиц, занимающихся незаконной игорной деятельностью в онлайн-среде. Заключения экспертов являются неотъемлемой частью следственных материалов и обеспечивают основу для дальнейших правовых мероприятий по пресечению таких преступлений.

Список литературы

1. Введенская О. Ю. Типичная обстановка незаконной организации и проведения азартных игр с использованием глобальной сети Интернет / О. Ю. Введенская // Современная научная мысль. – 2019. – № 2. – С. 264–268.

2. Долгинов С. Д. Следы электронных устройств в криминалистике // Шестой Пермский конгресс ученых-юристов: Российская национальная правовая система: современное состояние, тенденции и перспективы развития: материалы Междунар. науч.-практ. конф. – Пермь, 2015. – С. 266–267.

3. Потапов А. Н. История становления уголовной ответственности за совершение преступлений, связанных с незаконной организацией и проведением азартных игр // Юридическая наука и практика: Альманах научных трудов Самарского юридического института ФСИН России, Самара, 30 сентября 2019 года. – Т. 7. Ч. 2. – Самара: Самарский юридический институт ФСИН России, 2019. – С. 205–207.

4. Приговор Таганрогского городского суда Ростовской области № 1-533/2018 от 26 июля 2018. – URL: https://www.sudact.ru (дата обращения: 16.02.2024).

5. Решение Октябрьского районного суда г. Белгорода No 2А-2127/2018 2А-2127/2018 ~ М-1759/2018 М-1759/2018 от 4 мая 2018 г. – URL: https://www.sudact.ru (дата обращения 22.01.2024).

6. Устинова Т. Д. Проблемы квалификации незаконных организации и проведения азартных игр // Актуальные проблемы российского права. – 2019. – № 11(108). – С. 96–103.

К. С. Шубина,
кандидат юридических наук,
Московский университет Министерства внутренних дел
Российской Федерации имени В. Я. Кикотя

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ OSINT ДЛЯ СБОРА КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ

Аннотация. В статье проанализированы проблемы и перспективы использования технологии OSINT в целях сбора криминалистически значимой информации; изучены сферы деятельности, в которых применяется разведка по открытым источникам, в том числе правоохранительная деятельность; рассмотрены общедоступные источники, из которых может быть получена криминалистически значимая информация; систематизированы интернет-сервисы и приложения, предназначенные для сбора данных из открытых источников; на практических примерах продемонстрирована эффективность использования инструментов OSINT в раскрытии и расследовании преступлений; предложены процессуальные способы оформления результатов применения OSINT.

Ключевые слова: раскрытие и расследование преступлений, криминалистически значимая информация, следственные действия, протокол осмотра предметов (документов), цифровые технологии, OSINT, информационно-телекоммуникационная сеть Интернет, открытые источники, интернет-сайты, социальные сети

USING OSINT TECHNOLOGY TO COLLECT FORENSICALLY SIGNIFICANT INFORMATION

Abstract. The article analyzes the problems and prospects of using OSINT technology to collect forensically significant information; studies the areas of activity in which open source intelligence is used, including law enforcement; examines publicly available sources from which forensically significant information can be obtained; systematizes Internet services and applications designed to collect data from open sources; demonstrates the effectiveness of using OSINT services in solving and investigating crimes using practical examples; proposes procedural methods for formalizing the results of using OSINT.

Keywords: crime detection and investigation, forensically significant information, investigative actions, protocol of inspection of objects (documents), digital technologies, OSINT, information and telecommunications network Internet, open sources, Internet sites, social networks.

Введение. На сегодняшний день на территории Российской Федерации проживает более 144 млн человек, из них 130 млн являются активными пользователями информационно-телекоммуникационной сети Интернет. Около 75 % населения страны имеет один или несколько аккаунтов в социальных сетях, наиболее распространенными из которых являются WhatsApp (принадлежит компании Meta, признанной в России экстремистской организацией), Telegram и «ВКон-

такте» [12]. То есть примерно 106 млн человек ежедневно размещают о себе информацию, относящуюся к их персональным данным (Ф. И. О., дату и место рождения, семейное положение; образование; профессию и т. д.).

В 2023 г. объем скомпрометированных персональных данных в России достиг 1,12 млрд записей, что почти на 60 % больше, чем в 2022 г. [6] На практических примерах рассмотрим случаи нарушения права на конфиденциальность персональных данных. В январе 2023 г. сервис для изучения иностранных языков Duolingo стал жертвой кибератаки, в результате которой были опубликованы личные данные 2,6 млн. пользователей (имена, адреса электронной почты). Также в 2023 г. произошла утечка данных более чем 100 млн пользователей социальной сети «ВКонтакте» (имена, фамилии, адреса электронной почты, номера телефонов и даже IP-адреса). Таким образом, в результате широкого распространения социальных сетей и регулярных утечек данных в информационно-телекоммуникационной сети Интернет накопилось значительное количество информации о людях, включающей в себя не только общедоступные (Ф. И. О., возраст и место жительства), но и более конфиденциальные сведения (предпочтения, интересы, медицинские записи и даже финансовые данные).

Основная часть. В последние годы посредством информационных технологий совершаются и «традиционные» преступления (кража, совершенная с банковского счета, а равно в отношении электронных денежных средств; мошенничество; мошенничество в сфере компьютерной информации; торговля наркотическими средствами и психотропными веществами), при этом зачастую злоумышленники используют данные о личности жертв из открытых источников (мошенники в ходе телефонного разговора называют собеседника по имени и отчеству, упоминают имеющиеся банковские продукты и т. д.). Согласно статистическим данным, представленным на официальном сайте МВД России, в январе – феврале 2024 г. зарегистрировано 115,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 23,5 % больше, чем за аналогичный период прошлого года. С использованием сети Интернет совершается 80,2 % преступлений, около половины (45,8 %) с применением средств мобильной связи [5].

Вместе с тем сведения о личности преступника и самом преступлении, как правило, можно найти в сети Интернет. Однако для поиска информации из открытых источников требуется владение соответствующими знаниями и навыками о том, где и что искать. Данный процесс называют OSINT.

OSINT (Open Source Intelligence) берет свое начало во времена Второй мировой войны, когда союзниками создавались специальные группы для сбора данных об оккупированных территориях. С 1950-х годов разведывательные службы США начали активно применять технологии и методы для сбора данных из открытых источников, что ускорило развитие этой области. М. Бьюзен, эксперт по безопасности и автор книги Open Source Intelligence Techniques, и Д. Хагманн, основатель Американского института по сбору информации из открытых источников, внесли значительный вклад в развитие OSINT.

В справочнике по разведке из открытых источников, разработанном НАТО в ноябре 2001 г., рассматривается четыре категории источников информации для OSINT: Open Source Data (необработанные данные, доступные из публичных ис-

точников), Open Source Information (данные, которые были объединены, обработаны и отредактированы), Open Source Intelligence (информация, распространяемая для узкой аудитории), Validated OSINT (информация с высокой степенью доверия) [3. С. 63].

В научной литературе под OSINT понимается «разведывательная дисциплина, включающая в себя поиск, выбор, сбор разведывательной информации из общедоступных источников, а также ее анализ» [11. С. 132].

OSINT применяется в различных сферах деятельности для достижения разнообразных целей:

1. Международные организации применяют OSINT в целях мониторинга международных отношений, анализа глобальных тенденций и разработки соответствующих стратегий.

2. Бизнес-корпорации используют OSINT для наблюдения за деятельностью конкурентов, исследования новых рынков, планирования маркетинговой деятельности, а также выявления потенциальных угроз и уязвимостей в системах информационной безопасности.

3. Журналисты посредством OSINT проверяют достоверность обнаруженных фактов, разыскивают первоисточник информации и свидетелей.

4. Злоумышленники используют методы OSINT для сбора данных о будущих жертвах, что позволяет им проводить более эффективные целевые атаки (они могут использовать эту информацию для подготовки фишинговых рассылок или для выявления уязвимостей в системах безопасности компании).

5. Сотрудники правоохранительных органов применяют OSINT в целях обеспечения охраны общественного порядка и общественной безопасности, раскрытия и расследования преступлений, поиска без вести пропавших и лиц, совершивших преступление.

Сущность термина OSINT заключается в строгом соблюдении норм законодательства, а также получении информации из открытых источников, то есть без предварительного разрешения (санкции) суда на доступ к данным со стороны сотрудников правоохранительных органов. К общедоступным источникам, из которых может быть получена криминалистически значимая информация, относятся:

– СМИ: новости, заметки, статьи и другие публикации в прессе, телевидении, радио и онлайн-изданиях;

– научные исследования: публикации в журналах и электронных библиотеках, диссертации, материалы конференций;

– книги: справочники, энциклопедии, учебники и другие печатные издания;

– сайты, социальные сети, форумы и блоги;

– государственные реестры и открытые базы данных: например, информация о долгах граждан на сайтах судебных приставов;

– поисковые системы: использование стандартных браузеров и специализированных инструментов для поиска информации;

– анализ метаданных файлов: уточнение даты создания текстовых документов, имен пользователей и геолокации;

– данные о доменах: информация о технологиях, на которых построен сайт;

– непубличная документация, оказавшаяся в открытом доступе: документы, предназначенные для внутреннего пользования организаций, но случайно попавшие в сеть Интернет.

Кроме того, к общедоступным источникам информации, по мнению А. А. Бессонова, также относятся: сведения, полученные из утечек баз данных некоторых российских сервисов, таких как «Яндекс.Еда», Delivery Club, «Гемотест», СДЭК, «Почта России» и др.; во-вторых, информация, добытая из открытых источников, социальных сетей и «Даркнета», посредством программного комплекса «Охотник» [7]. Рассматриваемый комплекс позволяет: устанавливать личности людей и связи между ними, включая скрытые и удаленные данные, информацию из социальных сетей; разыскивать объекты по географическим координатам; отслеживать деятельность закрытых преступных сообществ, форумов и торговых площадок в «Даркнете»; анализировать операции с криптовалютами и контент социальных сетей и веб-страниц [1. С. 43–44].

Однако 23 января 2024 г. Государственной Думой Российской Федерации в первом чтении был принят проект Федерального закона № 502104-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях (в части усиления ответственности за нарушение порядка обработки персональных данных)» и представлены поправки к нему. Законопроект регламентирует введение административной ответственности в виде штрафов для компаний, допустивших утечку личных данных граждан, а также за использование, передачу, сбор, хранение персональных данных, полученных незаконным путем, и создание информационных ресурсов, распространяющих такие сведения [2]. Таким образом, дискуссионным является вопрос отнесения информации из утечек баз данных к общедоступным источникам.

Для сотрудников правоохранительных органов неоспоримое преимущество использования сервисов OSINT заключается в оперативном получении криминалистически значимой информации (сведений, имеющих отношение к раскрытию и расследованию преступления). По результатам анализа и проверки достоверности обнаруженных данных могут быть выдвинуты следственные версии, выбраны эффективные тактико-криминалистические приемы при производстве следственных действий, определен алгоритм действий на последующих этапах расследования уголовного дела.

Сервисы OSINT, как правило, специализируются на определенных областях поиска, что позволяет их классифицировать по типу искомой информации:

1. Сервисы, предназначенные для сбора информации по Ф. И. О.:

а) Namebook.club – уникальная система поиска людей (собирает информацию из различных источников, таких как социальные сети, блоги, форумы);

б) Rfpoisk.ru – сервис поиска людей, по базе данных (позволяет обнаружить телефон, домашний адрес, дату рождения, информацию о месте службы в армии, учебных заведениях и т. д.);

в) Botsman.org – система поиска людей (бот отбирает информацию из всех открытых источников – ВКонтакте, Facebook[2], Одноклассники, Twitter[3], Pinterest, Tumblr и т. д.) (рис. 1. Интерфейс сайта https://botsman.org);

[2] Facebook – социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

[3] Twitter (X) – социальная сеть, заблокированная на территории Российской Федерации за распространение незаконной информации.

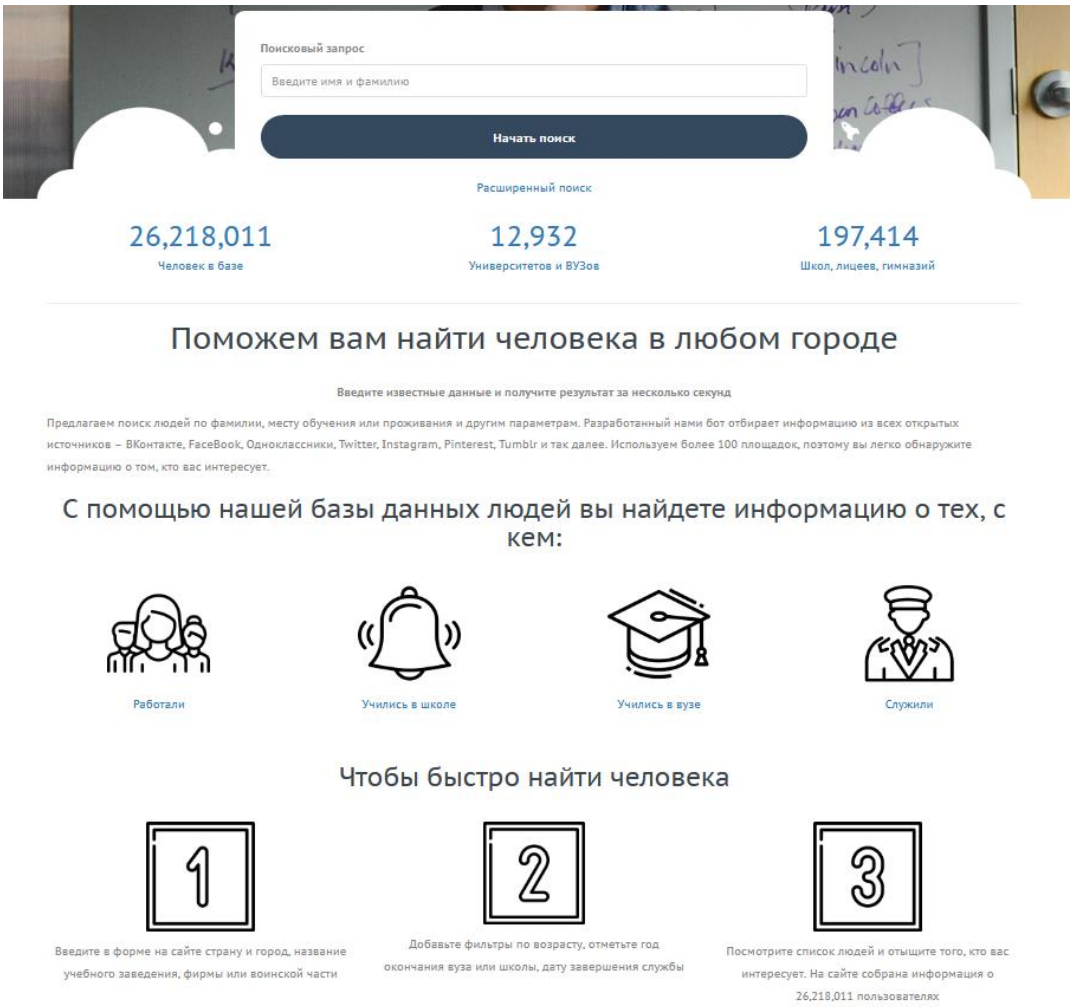

Рис. 1. Интерфейс сайта https://botsman.org

г) Yandex.people, Fio.stop-list.info – поиск информации о человеке по Ф. И. О. из социальных сетей, государственных реестров; справочников и т. д.

2. Сервисы для сбора информации по номеру телефона:

а) PhoneInfoga – продвинутая утилита, позволяющая получать данные о стране, операторе связи, типе линии и другую информацию, связанную с номером телефона;

б) Maltego и SpiderFoot – комплексные программные решения, способные интегрировать внешние сервисы и базы данных для создания графов расследований и обмена ими с другими пользователями;

в) Dork Search и Advangle – инструменты, предназначенные для автоматизации и предоставления подсказок при составлении расширенных операторов поиска, известных как Google Dorks;

г) Nomer.org – информационный сайт о телефонном справочнике СНГ;

д) Getcontact – приложение, позволяющее установить личность абонента по номеру телефона (рис. 2. Пример поиска по абонентскому номеру в приложении Getcontact).

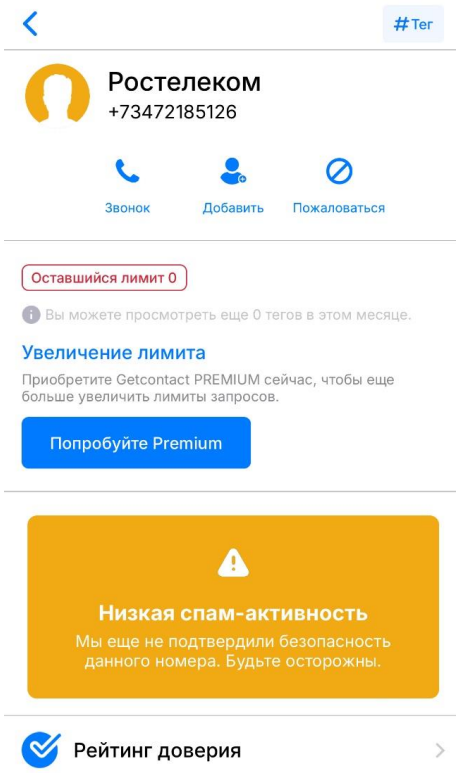

Рис. 2. Пример поиска по абонентскому номеру в приложении Getcontact

3. Сервисы для сбора информации об электронной почте и никнеймах:

а) Hunter.io – сервис, который находит адреса электронной почты, связанные с определенным доменом;

б) Emailsherlock – автоматический поиск по email-адресу;

в) Namechk.com – сайт, который находит аккаунты человека во всех социальных сетях и мессенджерах (рис. 3. Интерфейс сайта Namechk.com).

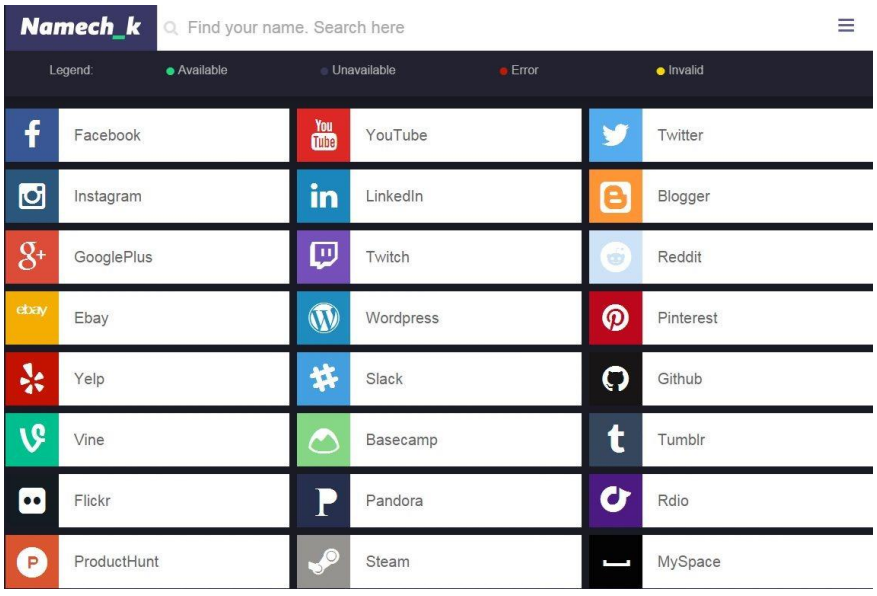

Рис. 3. Интерфейс сайта Namechk.com

4. Сервисы для сбора информации по фотографии:

а) InVID-WeVerify – расширение для браузеров Chrome и Firefox, которое позволяет получать контекстную информацию о видео на платформах вроде Facebook[4] и YouTube, выполнять обратный поиск изображений в поисковых системах, таких как Google, Baidu или «Яндекс», просматривать метаданные и ключевые кадры, а также узнавать, кто первым загрузил изображение или видео в сеть Интернет, для установления авторства;

б) Google Lens – приложение от Google, способное распознавать объекты на фотографиях из галереи или с камеры смартфона, предлагая информацию о товарах, которые можно купить, переводя текст с физических носителей, находя информацию о растениях и животных, создавая события в календаре на основе данных с листовок и билетов, сохраняя контакты с визиток и т. д.;

в) «Яндекс Картинки», «Google Картинки» – сервисы для поиска объекта по картинкам и фотографиям в сети Интернет, доступна генерация фото людей и изображений посредством нейросети;

г) PimEyes – сервис для поиска по картинкам и фотографиям, определения объектов на фото (рис. 4. Интерфейс сайта https://pimeyes.com/en);

д) SunCalc.org – онлайн-инструмент для определения положения солнца и теней в разные дни и времена суток в разных точках мира;

е) Metadata2go.com – онлайн-инструмент для доступа к скрытым метаданным изображений, видео и документов;

ж) Reveal Image Verification Assistant – онлайн-инструмент для анализа достоверности изображений в медиа, включающий алгоритмы обнаружения подделки, анализ метаданных, геолокации GPS и извлечение миниатюр EXIF.

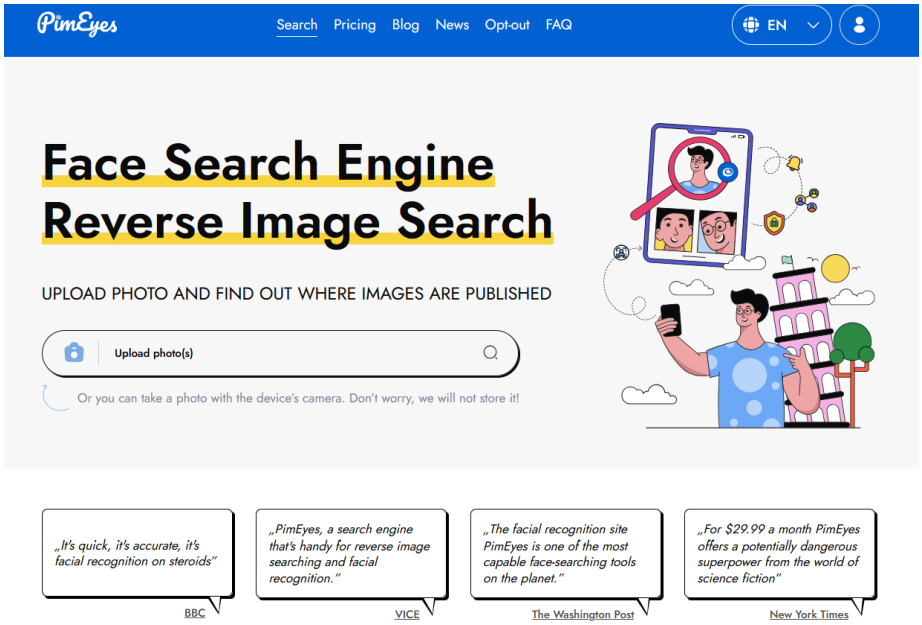

Рис. 4. Интерфейс сайта https://pimeyes.com/en

[4] Facebook – социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

5. Сервисы для сбора информации по устройствам:

а) Shodan – поисковик, который индексирует устройства, подключенные к сети Интернет, и предоставляет детальную информацию о них (с его помощью можно отслеживать незащищенные камеры видеонаблюдения, искать уязвимые серверы или устройства) (рис. 5. Интерфейс сайта https://www.shodan.io);

б) Censys – поисковик по интернет-инфраструктуре, который помогает анализировать SSL-сертификаты, искать уязвимые устройства в конкретной подсети;

в) GeoCreepy – инструмент для сбора геолокационных данных из твитов и фотографий. С его помощью можно отслеживать местоположение человека, анализировать паттерны перемещения.

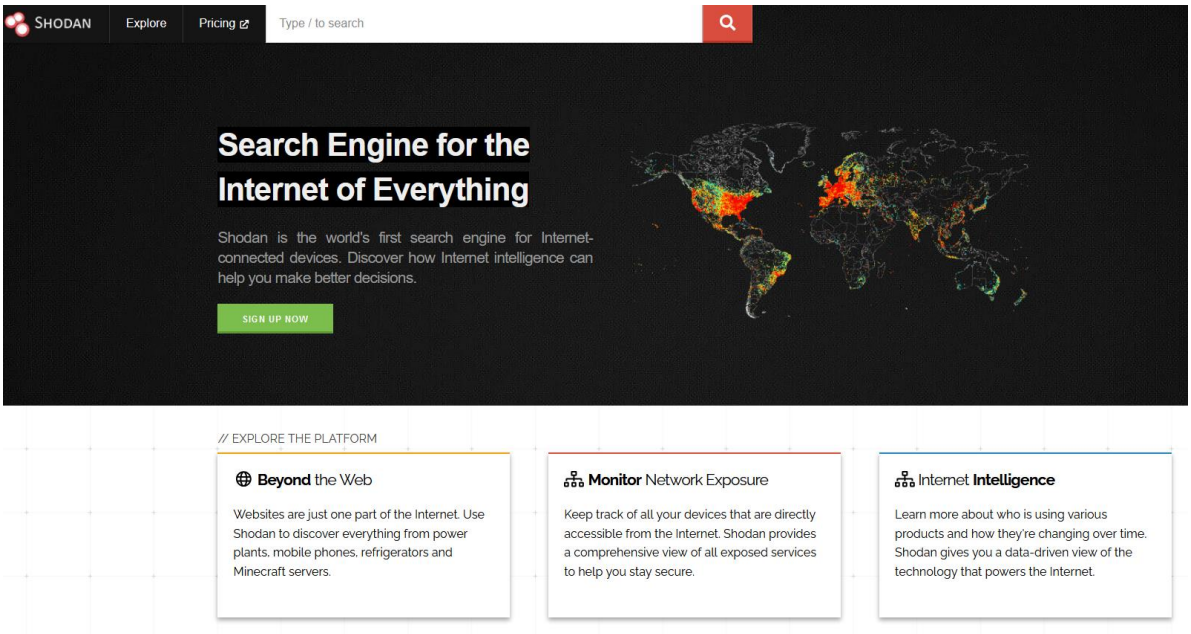

Рис. 5. Интерфейс сайта https://www.shodan.io

6. Сервисы для сбора информации о домене:

а) BigDomainData.com – предоставляет обширную базу данных о доменах, включая информацию о владельцах, регистраторах, дате регистрации и окончания действия домена;

б) WhoisHistory.ru – предлагает доступ к архивным данным о доменах, что полезно для анализа изменений (имеет русскоязычный интерфейс и поддержку, что облегчает работу для пользователей из России и стран СНГ);

в) Phonebook.cz – предоставляет множество функций бесплатно, включая поддержку API для интеграции с другими сервисами;

г) Whois.DomainTools.com – предлагает обширный функционал для анализа доменов, включая DNS, SSL и другие инструменты;

д) DRS.WhoisXmlApi.com – позволяет автоматизировать сбор данных и интегрировать их в другие системы через API (имеет обширную базу данных и поддержку большого количества доменных зон, но платные функции доступны только по подписке);

е) Archive.org, Cashedview.com – предоставляют доступ к архивным версиям страниц сайтов.

Известны успешные случаи установления местонахождения лиц, совершивших преступления, с помощью сервисов OSINT.

Так, в 2011 г. суд Нидерландов приговорил гражданина Ирана Ш. Гейбе к тринадцати годам лишения свободы за ограбление и покушение на убийство. Однако после вынесения приговора преступнику удалось скрыться, из-за чего он был объявлен в розыск. В 2015 г. Шахин создал аккаунт в Instagram[5], в котором размещал фотографии и обвинял голландский суд в некомпетентности. В 2019 г. некоммерческая ассоциация Bellingcat, специализирующаяся на OSINT-расследованиях, смогла установить местонахождение Ш. Гейбе. Сотрудниками ассоциации был проанализирован профиль мужчины в указанной социальной сети (опубликованные фото и видео). Изучались только те изображения, на которых разыскиваемый находился у предметов, с которыми можно было связать его местоположение (Гейбе рядом с автомобилем, в клубе, держит фирменный нож). Важно отметить, что Шахин намеренно использовал фейковые геотеги для ведения в заблуждение сотрудников полиции.

Путем сопоставления фото с панорамными снимками в «Яндекс.Картах» и Google Streetview удалось определить места, где бывал Шахин, а также лиц, с которыми он контактировал (в том числе у кого заказывал ножи или арендовал машину). Один из видеороликов был снят мужчиной у своего дома, эксперты установили расположение домовладения, а подписчики в Twitter[6] определили точный адрес.

Посредством сбора информации из открытых источников ассоциация Bellingcat обнаружила местонахождение осужденного Ш. Гейбе в г. Амирдашт (Иран), что подтвердил разыскиваемый в личной переписке. Однако задержать его не представляется возможным из-за отсутствия договора об экстрадиции между Нидерландами и Ираном.

Другим примером успешного использования OSINT в целях установления подозреваемого является дело о гибели Ю. Савенка, который был найден прохожими в бессознательном состоянии на автобусной остановке в Нижнем Новгороде в ноябре 2017 г. Очевидцы вызвали скорую помощь, после чего мужчина был доставлен в токсикологическое отделение больницы, где скончался. Согласно медицинскому заключению причиной смерти явилась открытая черепно-мозговая травма и отек головного мозга. Предварительное следствие по данному уголовному делу неоднократно приостанавливалось и вновь возобновлялось.

Спустя три года мать погибшего обратилась за помощью к адвокату Л. Козаку, который, ознакомившись с материалами дела, пришел к выводу, что имеющиеся показания свидетелей смоделированы под версию следствия о падении Ю. Савенка в состоянии алкогольного опьянения. Так, очевидцем «падения» был

[5] Instagram – социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

[6] Twitter (X) – социальная сеть, заблокированная на территории Российской Федерации за распространение незаконной информации.

бездомный, ранее обращавшийся в полицию с заявлением о восстановлении паспорта, и получивший его в день проверки показаний на месте. Другой свидетель (администратор хостела) в личных целях использовал банковскую карту Ю. Савенка. А допрошенный в качестве свидетеля судебно-медицинский эксперт, несмотря на имеющиеся посмертные снимки и описание травм в медицинской карте, подтвердил отсутствие на теле погибшего каких-либо повреждений.

Собственное расследование Л. Козак начал с дистанционного изучения места происшествия с помощью сервисов «Яндекс.Карты» и Google.Maps и установил, откуда могло быть видно место гибели мужчины (будка охранника автобусной станции, ларек по продаже шаурмы, автомастерская, здание хостела и др.). Таким образом, адвокат установил ключевых свидетелей по уголовному делу: охранника автобусной станции; продавца шаурмы; таксистов, находящихся рядом с местом происшествия; жителей хостела, занимавших номера на втором этаже здания, окна которых выходят на место обнаружения мужчины; сотрудников автомастерской.

Также адвокат нашел свидетеля (женщину, работавшую продавцом в магазине рядом с автобусной остановкой), устаревший абонентский номер которой был указан в протоколе допроса. Данный номер был привязан к уже неактуальному профилю в социальной сети «ВКонтакте», однако на страничке имелись фотографии, позволившие с помощью интернет-ресурса findclone.ru отыскать актуальные аккаунты пользователя по его фотографии. Связь со свидетелем была установлена, женщина отправила Л. Козаку видеозапись, на которой был запечатлен трезвый Ю. Савенок за несколько часов до гибели без травм на лице.

В своей работе защитник использовал банк судебных решений ГАС «Правосудие» и интернет-ресурс fssp.ru, которые позволили ему установить «фейковых» свидетелей, ранее неоднократно осужденных и дающих ложные показания. Посредством TelegramCheckerBot и SmartSearchBot были обнаружены важные свидетели (работник автомастерской и сотрудник хостела, видевшие драку между Ю. Савенком и двумя мужчинами, которая привела к гибели первого), автомобили подозреваемых, их актуальные телефонные номера и страницы в социальных сетях, образцы голоса, фотоснимки и др. Интернет-ресурс Mmnt.ru помог выявить связи свидетелей и подозреваемых с иными лицами, контрагентами, а также места их жительства.

Таким образом, всего за месяц Л. Козаку удалось получить описание внешности подозреваемых в убийстве Ю. Савенка, используемых ими транспортных средств и найти ключевых свидетелей их изобличивших (некоторые из них в целях обеспечения безопасности были засекречены) [4].

С процессуальной точки зрения результаты поиска информации из открытых источников, в частности сети Интернет, могут быть оформлены путем составления протокола осмотра предметов (документов) с фототаблицей (если при производстве следственного действия осуществлялось фотографирование; снятие скриншотов экрана устройства или электронного образа). При этом привлечение специалиста к осмотру веб-страниц, по нашему мнению, является обязательным, так как он, обладая соответствующими знаниями и навыками, используя программные модули, способен выявить цифровые данные, выраженные в виде скрытых ссылок, а также проанализировать исходный код страницы [9. С. 79].

Однако, по мнению К. Ю. Яковлевой, «в уголовном процессе технология OSINT – это технология, которая применима в ходе производства такого следственного действия, как обыск места нахождения электронной информации» [10. С. 135]. В качестве основного аргумента названа возможность осуществления поисковых действий только в рамках производства обыска. При этом используется авторская терминология («обыск места нахождения электронной информации»), противоречащая тексту УПК РФ. Не уточняется, нужно ли получать судебное разрешение для проведения обыска, связанного с поиском электронной информации.

Более обоснованной представляется точка зрения Ю. А. Телевицкой о том, что изъятие общедоступной информации из электронных сетей осуществляется путем производства осмотра электронных сетей, а обыск проводится при наличии препятствий в доступе к информации (например, требуется регистрация или введение пароля) [8. С. 240].

Заключение. Следует еще раз отметить, что полученные с помощью инструментов OSINT данные подлежат тщательной проверке, так как могут быть не просто устаревшими (например, за три года абонентский номер был заблокирован и передан другому пользователю), но и недостоверными с самого начала. Поэтому в статье сделан акцент на получении криминалистически значимой информации, которая в большей степени носит ориентирующий, а не доказательственный характер.

Таким образом, можно выделить следующие преимущества использования OSINT сотрудниками правоохранительных органов: сбор большого объема данных из открытых источников (социальных сетей, новостных сайтов, реестров); комплексный анализ собранной информации, позволяющий выявлять связи между свидетелями и подозреваемыми, а также исследовать их активность в сети Интернет; получение сведений из открытых источников обеспечивает оперативное реагирование на потенциальные угрозы и оптимизирует процесс раскрытия и расследования преступлений.

Список литературы

1. Бессонов А. А. Использование в раскрытии преступлений информации из открытых источников информации (OSINT) // Актуальные вопросы теории и практики оперативно-разыскной деятельности: сборник научных трудов Межведомственной научно-практической конференции, г. Москва, 16 сентября 2022 г. – М.: Моск. ун-т МВД РФ им. В. Я. Кикотя, 2022. – С. 40–45.

2. Законопроект № 502104-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях (в части усиления ответственности за нарушение порядка обработки персональных данных)» // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (СОЗД ГАС «Законотворчество») [Электронный ресурс]. – URL: https://sozd.duma.gov.ru/bill/502104-8 (дата обращения: 03.09.2024).

3. Иванов В. Ю. Использование OSINT в раскрытии и расследовании преступлений // Вестник Уральского юридического института МВД России. – 2023. – № 1(37). – С. 62–66.

4. Козак Л. Л. Расследование адвоката по открытым источникам: реанимация дела об убийстве // Уголовный процесс [Электронный ресурс]. – URL: https://e.ugpr.ru (дата обращения: 03.09.2024).

5. Краткая характеристика состояния преступности в Российской Федерации за январь – февраль 2024 года // Официальный сайт МВД России [Электронный ресурс]. – URL: https://мвд.рф/reports/item/48913905 (дата обращения: 03.09.2024).

6. Объем слитых персональных данных в РФ вырос на 60 процентов // ГК InfoWatch [Электронный ресурс]. – URL: https://www.infowatch.ru/company/presscenter/news/obyem- slitykh- personalnykh- dannykh- v- rf- vyros- na- shestdesyat- protsentov (дата обращения: 03.09.2024).

7. Свидетельство о государственной регистрации программ для ЭВМ от 7 декабря 2021 г. № 2021680077. Российский производитель ООО «Ти Хантер».

8. Телевицкая Ю. А. Выемка, осмотр и обыск в электронных сетях: понятие и разграничение // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2022. – № 4(60). – С. 238–242.

9. Шубина К. С. Актуальные проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Современные проблемы уголовного судопроизводства, криминалистики и судебной экспертизы: материалы XII Всероссийской научно-практической конференции, Саратов, 25 апреля 2024 года. – Саратов: Саратовский источник, 2024. – С. 77–81.

10. Яковлева К. Ю. Использование технологии OSINT в ходе обыска места нахождения электронной информации // Проблемы правовой и технической защиты информации. – 2023. – № 11. – С. 131–136.

11. Янгаева М. О., Павленко Н. О. OSINT. Получение криминалистически значимой информации из сети Интернет // Алтайский юридический вестник. – 2022. – № 2(38). – С. 131–135.

12. Digital 2024: Global Overview Report // Datareportal [Электронный ресурс] – URL: https://datareportal.com/reports/digital-2024-global-overview-report (дата обращения: 03.09.2024).