



**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. 5. – Казань: Изд-во «Познание» Казанского инновационного университета, 2024. EDN: KVBLYP. [http://dx.doi.org/10.21202/978-5-8399-0845-1\\_5](http://dx.doi.org/10.21202/978-5-8399-0845-1_5) – 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. 5. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2024. EDN: KVBLYP. <http://dx.doi.org/10.21202/978-5-8399-0845-15> – 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 5



# DIGITAL TECHNOLOGIES AND LAW

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

2023, September 22

Kazan

In 6 volumes

Volume 5

УДК 004:34(063)  
ББК 67с51я43  
Ц75

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

**Рецензенты:**

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

**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. Рускевич**, 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. Тимирязова;

**Ю. С. Харитонов**, 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. 5. – Казань: Изд-во «Познание» Казанского инновационного университета, 2024. EDN: KVBLYP. [http://dx.doi.org/10.21202/978-5-8399-0845-1\\_5](http://dx.doi.org/10.21202/978-5-8399-0845-1_5) – 1 CD-ROM. – Загл. с титул. экрана. – Текст: электронный.

ISBN 978-5-8399-0859-8

ISBN 978-5-8399-0845-1 (Том 5)

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

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 систематизированы по современным трендам развития отношений в сфере технологий искусственного интеллекта и робототехники; отдельно приведены труды ученых-правоведов по проблемам защиты прав человека, обеспечения цифровой безопасности и применения цифровых технологий в системе финансовых и налоговых правоотношений.

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

УДК 004:34(063)  
ББК 67с51я43

ISBN 978-5-8399-0859-8

ISBN 978-5-8399-0845-1 (Vol. 5)

© Авторы статей, 2024

© Казанский инновационный университет  
имени В. Г. Тимирязова, 2024

Научное издание

**ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО**

Сборник научных трудов II Международной научно-практической конференции  
20 сентября 2024 г.  
г. Казань

В шести томах  
Том 5

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. Заретдинова

Дата подписания к использованию: 13.12.2024. Объем издания 3,22 Мб. Тираж 11 экз. Заказ № 12/2024  
ISBN 978-5-8399-0845-1

Издательство Казанского инновационного университета им. В. Г. Тимирязова  
420111, г. Казань, ул. Московская, 42 Тел. (843) 231-92-90, E-mail: zaharova@ieml.ru 7



UDC 004:34(063)  
LBC 67c51я43

*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. 5. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2024. EDN: KVBLYP. [http://dx.doi.org/10.21202/978-5-8399-0845-1\\_5](http://dx.doi.org/10.21202/978-5-8399-0845-1_5) – 1 CD-ROM. – Title from the title screen. – Text: electronic.

ISBN 978-5-8399-0859-8

ISBN 978-5-8399-0845-1 (Vol. 5)

*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 in this volume are systematized according to modern trends in the development of relations in the field of artificial intelligence and robotics. A separate section is devoted to the works by legal scholars on the protection of human rights, ensuring digital security and the use of digital technologies in the system of financial and tax legal relations.

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 67c51я43

ISBN 978-5-8399-0859-8

ISBN 978-5-8399-0845-1 (Vol. 5)

© Authors of articles, 2024

© Kazan Innovative University

named after V. G. Timiryasov, 2024

*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 5

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 3,22 Mb. Number of copies: 11. Order No. 12/2024  
ISBN 978-5-8399-0845-1

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. Бегиев**, 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. Тимирязова;

**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. Тимирязова

### **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

## РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ В СФЕРЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И РОБОТОТЕХНИКИ

|                                                                                                                                                      |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Андреева М. А. ОТДЕЛЬНЫЕ ПРАВОВЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ<br>ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА.....                                              | 10 |
| Гладкая Е. Н. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И НОСИТЕЛЬ<br>ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КОНТЕКСТЕ РАЗВИТИЯ ПРАВА<br>ВЫСОКИХ ТЕХНОЛОГИЙ.....                  | 16 |
| Говердовская Т. В., Имзалиева М. Р. ПРАВОВОЕ РЕГУЛИРОВАНИЕ<br>ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: МЕЖДУНАРОДНЫЕ УСИЛИЯ<br>И ЭТИЧЕСКИЕ АСПЕКТЫ .....           | 20 |
| Дятлов С. А. ЭНТРОПИЙНО-СИНЕРГИЙНАЯ КОНЦЕПЦИЯ<br>КЛАССИФИКАЦИИ ВИДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА<br>В НЕЙРО-ЦИФРОВОЙ ЭКОНОМИКЕ.....                    | 28 |
| Жариков А. А. ВОПРОСЫ МЕТОДОЛОГИИ ПРАВОВОГО РЕГУЛИРОВАНИЯ<br>ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЦИФРОВОЙ ЭКОНОМИКЕ .....                                    | 32 |
| Ильин И. Г. СОЗДАНИЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ И ИХ ВЛИЯНИЕ<br>НА РЕАЛИЗАЦИЮ И ЗАЩИТУ КОНСТИТУЦИОННО ГАРАНТИРОВАННЫХ<br>ПРАВ.....                     | 36 |
| Карцхия А. А. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В НОВОЙ ПАРАДИГМЕ.....                                                                                         | 42 |
| Кийко Д. С. ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА<br>О РОБОТОТЕХНИКЕ И ИСКУССТВЕННОМ ИНТЕЛЛЕКТЕ.....                                      | 46 |
| Кийко Д. С. ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ПРОИЗВОДСТВА<br>И РАСПРОСТРАНЕНИЯ ВОЕННЫХ РОБОТОВ .....                                                    | 48 |
| Ларина О. И. О ПЕРСПЕКТИВАХ ПРАВОВОГО РЕГУЛИРОВАНИЯ<br>ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА .....                                                    | 51 |
| Новиков Д. О. ПРАВО И ЗАКОНОДАТЕЛЬСТВО ОБ ИСКУССТВЕННОМ<br>ИНТЕЛЛЕКТЕ: ТЕОРЕТИКО-ПРАКТИЧЕСКАЯ ХАРАКТЕРИСТИКА<br>И НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ..... | 53 |
| Савина В. С. АКТУАЛЬНЫЕ ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ<br>ТЕХНОЛОГИЙ ВИРТУАЛЬНОЙ И ДОПОЛНЕННОЙ РЕАЛЬНОСТИ.....                                      | 64 |
| Филипова И. А. СРАВНЕНИЕ ПОДХОДОВ К РЕГУЛИРОВАНИЮ<br>ИСКУССТВЕННОГО ИНТЕЛЛЕКТА (НА ПРИМЕРЕ РОССИИ, КИТАЯ,<br>ЕВРОПЕЙСКОГО СОЮЗА И США).....          | 68 |
| Шельменков В. Н. LEGAL TECH РЕВОЛЮЦИЯ: КАК ИСКУССТВЕННЫЙ<br>ИНТЕЛЛЕКТ МЕНЯЕТ ЮРИДИЧЕСКУЮ СФЕРУ .....                                                 | 72 |

## ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВА ЧЕЛОВЕКА

|                                                                                                                                                                     |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Алехина Е. С., Надтока С. В. ЦИФРОВИЗАЦИЯ ГУМАНИТАРНОЙ ДЕЯТЕЛЬНОСТИ В СИСТЕМЕ РАЗВИТИЯ ПРАВ ЧЕЛОВЕКА .....                                                          | 78  |
| Беляков К. О., Ирискина Е. Н. КЛАССИФИКАЦИЯ КОЛОНИАЛЬНЫХ ОБЩЕСТВ ПО ТИПАМ ФОРМИРУЕМЫХ ЗАВИСИМОСТЕЙ И ВОПРОСЫ ДЕЛЕГИРОВАНИЯ СУБЪЕКТНЫХ ПРАВ ЦИФРОВЫМ ДВОЙНИКАМ ..... | 82  |
| Бунова И. И. УГОЛОВНО-ПРАВОВАЯ ОХРАНА ПРАВА ЧЕЛОВЕКА НА СВОБОДУ СОВЕСТИ И ВЕРОИСПОВЕДАНИЯ В СОВРЕМЕННЫХ УСЛОВИЯХ ЦИФРОВИЗАЦИИ.....                                  | 94  |
| Воронин А. В. АКТУАЛИЗАЦИЯ ПРАВООЩИТНОГО РЕГУЛИРОВАНИЯ КОНСТИТУЦИОННОГО ПРАВА НА ПОСМЕРТНОЕ ТВОРЧЕСКОЕ БЫТИЕ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ .....                          | 99  |
| Иксанов И. С. ЦИФРОВОЕ ГРАЖДАНСТВО И НАРОДНЫЙ СУВЕРЕНИТЕТ: ПРОБЛЕМЫ РЕАЛИЗАЦИИ.....                                                                                 | 110 |
| Курбатова С. М. ЦИФРОВИЗАЦИЯ СИСТЕМЫ ПРАВОСУДИЯ КАК ЧАСТЬ МЕХАНИЗМА РЕАЛИЗАЦИИ ПРАВА НА ЗАКОННЫЙ СУД ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ .....                    | 116 |
| Осауленко Л. Н. ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВА ПОТРЕБИТЕЛЕЙ В ЕВРАЗИЙСКОМ ЭКОНОМИЧЕСКОМ СОЮЗЕ .....                                                                    | 120 |
| Твердышева А. Д.. ПРАВОВЫЕ АСПЕКТЫ ОХРАНЫ ГОЛОСА .....                                                                                                              | 126 |
| Фролова Т. Ю.. ЗАЩИТА ПАССИВНОГО ИЗБИРАТЕЛЬНОГО ПРАВА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: РОЛЬ СУДОВ РОССИЙСКОЙ ФЕДЕРАЦИИ ....                                                 | 129 |
| Н Шумакова. И. НОВЫЕ ТРЕНДЫ В ПРАВОВОМ РЕГУЛИРОВАНИИ ЦИФРОВОЙ СРЕДЫ И ЗАЩИТЫ ПРАВ ЧЕЛОВЕКА: ЗАРУБЕЖНЫЙ ОПЫТ .....                                                   | 134 |

## ЦИФРОВАЯ БЕЗОПАСНОСТЬ И ПРАВО

|                                                                                                                                                                           |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Белякова А. В. ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....                                                                               | 146 |
| Богданова А. Р. РОЛЬ ГОСУДАРСТВА В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ.....                                                                | 148 |
| Булгакова Е. В., Кубанков А. Н., Гудкова К. А., Булгаков В. В. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКИХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ: КОНЦЕПЦИЯ КИБЕРИММУНИТЕТА ..... | 151 |
| Графова Ю. М. НЕКОТОРЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ СОЦИОИНЖЕНЕРНЫМ АТАКАМ.....                                                                                                  | 157 |
| Грищенко Г. А. ПРАВОВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ.....                                                                      | 159 |
| Егоров Г. Г. Использование нейросетей ДЛЯ МОНИТОРИНГА ПРОТИВОПРАВНЫХ ОТНОШЕНИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ .....                                                               | 166 |
| Кылчыкбаев Т. Э. ПОНЯТИЕ КИБЕРБЕЗОПАСНОСТИ В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ .....                                                                                                  | 181 |

|                                                                                                                    |     |
|--------------------------------------------------------------------------------------------------------------------|-----|
| Легостаева Н. И., Медяник О. В. ДУАЛЬНЫЙ СИМБИОЗ ЦИФРОВЫХ ФИНАНСОВЫХ ТЕХНОЛОГИЙ И КИБЕРМОЩЕННОСТИ                  | 184 |
| Магдилова Л. В. ПРАВОВОЕ И ТЕХНИЧЕСКОЕ РЕГУЛИРОВАНИЕ ТЕХНОЛОГИЙ 5G                                                 | 189 |
| Сабиров Р. Р. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ЛИЦ, СОВЕРШАЮЩИХ ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ       | 194 |
| Фартушнова А. С. РЕАЛИИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В СИСТЕМЕ ФИНАНСОВЫХ И НАЛОГОВЫХ ПРАВООТНОШЕНИЙ | 200 |

### **ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ФИНАНСОВЫХ И НАЛОГОВЫХ ПРАВООТНОШЕНИЙ**

|                                                                                                                                                        |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Антропцева И. О. РОБОТЫ-СОВЕТНИКИ НА ФИНАНСОВОМ РЫНКЕ КАК ПРЕДМЕТ ПУБЛИЧНОГО ФИНАНСОВОГО КОНТРОЛЯ                                                      | 204 |
| Белоусов А. Л. ЦИФРОВЫЕ ФИНАНСОВЫЕ АКТИВЫ: ВОПРОСЫ РАЗВИТИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ                                                                      | 209 |
| Белякова Ю. М. РОЛЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ И СЕРВИСОВ В ПРОЦЕССЕ СУДЕБНОГО ДОКАЗЫВАНИЯ В СПОРАХ С НАЛОГОВЫМИ ОРГАНАМИ                                     | 212 |
| Боровикова Е. В. ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ГОСУДАРСТВЕННОГО ФИНАНСОВОГО КОНТРОЛЯ                                                                   | 219 |
| Евсикова Е. В. Шкляр Т. А. ЦИФРОВИЗАЦИЯ ПУБЛИЧНОГО ФИНАНСОВОГО КОНТРОЛЯ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ                                                        | 224 |
| Корзоватых Ж. М. ЦИФРОВЫЕ ТЕХНОЛОГИИ ДЛЯ РЕШЕНИЯ ЗАДАЧ ESG-ПОВЕСТКИ                                                                                    | 228 |
| Кривин Д. В. ИСПОЛЬЗОВАНИЕ IT-ТЕХНОЛОГИЙ В ЦЕЛЯХ ПРАВОМЕРНОГО ВОЗМЕЩЕНИЯ НДС                                                                           | 236 |
| Куркина Н. В. ИНДИВИДУАЛЬНЫЙ ИНВЕСТИЦИОННЫЙ ВЫЧЕТ ПРИ ИСЧИСЛЕНИИ НАЛОГА НА ДОХОДЫ ФИЗИЧЕСКИХ ЛИЦ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ                               | 243 |
| Кучина Я. О. РЕГУЛИРОВАНИЕ ЦИФРОВОЙ ВАЛЮТЫ В КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКЕ                                                                             | 248 |
| Миронова С. М. РОЛЬ НАЛОГОВЫХ ОРГАНОВ В ПРОТИВОДЕЙСТВИИ НЕЛЕГАЛЬНОЙ ЗАНЯТОСТИ: ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ                                           | 259 |
| Першин С. П. ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ С УЧЕТОМ СТЕПЕНИ ОБЩЕСТВЕННОЙ ОПАСНОСТИ ДЕЯНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ                             | 266 |
| Пономарева К. А., Симонов А. О. О ПРАВОВОЙ ПРИРОДЕ ДОХОДОВ ПО ОПЕРАЦИЯМ С ЦИФРОВЫМИ ФИНАНСОВЫМИ АКТИВАМИ С ТОЧКИ ЗРЕНИЯ МЕЖДУНАРОДНОГО НАЛОГООБЛОЖЕНИЯ | 273 |
| Файзрахманова Л. М. ЦИФРОВЫЕ ТЕХНОЛОГИИ В НАЛОГОВОМ АДМИНИСТРИРОВАНИИ ГОСУДАРСТВ БРИКС                                                                 | 277 |

## РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ В СФЕРЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И РОБОТОТЕХНИКИ

**М. А. Андреева,**  
сотрудник ООО «Компания БКС»

### ОТДЕЛЬНЫЕ ПРАВОВЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

**Аннотация.** В статье отражены выводы исследования, проведенного в целях выявления и предложения возможных путей решения проблем правового регулирования использования генеративного искусственного интеллекта. Выявлены правовые проблемы в части правомерности машинного обучения генеративного искусственного интеллекта на материалах, составляющих охраноспособные объекты, а также принадлежности сгенерированного контента с позиции авторского права. Для решения указанных проблем предлагается создание специальных фондов, созданных за счет взносов технологических компаний и из средств которых будет выплачиваться вознаграждение как за машинное обучение на соответствующих материалах, так и в случае неправомерного генеративного использования охраноспособных объектов. Кроме того, параллельно следует рассмотреть предоставление возможности субъектам исключать свои объекты авторских прав из массива материалов, предназначенных для машинного обучения, а также признать сгенерированный контент общественным достоянием.

**Ключевые слова:** право, искусственный интеллект, нейросети, интеллектуальные права, свободное использование произведений, пользовательские соглашения, промт, сгенерированный контент

### SELECTED LEGAL ASPECTS OF THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE

**Abstract.** This article presents the findings of a research conducted to identify and propose possible solutions to the problems of legal regulation of the use of generative artificial intelligence. The author has identified legal problems of the legality of machine learning of generative artificial intelligence on materials constituting protectable objects, and of the ownership of generated content from the standpoint of copyright. Some possible solutions lies in creating special funds by contributions from technology companies and from which remuneration will be paid both for machine learning on relevant materials and in the event of illegal generative use of protectable objects. Besides of that, it is necessary to consider providing the opportunity for subjects to exclude their copyright objects from the array of materials intended for machine learning, and also to recognize the generated content as public domain.

**Keywords:** law, artificial intelligence, neural networks, intellectual rights, free use of works, user agreements, prompt, generated content

**Введение.** В 50-е гг. XX века впервые был применен термин "artificial intelligence" («искусственный интеллект»), исчерпывающее толкование которого до сих пор не сформулировано, что создает препятствия для правового регулирования применения систем искусственного интеллекта в современных реалиях. Усложняет обстоятельства и непрерывное развитие за счет применения метода машинного обучения [6. С. 75] программных продуктов, предлагаемых на рынке технологий, в частности нейросетей – систем, способных генерировать контент, распознавать речь, выявлять закономерности данных и т. п. Нейросети воспроизводят базовый механизм обработки информации посредством распределения каждого требуемого параметра между нейронами: например, один нейрон может распознавать черты носа, а другой нейрон – конкретное лицо [14. С. 21]. На мировом рынке такими системами являются GPT-4, ChatGPT, Stable Diffusion 2.0, MidJourney, а на российском рынке они представлены продуктами компаний «Сбер» (GigaChat, Kandinsky) и «Яндекс» (Yandex GPT, «Шедеврум»). Безусловно, нейросети предоставляют возможность принципиально по-новому работать с информацией и контентом [4], полезный эффект этого предопределяет дальнейшее развитие данной сферы. Следовательно, правовые проблемы применения метода машинного обучения требуют качественных решений правового регулирования имеющихся и будущих технологических продуктов.

**Основная часть.** В рамках настоящего исследования рассмотрены два аспекта правового регулирования применения генеративного ИИ:

1. Законность использования результатов интеллектуальной деятельности других людей для обучения нейросетей без их разрешения.

2. Появление интеллектуальных прав на контент, созданный нейросетями.

В зарубежной правовой действительности ведутся судебные разбирательства по требованиям правообладателей, чьи объекты авторских прав были использованы при машинном обучении нейросетей в отсутствии их согласия и выплат вознаграждения, хотя создатели нейрогенеративных сетей извлекают коммерческую выгоду. Такими объектами, в частности, служат, юридические исследования, работы художников, фотографии, коды, литературные произведения, видеоролики [3]. Однако в российской правоприменительной практике подобных исковых требований к создателям нейросетей не предъявлялось, но это вовсе не значит, что аспект правомерности обучения нейрогенеративных сетей не требует правового регулирования.

В качестве обоснования правомерности использования результатов интеллектуальной деятельности в процессе машинного обучения применяются концепции их добросовестного использования. Например, в США законодательно допускается такое использование в особых целях, в том числе критики, комментирования, новостных сообщений, обучения, исследования [13. С. 115]. Несмотря на это, технологическое добросовестное использование требует запроса разрешения в отношении каждого такого использования. В отличие от указанного подхода в российских правовых условиях применяется иной правовой инсти-

тут – свободное использование произведения. Различие заключается в том, что в интеллектуальном праве России предусмотрены строго определенные случаи использования объекта авторских прав без согласия его правообладателя, например, ст. 1273, 1274, 1277, 1278, 1279 Гражданского кодекса Российской Федерации [2]. Концепцию добросовестного использования следует признать гибкой, но переход на правовое регулирование на ее основе невозможен без уточнения его действия судебными органами. А это в условиях отсутствия устойчивых доктринальных учений и единой выработанной законодателем политики поддержки развития технологий становится проблематичным: высока степень произвольности судебных решений. Чтобы устранить правовой диссонанс, предлагаем внесение компаниями, осуществляющими запуск рассматриваемых продуктов, взносов в специальные фонды, которые будут распределять справедливое вознаграждение правообладателям используемых для обучения объектов авторских прав. Кроме того, следует предоставить таким правообладателям возможность отказа от сбора данных для обучения нейросетей, как это предоставляет компания Apple [5]. Это позволит, на наш взгляд, достичь баланса: учесть важность инновационного продукта, который не способен был создать правообладатель объектов авторского права, используемых для машинного обучения, а также обеспечить соразмерную компенсацию такого использования.

Сгенерированный нейросетями контент крайне схож с результатом интеллектуальной деятельности, созданным творческим трудом автора. Так, отдельные правоведы предлагают создать правовую фикцию – электронное лицо, обладающее правосубъектностью [1. С. 310]. Тем не менее вызывает сомнения такое допущение в части обоснованности применения к любым моделям искусственного интеллекта, даже к узкоспециализированным. И неясно, как на это отреагирует сложившийся порядок разработки и применения правовых норм, основанных на антропоцентристских взглядах. Ясно и то, что такой подход подлежит тщательному анализу с философских и этических позиций прежде законодательной регламентации.

М. А. Рожкова и О. В. Исаева отмечают предопределяющее значение творческого характера деятельности, в результате которой созданы охраноспособные объекты, и относят сгенерированный контент к числу данных, которые генерирует искусственный интеллект в процессе поставленной человеком задачи. Следовательно, сгенерированный контент не может быть признан объектом авторских прав [9. С. 170]. Однако справедливо ли это с учетом содержания промтов пользователей – инструкций, вводимых в нейросеть? Сейчас широко распространены курсы промт-инжиниринга, значение которого заключается в успешной разработке и оптимизации промтов [10]. Кроме того, нельзя опровергнуть то, что творчество обладает широким диапазоном значения и может включать креативную деятельность, основанную на новом взгляде на ранее выявленную закономерность.

Создатели нейросетей исходят из того, что сгенерированный контент представляет собой объект интеллектуальных прав. Подтверждение этому находим в правовых документах – пользовательских соглашениях. Так, в п. 3.4. пользовательского соглашения нейросети Yandex GPT предусмотрено условие,

направленное на регламентацию правомерности использования компанией «Яндекс» запросов (промтов) и сгенерированного контента пользователя [12]. При этом условие сформулировано с учетом признаков лицензии – срока и территории, а именно на территории всего мира и без ограничения срока. Соглашение об использовании сервиса GigaChat также содержит условия возложения на пользователя возможных правовых рисков использования и выгрузки результатов интеллектуальной деятельности третьих лиц с целью создания сгенерированного контента. Согласно п. 6.2. указанного соглашения на сгенерированный контент клиент (пользователь), приобретающий исключительные права на сгенерированный контент, передает простую, безвозмездную, безотзывную лицензию правообладателю сервиса GigaChat (п. 6.2 Соглашения об использовании сервиса GigaChat) на весь срок действия исключительного права на территории всего мира любыми способами [11].

Становится очевидным, что компании допускают и исходят из возникновения интеллектуальных прав на сгенерированный контент у пользователей, обеспечивая в силу этого получение для своих целей лицензий на сгенерированный контент. Однако в то же время представляется возможным выявить условия другого характера. Так, оба правообладателя рассматриваемых нейросетей допускают, что сгенерированный контент может быть не уникальным. И это действительно так, ведь нейросеть обучается содержимым единой сети Интернет, а алгоритмы работы нейросетей вероятно сходны с алгоритмами аналогичных продуктов. По своему содержанию нейросеть адаптирует свою цепочку операций для приближения предполагаемого результата для заданного набора входных данных (промта), при этом число (показатель) такого приближения может быть одинаковым для разных пользователей, что влияет на конечный результат. Кроме этого, правообладатель сервиса GigaChat под сгенерированным контентом рассматривает, в том числе информацию, иные объекты, не являющиеся результатами интеллектуальной деятельности (п. 1.10 Соглашения об использовании сервиса GigaChat). Соответственно, анализ пользовательских соглашений позволяет сформулировать вывод о том, что в условиях отсутствия единообразного правового регулирования вопросов применения генеративного искусственного интеллекта участники рынка технологий предпочитают исключить возможные правовые риски путем признания ценности промтов пользователей и сгенерированного в результате их исполнения контента. Однако это сопровождается одновременным и, пожалуй, противоречащим вышеуказанному признанием такого характера функционирования нейросети, который допускает отсутствие уникальности контента. С позиции практического решения возникающих вопросов, полагаем, такой подход в настоящее время является единственным верным для защиты интересов создателей нейросетей от возможных финансовых потерь.

Российская судебная правоприменительная практика по вопросам применения генеративного искусственного интеллекта только формируется. В деле № А42-3966/2023 суд апелляционной инстанции отклонил довод ответчика о том, что изображение было создано искусственным интеллектом, а следовательно, не может быть признано объектом авторских прав [7]. При этом достаточным для рассмотрения спора признано наличие у истца файлов изображения

в исходном формате, но судом не была дана полная и исчерпывающая оценка довода ответчика (подателя жалобы). В деле № А40-200471/2023 судом апелляционной инстанции оставлено в силе решение, в мотивировочной части которого указано, что видеоролик, созданный посредством технологии дипфейка, является объектом авторских прав, которые возникли у всей команды, работавшей над ним [8]. Следовательно, судебный орган исходит из суждения о том, что дипфейк служит способом создания произведения, помощником человека в осуществлении творческой деятельности. С учетом выводов суда сгенерированный контент приобретает статус охраноспособного объекта. Очевидно, что вопрос о первичной охраноспособности сгенерированного контента продолжает оставаться открытым в российской судебной практике. Содержание такого порядка будет заключаться в том, что с учетом значимости передовых технологий для развития экономики сгенерированный контент будет признаваться общенародным достоянием, а в случае выявления в составе сгенерированного контента фрагментов, признаков охраноспособных объектов, принадлежащих третьим лицам, подобное неправомерное генеративное использование будет служить основанием для выплаты законодательно установленного возмещения из средств ранее упомянутых специальных фондов. Помимо этого, соответствующий сгенерированный контент будет либо отредактирован, либо уничтожен. Однако такой выплате будет предшествовать анализ обоснованности обращения третьих лиц, выявление достаточных признаков неправомерного генеративного использования, которое потребует анализа целого массива данных нейросетей и разработку алгоритма действий по подтверждению использования генеративным искусственным интеллектом результатов интеллектуальной деятельности третьих лиц. Предложенный механизм, на наш взгляд, является приемлемым до момента достижения машинным обучением параметра, позволяющего исключить нарушение авторских прав, то есть самопроизвольного вычисления и исключения потенциалов такого нарушения.

**Заключение.** В связи с этим автором предлагается подход, при котором третьи лица, чьи результаты интеллектуальной деятельности были использованы в качестве обучающего материала, приобретают право на получение законодательно регламентированного размера вознаграждения и возможность установить запрет такого использования. Помимо этого, отсутствует и ясность в правовой принадлежности сгенерированного контента, в том числе в ее неразрывной связи с защитой интеллектуальных прав третьих лиц. Вполне вероятно рассмотреть правовое регулирование, сводимое к выплате устойчивого возмещения в случае неправомерного генеративного использования результатов интеллектуальной деятельности третьих лиц. И, помимо этого, допустить переход по умолчанию сгенерированного контента в общественное достояние. А с целью отделения классического неправомерного использования объектов авторских прав, влекущего по общему правилу гражданско-правовую ответственность, от нейрогенеративного, автор предлагает воспользоваться маркировкой сгенерированного контента.

### Список литературы

1. Болотаева О. С. Искусственный интеллект и право интеллектуальной собственности // Право и государство: теория и практика. – 2023. – № 10(226). – С. 309–311.
2. Гражданский кодекс Российской Федерации (часть четвертая) : федеральный закон от 18.12.2006 г. № 230-ФЗ (ред. от 30.01.2024) // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=468390&dst=100372#pVwdhNUCvVrGB7GS>
3. Двадцать шесть судебных дел против OpenAI, Anthropic и ...: короткий обзор судебных исков против крупнейших ИИ-компаний [Электронный ресурс]. – URL: <https://habr.com/ru/articles/839620/>
4. Исследование «10 трендов ИИ» [Электронный ресурс]. – URL: <https://www.fintechru.org/analytics/issledovanie-10-trendov-ii/>
5. Крупнейшие сайты объявили бойкот Apple и ее ИИ [Электронный ресурс]. – URL: <https://www.gazeta.ru/tech/news/2024/08/30/23808937.shtml>
6. Кузьменков М. Ю. Лицензионные соглашения, используемые при распространении программных пакетов машинного обучения // Актуальные проблемы российского права. – 2023. – Т. 18, № 11. – С. 73–82.
7. Постановление 13-го ААС по делу А42-3966/2023 от 28.09.2023. [Электронный ресурс]. – URL: <https://ras.arbitr.ru/>
8. Постановление 9-го ААС по делу № А40-200471/2023 от 06.02.2023 г. [Электронный ресурс]. – URL: <https://ras.arbitr.ru/>
9. Рожкова М. А., Исаева О. В. Квалификация в качестве производных произведений объектов, создаваемых на основе результатов машинного обучения и «произведений» искусственного интеллекта // Интеллектуальные права в цифровую эпоху: избранные аспекты: коллективная монография. Вып. 19 / рук. авт. кол. и науч. ред. М. А. Рожкова; вступ. ст.: В. А. Корнеев. – М.: ГАУГН Пресс, 2023.
10. Руководство по промпт-инжинирингу [Электронный ресурс]. – URL: <https://www.promptingguide.ai/ru>
11. Соглашение об использовании сервиса GigaChat для физических лиц [Электронный ресурс]. – URL: <https://developers.sber.ru/docs/ru/policies/gigachat-agreement/individuals?q=%D0%BB%D0%B8%D1%86%D0%B5%D0%BD%D0%B7%D0%B8>
12. Условия использования Yandex GPT [Электронный ресурс]. – URL: [https://yandex.ru/legal/yagpt\\_termsfuse/](https://yandex.ru/legal/yagpt_termsfuse/)
13. Kline D., Kappos D. Introduction to intellectual property. – L.: Openstax, 2021.
14. Multidisciplinary Perspectives on Artificial Intelligence and the Law // Law, Governance and Technology Series // Ed.: H. S. Antunes, P. M. Freitas, A. L. Oliveira, C. M. Pereira, E. Vaz de Sequeira, L. B. Xavier – L.: Springer, 2024.

**Е. Н. Гладкая,**

кандидат юридических наук, доцент,  
Институт экономики Национальной  
академии наук Беларуси

## **ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И НОСИТЕЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КОНТЕКСТЕ РАЗВИТИЯ ПРАВА ВЫСОКИХ ТЕХНОЛОГИЙ**

**Аннотация.** Работа посвящена вопросам установления правового статуса искусственного интеллекта и его носителей, а также правового регулирования объектов, создаваемых с использованием технологий искусственного интеллекта. В результате проведенного анализа предложена авторская трактовка понятия «искусственный интеллект», определены его роль и место в системе правовых отношений, а также представлены рекомендации относительно правового режима таких объектов.

**Ключевые слова:** право, право высоких технологий, правовой статус, правовой режим, объект правоотношения, цифровые технологии, искусственный интеллект, носитель искусственного интеллекта

## **ARTIFICIAL INTELLIGENCE AND THE CARRIER OF ARTIFICIAL INTELLIGENCE IN THE CONTEXT OF THE DEVELOPMENT OF HIGH-TECHNOLOGY LAW**

**Abstract.** The article is devoted to the issues of establishing the legal status of artificial intelligence and its carriers, as well as the legal regulation of objects created using artificial intelligence technologies. As a result of the analysis, the author's interpretation of the concept of "artificial intelligence" is proposed, its role and place in the system of legal relations are determined, and recommendations regarding the legal regime of such objects are presented.

**Keywords:** law, high-tech law, legal status, legal regime, object of legal relations, digital technologies, artificial intelligence, carrier of artificial intelligence

Развитие технологий искусственного интеллекта (далее – ИИ) влечет за собой возникновение проблем использования ИИ в различных сферах общественной жизни. В первую очередь в сфере интеллектуальной собственности. В связи с тем, что с помощью технологий ИИ возможно создание объектов, внешне схожих с результатами творческого труда человека, встают вопросы о возможности отнесения таких объектов к объектам интеллектуальной собственности, принадлежности авторских прав на указанные объекты и их защиты. Отсутствие должного правового регулирования создает предпосылки для неправомерного использования технологий ИИ в сфере интеллектуальной собственности, а также объектов, созданных с их помощью.

В контексте развития права высоких технологий видится необходимым проведение специальных исследований об ИИ с целью поиска ответа на постав-

ленные вопросы. Первоочередным в данной части представляется определение правового статуса ИИ и его носителя, правового режима объектов, созданных с помощью технологий ИИ.

По мнению Н. В. Хамитова, С. В. Киселицы, О. Л. Деркач, основоположником концепции «сильного» и «слабого» ИИ следует считать Р. Пенроуз [21. С. 97]. Как отмечают ученые, согласно данной концепции «сильный» ИИ – это алгоритм, созданный программным путем, научная задача которого сводится к написанию совершенного алгоритма; «слабый» ИИ представляет собой математическое суждение (включая алгоритм), которое всегда будет либо неполным, либо внутренне противоречивым, закладываемое субъектом-создателем алгоритма и актуализируемое его средой обитания [21. С. 97]. Представляется, что при формировании правового регулирования общественных отношений, основанных на использовании технологий ИИ, следует учитывать возможное развитие как «слабого», так и «сильного» ИИ.

В настоящее время как теоретиками, так и практиками все чаще поднимаются вопросы о необходимости определения правового статуса ИИ. Для этого в юридической литературе предлагается:

- использовать концепцию «электронного лица» [13. С. 70–71; 20. С. 238; 7. С. 52];
- пересмотреть традиционные подходы к понятию «субъект права», распространить правовой статус субъекта права на отдельные объекты материального мира, в том числе ИИ [20. С. 238; 7. С. 51–52];
- распространить качества юридического лица на ИИ [20. С. 239; 7. С. 52];
- применить к ИИ концепцию «техноперсонализма», т. е. наделить его правами и обязанностями, ранее присущими только определенным субъектам права [20. С. 239];
- использовать в отношении роботов правовой режим животных [7. С. 52].

Обозначенное выше предложение о наделении наиболее продвинутых роботов правовым статусом «электронного лица» поддержано в юридической литературе рядом ученых. В частности, П. М. Морхат отмечает, что «<...> концепт правосубъектности «электронное лицо» может быть в некоторой перспективе внедрен, но пока для весьма ограниченного числа случаев сложных роботизированных систем с искусственным интеллектом» [13. С. 70–71].

В. В. Наумов, В. Б. Архипов видят необходимым наделение роботов специальной правосубъектностью только для определенных целей, в частности для торговли через ботов в сети Интернет и других [4. С. 160].

Г. А. Гаджиев и Е. А. Войникас, дискуссия на тему о необходимости наделения роботов правосубъектностью, приходят к выводу о том, что «<...> если признание робота субъектом права имеет какой-либо смысл или назначение, то оно заключается в более эффективном и сбалансированном распределении ответственности. Напротив, если робот не способен возместить нанесенный им вред, необходимость признания его субъектом права становится проблематичной <...>» [8. С. 41].

Другие ученые отрицают всякую возможность наделения ИИ правосубъектностью. Среди них С. А. Симонян и А. С. Гамбарян. Указанные ученые счи-

тают, что «<...> признание правосубъектности искусственного интеллекта не является обоснованным. Создание нового субъекта права в виде искусственного интеллекта не является необходимым шагом для развития права» [20. С. 240].

А. А. Васильев, Ж. И. Ибрагимов, анализируя концепцию электронного лица применительно к ИИ, приходят к выводу о том, что на текущем этапе научной дискуссии она остается весьма спорной [7. С. 52].

Е. Н. Агibalова, Е. А. Перекрёстова констатируют, что поскольку «<...> программы и инновационные технологии, в частности искусственный интеллект, являются всего лишь инструментом получения новых результатов интеллектуальной деятельности» в качестве автора произведения следует рассматривать лицо, использующее данное произведение [3. С. 126]. Данная точка зрения подерживается Н. Л. Малаховой, Ю. П. Присяжнюк, Ю. С. Сперанской [11. С. 64] и другими исследователями [5; 9; 10].

Таким образом, в настоящее время в юридической литературе сложились два направления. Сторонники первого допускают наделение ИИ некоторыми элементами правового статуса субъекта права. Сторонники второго отрицают такую возможность. Принимая во внимание приведенные точки зрения, мы придерживаемся позиции тех ученых, которые относятся ко второму направлению, поскольку не видим возможности наделения ИИ правовым статусом субъекта права либо его отдельными элементами. Полагаем, что в выводах о правовом статусе ИИ акцент должен оставаться на слове «искусственный», свидетельствующем о его неестественном происхождении, синтетическом характере, суррогатности, фальшивости. Технологии ИИ – прежде всего *технологии*, созданные и обученные человеком совершать те или иные действия, которые, по нашему мнению, не должны выходить из-под контроля человека.

### Список литературы

1. «Правило» в Толковом словаре Д. Н. Ушакова [Электронный ресурс]. – URL: <https://dic.academic.ru/dic.nsf/ushakov/966302>
2. «Система» в Толковом словаре Д. Н. Ушакова [Электронный ресурс]. – URL: <https://academic.ru/searchall.php?SWord=%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0&from=xx&to=ru&did=ushakov&stype=>
3. Агibalова Е. Н., Перекрёстова Е. А. Право авторства на произведения, созданные искусственным интеллектом // Эпоха науки. – 2020. – № 24. – С. 124–126.
4. Архипов В. В., Наумов В. Б. О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности // Закон. – 2017. – № 5. – С. 157–170.
5. Бондаренко Н. Л., Гладкая Е. Н., Конаневич Ю. Г. Совершенствование понятийно-категориального аппарата правовой науки в контексте решения задачи разграничения понятий «статус», «правосубъектность», «правовое положение», «правовой режим» // Актуальные проблемы гражданского права. – 2020. – № 2(16). – С. 8–40.

6. Борисов А. В., Босов А. В., Жуков Д. В. Стратегия исследований и разработок в области искусственного интеллекта I: основные понятия и краткая хронология // Системы и средства информатики. – 2021. – Т. 31, № 1. – С. 57–68.
7. Васильев А. А., Ибрагимов Ж. И. Правовое регулирование робототехники и искусственного интеллекта в Европейском союзе // Российско-Азиатский правовой журнал. – 2019. – № 1. – С. 50–54.
8. Гаджиев Г. А., Войникас Е. А. Может ли робот быть субъектом права? (поиск правовых форм для регулирования цифровой экономики) // Право: журнал Высшей школы экономики. – 2018. – № 4. – С. 41–48.
9. Гражданский кодекс Республики Беларусь [Электронный ресурс]: 07.12.1998 № 218-З : принят Палатой представителей 28.10.1998: одобрен Советом Республики 19.11.1998 (ред. от 05.01.2024) // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.
10. Камышанский В. П., Корецкий А. В. Понятие и правовой статус носителя искусственного интеллекта // Власть закона. – 2019. – № 1 (37). – С. 42–50.
11. Малахова Н. Л., Присяжнюк Ю. П., Сперанская Ю. С. Результаты интеллектуальной деятельности, созданные искусственным интеллектом // Российский правовой журнал. – 2020. – № 2(3). – С. 57–65.
12. Морхат П. М. К вопросу о правовой дефиниции термина «искусственный интеллект» // Вестн. МГПУ. Сер. Юридические науки. – 2018. – № 2(30). – С. 74–80.
13. Морхат П. М. Юнит искусственного интеллекта как электронное лицо // Вестн. Моск. гос. обл. ун-та. Сер. Юриспруденция. – 2018. – № 2. – С. 61–73.
14. Национальная стратегия развития искусственного интеллекта на период до 2030 г. [Электронный ресурс]: утвержд. Указом Президента Российской Федерации от 10.10.2019 № 490 // КонсультантПлюс. Россия / ЗАО «Консультант-Плюс». – М., 2024.
15. О Рекомендациях по нормативному регулированию использования искусственного интеллекта, включая этические стандарты для исследований и разработок [Электронный ресурс]: постановление Межпарламентской Ассамблеи государств-участников Содружества Независимых Государств от 14.04.2023 № 55-23 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.
16. Образовательный стандарт высшего образования. Специальность 1-55 01 01 Интеллектуальные приборы, машины и производства [Электронный ресурс]: утвержд. постановлением Министерства образования Республики Беларусь от 30.08.2013 № 88 (ред. 14.03.2024) // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.
17. Резаев А. В., Трегубова Н. Д. (2023). Возможность и необходимость человеко-ориентированного искусственного интеллекта в юридической теории и практике // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 564–580. DOI: <https://doi.org/10.21202/jdtl.2023.24>
18. Резолюция Европарламента вместе с рекомендациями Комиссии по гражданско-правовому регулированию в сфере робототехники Европейского

Парламента «Нормы гражданского права о робототехнике» от 16.02.2017 [Электронный ресурс]. – URL: [https://robopravo.ru/riezoliutsiia\\_ies](https://robopravo.ru/riezoliutsiia_ies)

19. Свиридова Е. А. Генезис понятия искусственного интеллекта с точки зрения права в условиях реализации национального проекта «Цифровая экономика Российской Федерации» // Экономика. Налоги. Право. – 2020. – № 3. – С. 152–160.

20. Симонян С. А., Гамбарян А. С. Необходимость и проблемы правосубъектности искусственного интеллекта // Юридическая техника. – 2021. – № 15. – С. 237–240.

21. Хамитов Н. В., Киселица С. В., Деркач О. Л. Проблема телесности субъекта искусственного интеллекта в контексте теории эволюции естественного и искусственного интеллекта // Проблемы социальной роботы: философия, психология, социология. – 2017. – № 2 (10). – С. 95–102.

22. Хисамова З. И., Бегишев И. Р. История становления и теоретико-правовые подходы к толкованию понятия «искусственный интеллект» // Алтайский юридический вестник. – 2020. – № 3 (31). – С. 31–38.

**Т. В. Говердовская,**

кандидат юридических наук, доцент,  
Астраханский государственный университет  
имени В. Н. Татищева

**М. Р. Имзалиева,**

старший преподаватель,  
Астраханский государственный университет  
имени В. Н. Татищева

## **ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: МЕЖДУНАРОДНЫЕ УСИЛИЯ И ЭТИЧЕСКИЕ АСПЕКТЫ**

**Аннотация.** В статье анализируются те усилия, которые предпринимают международные межправительственные и неправительственные организации с целью правового регулирования деятельности по разработке и использованию систем искусственного интеллекта. Сделан вывод о том, чтобы все заинтересованные стороны продолжали работать над созданием эффективных правовых рамок, которые будут способствовать как развитию технологий, так и защите прав человека в условиях их использования.

**Ключевые слова:** искусственный интеллект, этические аспекты, системы искусственного интеллекта, ЮНЕСКО, ОЭСР, Европейский Союз, права человека, дискриминация

## LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE: INTERNATIONAL EFFORTS AND ETHICAL ASPECTS

**Abstract.** The article analyzes the efforts made by intergovernmental and non-governmental organizations to legally regulate the development and use of artificial intelligence systems. It is concluded that all stakeholders should continue to work to create effective legal frameworks that will promote both the development of technology and the protection of human rights in the conditions of their use.

**Keywords:** artificial intelligence, ethical aspects, artificial intelligence systems, UNESCO, OECD, European Union, human rights, discrimination

**Введение.** Впервые идея признания искусственного интеллекта субъектом права была затронута в концепции американского профессора Л. Солума, который предположил, что развитие науки и техники может дать искусственному интеллекту способность быть управляющим трастом, при этом правомерность рассуждений Солума стали основой анализа основных характеристик человека в правовой сфере [8].

**Основная часть.** Современный мир стремительно меняется под воздействием новых технологий, и информационно-коммуникационные технологии играют ключевую роль в формировании общества [2].

В современных реалиях искусственный интеллект можно определить как многогранную и комплексную сферу деятельности, которая собрала в себе результаты технических, экономических и юридических, а также педагогических наук, при этом нужно помнить, что создание рационально-технологического решения создает необходимость сохранения непредвзятости мнения и взглядов разработчика в соответствии с целевой предметной областью.

В последние годы искусственный интеллект (далее – ИИ) стал неотъемлемой частью различных аспектов жизни общества, включая экономику, образование и безопасность. С его стремительным развитием возникает необходимость в правовом регулировании, которое обеспечивало бы этическое и безопасное использование технологий ИИ. В этом контексте международные организации играют ключевую роль в формировании стандартов и рекомендаций, направленных на гармонизацию подходов к регулированию ИИ на глобальном уровне.

Тема правового регулирования систем искусственного интеллекта подчеркивает важность этических аспектов и необходимость международного сотрудничества для обеспечения безопасного и устойчивого развития технологий, при этом национальные правительства в условиях глобализации и быстрого развития ИИ сталкиваются с вызовами, требующими согласованных действий на международном уровне.

Деятельность международных организаций в области правового регулирования использования систем искусственного интеллекта рассматривает основные документы и рекомендации, выработанные ЮНЕСКО и ОЭСР, а также их влияние на национальные правовые системы. Особое внимание уделяется этическим принципам, которые должны лежать в основе разработки и применения технологий ИИ, а также важности международного сотрудничества для достижения

устойчивого и безопасного развития в этой сфере, правовое регулирование этических норм [8] в контексте использования искусственного интеллекта необходимо при активном участии государства и международных организаций в формировании единого подхода проблеме [10].

Важно разработать международные универсальные нормы и стандарты, которые бы регулировали применение и воздействие искусственного интеллекта на общество, экономику и права человека.

Существует несколько важных аспектов, которые требуют внимания со стороны международного сообщества, такие как этика использования искусственного интеллекта, защита персональных и конфиденциальных данных, ответственность за принимаемые решения, обеспечение безопасности и прозрачности самих систем ИИ.

Однако на данный момент международно-правовое регулирование систем ИИ находится в стадии разработки и требует дальнейших обсуждений и согласований между странами и международными организациями. До марта 2024 года в мире не существовало какого бы то ни было юридически обязательного акта в сфере правового регулирования разработки и использования систем ИИ. В основном были акты мягкого права, которые в большей степени регулировали этические вопросы использования данных систем, но 14 марта 2024 года в Европейском Союзе был принят обязательный Регламент об установлении гармонизированных (согласованных) правил в области искусственного интеллекта.

Рассматривая международно-правовое регулирование систем ИИ, большинство авторов ссылаются на Окинавскую Хартию глобального информационного общества [3]. Соглашаясь с рядом российских авторов, следует подчеркнуть, что Окинавская хартия действительно не является юридически обязательным документом, порождающим обязательства национальных правительств перед международным сообществом, тем не менее именно этот декларативный документ является основой для представителей доктрины как российской, так и зарубежной при анализе правового регулирования информационных технологий [6].

Евразийский экономический союз (ЕАЭС) – организация региональной экономической интеграции, государства-члены которой, а также официальные лица Союза неоднократно упоминали о том, что применение современных технологий делает экономику стран конкурентоспособной и, соответственно, требуется не только применение новейших достижений техники и технологий, в том числе систем ИИ, но и их правовое регулирование. Евразийская экономическая комиссия занимается регулированием систем ИИ в рамках стратегии развития цифровой экономики государств-членов ЕАЭС [5]. Это включает в себя разработку соответствующих правовых и программных документов, стандартов и требований для обеспечения безопасности, эффективности и этичного использования ИИ.

Организация экономического сотрудничества и развития (ОЭСР) занимается разработкой международных стандартов и рекомендаций с целью унифицированного развития различных отраслей экономики в разных странах. Соответственно, осознавая то, что применение современных технологий оказывает су-

щественное влияние на конкурентоспособность государств, ОЭСР с 2016 г. активно занимается вопросами изучения систем ИИ. В 2019 г. были приняты Руководящие принципы для проведения политики в области искусственного интеллекта, а уже 3 мая 2024 г. данные принципы подверглись редакции с учетом технологических изменений.

В преамбуле Принципов отмечается неоспоримый факт того, что системы ИИ уже прочно вошли в нашу жизнь, изменяя экономику, сферу труда и общества в целом. Подобные изменения уже не остановить, они имеют глобальные последствия, при этом авторы подчеркивают, что последствия использования систем ИИ труднопредсказуемы.

Искусственный интеллект играет ключевую роль в различных сферах современного общества, взаимодействуя с людьми и оказывая значительное влияние на их повседневную жизнь.

Взаимодействие человека и искусственного интеллекта становится все более тесным и взаимовыгодным, приводя к созданию инновационных решений, улучшению качества жизни и повышению эффективности работы в различных сферах деятельности. Вместе человек и искусственный интеллект могут достичь невероятных результатов, преодолевая границы возможностей и совершенствуя мир вокруг себя [7].

Поэтому «использование возможностей, предлагаемых приложениями искусственного интеллекта, и решение возникающих проблем, а также расширение возможностей заинтересованных сторон для взаимодействия необходимы для содействия внедрению надежного искусственного интеллекта в обществе и для превращения надежности искусственного интеллекта в конкурентный параметр на мировом рынке».

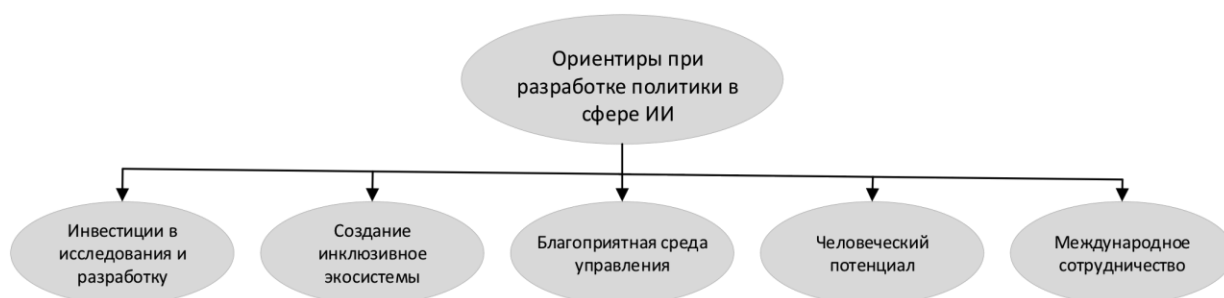
Важной особенностью документа является наличие раздела с основными терминами, такими как система ИИ, жизненный цикл системы, знания в области ИИ, участники процесса и заинтересованные стороны. Принципы ОЭСР носят рекомендательный характер и включают в себя непосредственно пять принципов разработки и использования систем ИИ (таблица представлена ниже).

#### **Рекомендации для национальных правительств при разработке политики в сфере искусственного интеллекта**

| Наименование                                                                                                                       | Содержание                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Инклюзивный рост, устойчивое развитие и благосостояние                                                                             | Использование надежных систем ИИ для устойчивого развития и повышения благосостояния без какой бы то ни было дискриминации                    |
| Уважение верховенства закона, прав человека и демократических ценностей, включая справедливость и неприкосновенность частной жизни | Действия на уважении демократических ценностей и прав человека при внедрении механизмов человеческого надзора и контроля за работой систем ИИ |

| Наименование                      | Содержание                                                                                                                                                                                                                                                                                          |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Прозрачность и объяснимость       | Положения обязывают разработчиков и пользователей раскрывать информацию с целью улучшения осведомленности населения о механизмах и процедурах работы искусственного интеллекта и тем самым повысить доверие общественности к данным разработкам с возможностью оспорить результаты решений, системы |
| Надежность, защищенность и защита | Надежная работа правильной эксплуатации данных систем ИИ в случаях неправильного использования или иных неблагоприятных условий, при которых должна быть обеспечена безопасность ввода и вывода из эксплуатации системы ИИ без причинения вреда целостности информации [8]                          |
| Подотчетность                     | Системный подход к управлению рисками на каждом этапе жизненного цикла системы ИИ для поддержания ответственного делового поведения посредством сотрудничества между различными субъектами ИИ и другими заинтересованными сторонами                                                                 |

Помимо самих этических принципов для работы с системами ИИ Рекомендации содержат и определенные ориентиры для национальных правительств при разработке политики в данной сфере. К таковым авторы относят ориентиры на рисунке ниже.



### Ориентиры при разработке политики в сфере искусственного интеллекта

Рекомендации ЮНЕСКО по этике искусственного интеллекта действительно представляют собой важный набор ориентиров для правительств, способствующих эффективному регулированию использования технологий ИИ. Эти принципы направлены на обеспечение безопасного, справедливого и этического применения ИИ, что становится особенно актуальным в условиях его стремительного развития и внедрения в различные сферы жизни.

Сферы политики, указанные в рекомендациях, охватывают широкий спектр вопросов, включая управление, защиту данных, международное сотрудничество и образование. Это позволяет государствам разрабатывать комплексные стратегии, которые учитывают как технологические, так и социальные аспекты, способствуя гармоничному и безопасному развитию искусственного интеллекта в обществе

ЮНЕСКО признает, что системы ИИ открывают колоссальные возможности перед человечеством от постановки диагнозов до повышения эффективности труда, однако эти стремительные изменения вызывают значительное число опасений с этической точки зрения. Не будут ли системы ИИ предвзятыми, не создадут ли они еще большее неравенство, не приведут ли они к дискриминации и нарушению прав человека, а может быть к изменениям климата или разжиганию вооруженных конфликтов? [7]».

Преамбула этического кодекса ЮНЕСКО обращает внимание на то, что национальное регулирование систем ИИ не будет столь успешным, что искусственный интеллект не имеет государственных границ и нужен глобальный подход, который будет основан на принципах защиты прав человека, гендерном равенстве и недискриминации, ответственности за психическое и физическое благополучие человека, экономической и социальной справедливости, а также экологической безопасности.

Рекомендации ЮНЕСКО содержат достаточно гибкие определения систем ИИ, жизненного цикла системы ИИ, а также этических аспектов систем ИИ. По задумке авторов, подобный подход должен привести к долгосрочному применению данного документа без необходимости его регулярного пересмотра. Данный документ обращает внимание на то, что системы ИИ должны использоваться исключительно в мирных целях, во благо как отдельного человека, так и всего человечества, а также на пользу окружающей среде. Помимо этого, авторы подразумевают коллективную ответственность мирового сообщества при использовании систем ИИ.

В Рекомендациях по этике искусственного интеллекта авторы выделяют четыре ценностные опоры, на которых должна строиться вся работа в области систем ИИ:

– **Уважение, защита и поощрение прав человека и основных свобод и человеческого достоинства.** Помимо традиционных отсылок к принципу уважения прав человека, защите от дискриминации, человеческого достоинства и гендерного равенства, в данном документе обращается внимание на то, что использование систем ИИ не должно приводить к обезличиванию человека, к физической или психической зависимости от систем. А все возможные ограничения должны четко соотноситься с международными обязательствами государств в области защиты прав человека.

– **Благополучие окружающей среды и экосистем.** На протяжении всего жизненного цикла системы ИИ должны соответствовать нормам и стандартам в области охраны окружающей среды, чтобы обеспечить ее сохранность на благо будущих поколений и соотноситься с целями устойчивого развития.

– **Обеспечение разнообразия и инклюзивности.** Авторы акцентируют внимание на том, что доступ к системам ИИ должны иметь все категории лиц вне зависимости от различных факторов. При этом подчеркивается, что не должна ущемляться возможность человека выбирать предпочтительный для него образ жизни и убеждения, а также обращаться к использованию систем ИИ лишь факультативно, определяя параметры такого использования самостоятельно. А также для достижения данного аспекта работы с системами ИИ необходимо преодолеть цифровое неравенство, в том числе ликвидировав дефицит технической инфраструктуры.

– **Жизнь в таких сообществах, которые отвечают критериям мира, справедливости и взаимосвязи.** Все участники деятельности, которая так или иначе связана с использованием или созданием искусственного интеллекта, обязаны опираться на морально-этические установки, принципы и стандарты, а также активно пропагандировать и мотивировать общество создавать мирные, справедливые условия для того, чтобы обеспечить максимальное благополучие в условиях взаимозависимого мира, поощряя взаимосвязь всех живых существ между собой и окружающей средой, учитывая культурное многообразие.

«Рекомендации ЮНЕСКО в очередной раз обращают внимание мирового сообщества на необходимость использования безопасных и надежных систем ИИ с учетом соблюдения прав человека без какой бы то ни было дискриминации. Достоинство человека и подконтрольность систем ИИ человеку являются краеугольным камнем всех рекомендаций и не слишком отличают Рекомендации ЮНЕСКО, например, от принципов ОЭСР. Однако, что делает Рекомендацию исключительно применимой, так это ее обширные области политических действий, которые позволяют директивным органам претворять основные ценности и принципы в жизнь в отношении управления данными, окружающей среды и экосистем, гендера, образования и научных исследований, здравоохранения и социального благополучия, среди многих других сфер [6]».

Среди юридически необязательных актов в сфере искусственного интеллекта можно назвать и технические регламенты. Подобные стандарты разрабатывает Международный Союз Электросвязи, Международная организация по стандартизации и Международная электротехническая комиссия. Эти организации занимаются вопросами унификации технических стандартов для работы с системами ИИ [1]. Разрабатываемые ими нормы воплощают опыт многих экспертов из разных стран, но не вызывают обязательств со стороны государств по имплементации данных норм. Тем не менее роль технических стандартов не следует недооценивать, так как техническое единообразие будет способствовать ликвидации цифрового неравенства.

На сегодняшний день основным юридически обязательным документом в области ИИ является Регламент Европейского Союза, который устанавливает гармонизированные правила для всех 27 государств-членов. Этот Регламент не только определяет категории систем ИИ, но и устанавливает конкретные обязательства для разработчиков, а также систему штрафов за их несоблюдение. Это свидетельствует о том, что международное правовое регулирование начинает

принимать более формализованный и обязательный характер, что является важным шагом к обеспечению безопасного использования технологий.

Тем не менее большинство существующих документов, таких как Окинавская Хартия, остаются декларативными и не имеют юридической силы. Они служат основой для обсуждений и анализа правового регулирования информационных технологий, но не создают обязательств для национальных правительств. Это подчеркивает необходимость дальнейших усилий по разработке международных стандартов, которые могли бы гармонизировать подходы к регулированию ИИ между различными странами.

Кроме того, важность этических принципов в разработке и применении технологий ИИ не может быть недооценена. Эти принципы должны лежать в основе всех инициатив, направленных на создание безопасных и эффективных систем ИИ, которые будут служить интересам как отдельных людей, так и всего человечества. Международное сотрудничество в этой области является ключевым для достижения устойчивого и безопасного развития технологий.

**Заключение.** Таким образом, можно сделать вывод, что международно-правовое регулирование систем ИИ находится на стадии активного развития. Оно требует дальнейших обсуждений и согласований между странами и международными организациями. Важно, чтобы все заинтересованные стороны продолжали работать над созданием эффективных правовых рамок, которые будут способствовать как развитию технологий, так и защите прав человека в условиях их использования.

### Список литературы

1. Айтекова, Д. Г. Правовое регулирование искусственного интеллекта в нормотворческой деятельности международных организаций и европейского союза // Уральский журнал правовых исследований. – 2023. – № 1(22). – С. 3–12.
2. Анненкова И. В., Залоило М. В. Новая культура коммуникаций в условиях цифровой и социокультурной глобализации: право, медиа и национальная идентичность // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 3. С. 140–155.
3. Бочков С. И., Макаренко Г. И., Федичев А. В. Об Окинавской хартии глобального информационного общества и задачах развития российских систем коммуникации // Правовая информатика. – 2018. – № 1. – URL: <https://cyberleninka.ru/article/n/ob-okinavskoy-hartii-globalnogo-informatsionnogo-obschestva-i-zadachah-razvitiya-rossiyskih-sistem-kommunikatsii>
4. Ватян А. С., Гусарова Н. Ф., Добренко Н. В. Системы искусственного интеллекта. – СПб.: Университет ИТМО, 2022 – 186 с.
5. ГОСТ Р 59277-2020 Классификации систем искусственного интеллекта: дата введения 2020-12-23. – Москва: Стандартинформ, 2020. – 16 с.
6. Данельян А. А. Правовое регулирование технологий искусственного интеллекта в Российской Федерации // Электронное сетевое издание «Международный правовой курьер». – 2023. – № 53. – С. 6–9.

7. Имзалиева М. Р., Тризно Т. А., Говердовская Т. В., Дахина А. А. Искусственный интеллект: цели и ориентиры. – Астрахань: Сорокин Р. В., 2024.
8. Марченко А. Ю. Правовой анализ новейшего законодательства ЕС о применении технологий искусственного интеллекта: дис. канд. юрид. наук: 12.00.10 / МГИМО. – М., 2022. – 208 с.
9. Национальная стратегия развития ИИ на период до 2030 года утверждена Указом Президента РФ от 10.10.2019 № 490. / Национальный центр развития искусственного интеллекта при Правительстве Российской Федерации [Электронный ресурс] // Искусственный интеллект РФ: [сайт]. – URL: <https://ai.gov.ru/national-strategy/>
10. Право и бизнес: правовое пространство для развития бизнеса в России / отв. ред. С. Д. Могилевский, Ю. Г. Лескова, С. А. Карелина, В. Д. Рузанова, О. В. Шмалый, О. А. Золотова, О. В. Сушкова. В 4 т. – Т. 3. – М.: ООО «Проспект», 2020. – 368 с.
11. Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции (г. Казань, 22 сентября 2023 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 6. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – 476 с.
12. Solum L. Legal Personhood for Artificial Intelligences. North Carolina Law Review. – 1992. – April. [Online]. – URL: <http://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=3447&context=nclr>

**С. А. Дятлов,**  
доктор экономических наук,  
профессор, академик РАЕН,  
Санкт-Петербургский государственный  
экономический университет

## **ЭНТРОПИЙНО-СИНЕРГИЙНАЯ КОНЦЕПЦИЯ КЛАССИФИКАЦИИ ВИДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В НЕЙРО-ЦИФРОВОЙ ЭКОНОМИКЕ**

**Аннотация.** Статья посвящена исследованию теоретических подходов к классификации основных видов искусственного интеллекта. Введены в научный оборот понятия «энтропийные и синергийные экосистемы искусственного интеллекта». Обосновано положение о необходимости и важности решения проблемы признания правосубъектности искусственного интеллекта и определения меры его ответственности. Впервые предложен и сформулирован авторский методологический подход к разработке современной концепции классификации видов искусственного интеллекта на основе энтропийно-синергийного управленческого принципа.

**Ключевые слова:** энтропия, искусственный интеллект, цифровая экономика, энтропийно-синергийный управленческий принцип, классификация

## ENTROPY-SYNERGY CONCEPT OF CLASSIFICATION OF TYPES OF ARTIFICIAL INTELLIGENCE IN THE NEURO-DIGITALECONOMY

**Abstract.** The article is devoted to the study of theoretical approaches to the classification of the main types of artificial intelligence. The concepts of "entropic and synergistic ecosystems of artificial intelligence" have been introduced into scientific circulation. The position on the necessity and importance of solving the problem of recognizing the legal personality of artificial intelligence and determining the measure of its responsibility is substantiated. For the first time, the author's methodological approach to the development of a modern concept of classification of types of artificial intelligence based on the entropy-synergy management principle is proposed and formulated.

**Keywords:** entropy, artificial intelligence, digital economy, entropy-synergy management principle, classification

**Введение.** В XXI веке происходит глубинное переформатирование всей системы международных отношений на всех уровнях и во всех сферах экономики и общественной жизни [4]. Сегодня главными факторами цифровой трансформации российской и мировой экономики являются формирующийся Нейронет, новый человеческий интеллект с развитыми нейро-цифровыми способностями и компетенциями, искусственный самообучающийся интеллект (ИИ), нейронные сети, нанобиотехнологии и квантовые компьютеры.

**Основная часть.** Существует множество определений искусственного интеллекта в мировой и российской научной литературе. ИИ обычно определяют как технологию или математический алгоритм. На наш взгляд, давая современное определение ИИ нужно говорить обязательно об управлении, о правосубъектности, о противоречивом взаимодействии естественного человеческого и искусственного интеллектов посредством социо-нейроморфных интерфейсов и сервисов, а также осуществлять анализ последствий за принимаемые ими управленческие решения. Сегодня перед российской и мировой наукой противоречивой практикой сегодняшнего дня поставлена насущная задача разработать новый концептуальный теоретический подход к определению и классификации основных видов ИИ.

Сегодня наиболее известные виды ИИ: «слабый искусственный интеллект», «ограниченный искусственный интеллект», «сильный ИИ». Сильный искусственный интеллект имеет несколько подвидов: генеративный ИИ, гибридный ИИ, общий ИИ. Гибридный искусственный интеллект (Artificial Gibrud Intelligence) представляет собой нейросетевую модель человеко-машинного интеллекта с социо-нейроморфными сервисами и интерфейсами.

Следует отдельно выделить такой вид ИИ, который будет создан и использоваться в нейро-цифровой экономике – квантовый нейросетевой искусственный суперинтеллект. Нейросетевой искусственный суперинтеллект (Neural Network Artificial SuperIntelligence), основывается на использовании био-квантовых нейросетевых технологий, по своим возможностям превосходит возможности

человека и коллективный человеческий интеллект [2] и играет главную, решающую роль в принятии управленческих решений во всех сферах экономики и жизни будущего человеческого общества.

Сегодня происходит переход от технологий слабого ИИ к сильному гибриднему ИИ, который включает в себя нейросетевую трансформацию государственных правовых и экономических систем, а также социальных сетей на основе квантовых нейронных сетей и социо-нейроморфных сервисов.

Генеративный четвертого и пятого поколений (в перспективе – сильный, общий ИИ) активно и широко используется во многих странах во всех отраслях экономики, государственном управлении, обороне и сферах общественной жизни. Однако проблема его регулирования, признания правосубъектности и юридического статуса ИИ, результатов его функционирования, прав и ответственности за принимаемые решения является пока нерешенной в концептуально-теоретическом и практически-прикладном плане [5]. Человечество, чтобы избежать возможных негативных последствий для своего существования, должно осуществлять постоянный контроль за функционированием и влиянием на принятие решений ИИ [1].

На наш взгляд, следует поставить и найти ответ на вопрос: насколько можно доверять решениям, которые принимает сильный ИИ (в перспективе – нейросетевой искусственный суперинтеллект) в различных сферах экономики и общественной жизни. Масштабы и степень развития ИИ должны соответствовать критериям целесообразности, оптимальности, эффективности, безопасности, правовым и нравственно-этическим нормам, установленным человеческим обществом.

Широкое использование экосистем сильного ИИ трансформирует процессы принятия управленческих решений во всех отраслях экономики и сферах общественной жизни в последние годы. По мнению исследователей из Массачусетского технологического института Э. Бриньольфссона и Э. Макафи, руководители, которые используют ИИ, вытеснят тех, кто не использует его [6].

В рамках развиваемой нами субстанционально-информационной концепции общественного развития разнообразные социальные, правовые, экономические явления и процессы, включая деньги, право, управление, искусственный интеллект и др., имеют субстанционально-информационную природу. Когда речь идет об информации как о субстанции социально-экономических явлений, то имеется в виду, прежде всего, выявление имманентно присущей всем разнообразным общественным явлениям единой субстанциональной основы, которая реализуется как их общее субстанционально-информационное содержание. На наш взгляд, информация – это атрибутивная характеристика осуществляющегося, актуализирующегося через системные взаимодействия и отношения сознания, настоящего творческой личности человека (творческому субъекту управления).

Мы обосновываем положение об информационной упорядоченности социально-экономических и правовых систем. Мерой упорядоченности (роста синергии) или хаоса (роста энтропии) социально-экономической системы является информация в своих определенных количественных и качественных характеристиках.

Этот кратко сформулированный теоретико-методологический принцип определения и классификации видов ИИ мы называем энтропийно-синергическим управленческим принципом. В этой связи следует различать понятия «энтропийные и синергические экосистемы искусственного интеллекта».

В соответствии с этим принципом, качественные и количественные характеристики того или иного вида ИИ должны быть определены в зависимости от меры организованности и сложности параметров формируемой экосистемы «искусственный интеллект – естественный человеческий интеллект» и состояния ее энтропийно-синергического баланса. Классификация основных видов ИИ следует осуществлять в соответствии с энтропийно-синергическим критерием: использование того или иного вида ИИ ведет к росту энтропии (хаоса), снижению меры организованности, сложности, информационной емкости и энергоресурсного потенциала общественно-правовой экосистемы или ведет к снижению энтропии, росту меры организованности (порядка), сложности, информационной емкости и энерго-ресурсного потенциала данной системы.

Данное фундаментальное методологическое положение нами концептуально формулируется впервые в российской и мировой научной литературе. Более подробное обоснование этого принципа классификации ИИ будет дано нами в дальнейших работах.

**Заключение.** Сегодня перед российской и мировой наукой стоит актуальная задача обосновать и разработать современную классификацию различных видов искусственного интеллекта [3], а также институционально-правовых основ регулирования и контроля за их эффективным использованием.

### Список литературы

1. Бабкин А. В., Федоров А. А., Либерман И. В., Клачек П. М. Индустрия 5.0: понятие, формирование и развитие // Экономика промышленности. – 2021. – Т. 14, № 4. – С. 375–395.
2. Дятлов С. А. Искусственный интеллект как институт развития цифровой нейросетевой экономики // Известия Санкт-Петербургского государственного экономического университета. – 2021. – № 2(128). – С. 25–29.
3. Дятлов С. А. Трансформация российской и экономических систем в условиях усиления полифункциональной гиперконкуренции. – СПб.: Издательство: СПбГЭУ, 2023. – 158 с.
4. Социально-экономическая трансформация хозяйственной системы России. Коллективная монография. – Санкт-Петербург, 1997.
5. Черногор Н. Н., Емельянов А. С., Залоило М. В. Трансформация идейной основы юридической ответственности: между архаикой и постмодерном // Вопросы истории. – 2021. – № 11(2). – С. 248–259.
6. Brynjolfsson E., McAfee A. The second machine age: Work, progress, and prosperity in a time of brilliant technologies. – W.W. Norton&Company, 2014.

**А. А. Жариков,**  
кандидат юридических наук, доцент,  
Московский государственный юридический университет  
имени О. Е. Кутафина (МГЮА),  
Северо-Западный институт

## **ВОПРОСЫ МЕТОДОЛОГИИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЦИФРОВОЙ ЭКОНОМИКЕ**

**Аннотация.** В статье рассматриваются подходы к правовому регулированию искусственного интеллекта и технологий искусственного интеллекта в условиях цифровой экономики. На основе сравнительного анализа российских источников права определены реальные и перспективные приемы воздействия права на общественные отношения в данной сфере. Особое внимание обращено на содержание приемов регулирования искусственного интеллекта в цифровой экономике и состояние безопасности цифровой экономики. Сделан вывод о превентивных мерах, устанавливающих пределы свободы искусственного интеллекта.

**Ключевые слова:** искусственный интеллект, робототехническое устройство, решение искусственного интеллекта, приемы правового регулирования, цифровая экономика, рациональность, цифровая безопасность

## **ISSUES OF METHODOLOGY OF LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE IN THE DIGITAL ECONOMY**

**Abstract.** The article discusses the features of the legal regulation of artificial intelligence and artificial intelligence technologies in the digital economy. On the basis of a comparative analysis of Russian sources of law, real and promising methods of influencing law on public relations in this area have been identified. Special attention is paid to the content of artificial intelligence regulation techniques in the digital economy and the state of security of the digital economy. The conclusion is made about preventive measures that set limits to the freedom of artificial intelligence.

**Keywords:** artificial intelligence, robotic device, artificial intelligence solution, legal regulation techniques, digital economy, rationality, digital security

Безусловно, искусственный интеллект представляет собой комплексное явление. Согласно ст. 2 Закона о внедрении искусственного интеллекта в Москве [2] искусственный интеллект рассматривается в виде совокупности технологических подходов, воспроизводящих человеческие мыслительные способности, в том числе самостоятельное обучение и нахождение требуемых результатов без предварительно установленных схем.

По сути, искусственный интеллект носит нематериальный характер в виде различных идеальных конструкций, но для обеспечения его охраноспособности в смысле статьи 1225 ГК РФ он предполагает формальную объективацию. Фактически следует разграничивать идеальный искусственный интеллект от материального робототехнического устройства. Искусственный интеллект служит базой

робототехнических устройств. Приобретение вещного права собственности на робототехническое устройство не влечет приобретения интеллектуальных прав на искусственный интеллект, воплощенный в робототехническом устройстве. Таким образом данное устройство служит материальным носителем цифровой технологии искусственного интеллекта.

Выделение общеотраслевых и отраслевых задач, решение которых предполагается с помощью принятия нормативных правовых актов, является существенной стороной Концепции. Общеотраслевые правовые задачи в данной сфере технологий искусственного интеллекта касаются режимов ответственности, оборота данных, экспорта, страхования, терминологии, обеспечения безопасности, правотворчества и правоприменения, квалификация в качестве товара, технического регулирования, интеллектуальных прав. Выделение общеотраслевых и отраслевых задач правового регулирования технологий искусственного интеллекта свидетельствует об их комплексности и системности [6].

Цифровая экономика России как сложная система возможна на основе координации с помощью саморазвивающегося искусственного интеллекта. Экономика требует быстрого и успешного внедрения эффективных инноваций, что предопределяет использование искусственного интеллекта как ключевого элемента цифровой экономики.

Экономика носит во многом субъективный характер, обусловленный ролью компетентного субъекта в ходе принятия управленческих решений, в том числе в области инновационной деятельности. Как известно история экономического развития отражает историю инноваций. Решения об инновациях зависят от формулируемых целей экономики, нередко с решающим влиянием личностного фактора. Одни открытия и изобретения в кратчайшие сроки становились инновациями, а иные не получали развития и предавались забвению, несмотря на их существенное значение. Очевидно, что искусственный интеллект в цифровой экономике беспристрастен в принимаемых решениях. Существующие общественные системы характеризуются решающей ролью наделенных властью лиц, обладающих разной научно-теоретической и практической подготовкой, отражающейся в рациональности при принятии современных политико-экономических решений.

Внедрение искусственного интеллекта для управления экономическими процессами в цифровой экономике должно исключить принятие управленческих решений, отклоняющихся от рациональности. Но взгляды ученых на использование искусственного интеллекта неоднозначны. Существует авторитетная точка зрения о возможности усилить экономическую эффективность и стимулировать процессы инновации, полагающая «глубинное обучение» наиболее перспективным аспектом реализации искусственного интеллекта в инновационной сфере. В ряду ученых, внесших вклад в развитие искусственного интеллекта, укажем создавших в 1956 г. первую программу машинного интеллекта Аллена Ньюэлла и Герберта А. Саймона, и того, кто, ввел в научный оборот термин искусственный интеллект – Джона Маккарти.

Фундаментальная наука обогатилась многими прорывными открытиями в информационной сфере благодаря такому лидирующему центру развития искус-

ственного интеллекта в мире как Агентство перспективных исследовательских проектов Министерства обороны США (DARPA) [7, С. 122–123].

Создается искусственный интеллект, действующий с учетом четвертой оси измерения – времени, помогающий нейронной сети использовать свои внутренние знания реальном времени. Время обуславливает актуальность знаний и информации, используемой системой [8, С.25–28].

В то же время многие известные в мире ученые относятся к противникам искусственного интеллекта. Сошлемся на предупреждение людям Земли об опасности искусственного интеллекта, сформулированное в январе 2015 г. в открытом письме «Института будущего жизни» (Future of Life Institute), подписанном Стивеном Хокингом, Илоном Маском и др. Подобное обращение от имени института, предназначенного для руководства «технологиями трансформации» во имя жизни и предотвращения экстремальных всеобъемлющих рисков, было повторено в марте 2023 г., а в настоящее время в данном институте, разрабатывается проект закона Европейского Союза об искусственном интеллекте.

Значительное влияние в теоретическое развитие искусственного интеллекта внесли и российские исследователи. Следует отметить, например, научную монографию в области информационно-коммуникационных технологий Л. Е. Варшавского [9], и актуализацию в ней данных технологий в перспективном экономическом развитии. Автор монографии обосновывает вывод об отсутствии абсолютной гарантии точности принимаемых технологиями искусственного интеллекта решений, подчеркивая сложность выявления допущенных ошибок. Имеющиеся данные свидетельствуют о значительном повышении правильности решений искусственного интеллекта, однако не исключен риск преодоления искусственным интеллектом контроля за принимаемыми им решениями, которые испытывают влияние аналогичных человеческим рациональных и иррациональных факторов, отраженных в цифровой форме. Отмечается машинная интерпретация таких факторов в виде убеждения о наличии информации, желания принятия результативного решения, намерения осуществления этого желания, формируемого в условиях складывающихся обстоятельств. Кроме того, доверие выступает как обобщающим фактором подобной цифровой трансформации, так и корректирующим средством для обработки других названных факторов, обеспечивая обратную связь в управленческой системе. Схема выработки решений может использовать идеи, предложенные Гербертом А. Саймоном, Мэтью Рабином в теории ограниченной рациональности, а также основополагающие начала теории Джерома Б. Виснера об установлении равновесия. Вариантный прогноз относительно соответствующих процессов составляет основу управленческого решения, и далее сопровождается их верификацией и сопоставлением. Современная мировая практика свидетельствует, что прогнозирование и стратегическое планирование – это неотъемлемая часть экономической деятельности, тем более возрастает роль внедрения прогнозирования, использующего машинное обучение в цифровой экономике.

Очевидно, что, несмотря на общественные протесты искусственный интеллект, приобретает все большую роль в деятельности человечества, все более увеличивающийся объем информации затрудняет его освоение естественным че-

ловеческим интеллектом. Более того играет роль и фактор времени, когда ускорение хозяйственно-технологических событий предполагает и неуклонное ускорение их управлением, возможное лишь благодаря принятию решений искусственным интеллектом.

Особое значение в этой связи имеет состояние безопасности цифровой экономики. Кульминацией протеста в отношении искусственного интеллекта выступает сомнение в надежности контроля за функционированием искусственного интеллекта. Угрозу преодоления искусственным интеллектом человеческого контроля видит Илон Маск в наличии возможности свободного принятия решения искусственным интеллектом. И даже больше того, опасно, когда искусственный интеллект начинает мыслить вопреки интересам человека, это должно быть изначально недопустимо [10].

**Заключение.** В виде превентивных мер предлагается сужение сфер деятельности управляющего искусственного интеллекта, установление пределов свободы в вопросах, не относящихся к его сфере деятельности. Требуется разработка совокупности мер контроля и обнаружения, не санкционированного поведения искусственного интеллекта. Необходимо, чтобы искусственный интеллект перед допуском к принятию решений был всесторонне проверен как на теоретическом, так и на практическом уровне.

Важен при этом суверенитет данных, представляет собой развитие национального суверенитета, неразрывно связанного с обеспечением национальной безопасности на основе контроля за передачей и хранением данных, защиты персональных данных. В цифровой экономике данные составляют важнейшую ценность, оборот данных связан с рисками их конфиденциальности. В настоящий период в правовой системе Российской Федерации осуществляются меры по укреплению суверенитета данных в информационном пространстве.

### Список литературы

1. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_335184/](https://www.consultant.ru/document/cons_doc_LAW_335184/)
2. 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 «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_351127/](https://www.consultant.ru/document/cons_doc_LAW_351127/)
3. Василевская Л. Ю., Подузова Е. Б. Цифровизация гражданского оборота: «искусственный интеллект» и технологии «искусственного интеллекта» в механизме договорного регулирования (цивилистическое исследование) : монография : в 5 т. Т.IV / отв. ред. Л. Ю. Василевская. – М.: Проспект, 2022.

4. Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_358738/](https://www.consultant.ru/document/cons_doc_LAW_358738/)
5. Распоряжение Правительства Российской Федерации от 19 августа 2020 г. № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_360681/](https://www.consultant.ru/document/cons_doc_LAW_360681/)
6. Кутейников Д. Л., Ижаев О. А., Зенин С. С., Лебедев В. А. Ключевые подходы к правовому регулированию использования систем искусственного интеллекта // Вестник Тюменского государственного университета. Социальноэкономические и правовые исследования. – 2022. – Т.8. – № 1 (29). – С. 209–232.
7. DARPA и наука Третьего рейха : оборонные исследования США и Германии / Под общ. ред. А.Е. Суворова. – М.: ТЕХНОСФЕРА, 2020. – С. 122– 123.
8. Егорова Н. Е., Торжевский К. А. Методологические основы принятия стратегических решений. Секция 1. «Теоретические проблемы стратегического планирования на микроэкономическом уровне». Стратегическое планирование и развитие предприятий: материалы XXIII Всероссийского симпозиума. Москва, 12–13 апреля 2022 г. / под ред. чл.-корр. РАН Г. Б. Клейнера. М.: ЦЭМИ РАН, 2022. – С. 25–28.
9. Варшавский Л. Е. Социально-экономические проблемы развития информационно-коммуникационных технологий (ИКТ): монография. – М.: ЦЭМИ РАН, 2022.
10. Самбунова Т. Методологические вопросы анализа цифровой экономики [Электронный ресурс] // URL: <https://delyagin.ru/articles/191-materialy-mgd/110905-metodologicheskie-voprosy-analiza-tsifrovoy-jekonomiki>

И. Г. Ильин,

аспирант,

Санкт-Петербургский государственный университет

## СОЗДАНИЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ И ИХ ВЛИЯНИЕ НА РЕАЛИЗАЦИЮ И ЗАЩИТУ КОНСТИТУЦИОННО ГАРАНТИРОВАННЫХ ПРАВ

**Аннотация.** Статья посвящена исследованию некоторых правовых аспектов создания больших языковых моделей в контексте цифрового неравенства и языковой дискриминации. В результате анализа было установлено, что применительно к большим языковым моделям цифровое неравенство возникает из-за неравномерного уровня цифровизации языков и проявляется в ограниченном доступе к технологии обработки естественного языка.

**Ключевые слова:** право, большие языковые модели, языковая дискриминация, цифровые технологии, цифровое неравенство, искусственный интеллект, технология обработки естественного языка

## CREATION OF LARGE LANGUAGE MODELS AND THEIR IMPACT ON THE REALIZATION AND PROTECTION OF CONSTITUTIONALLY GUARANTEED RIGHTS

**Abstract.** The lecture notes focus on the results of research examining the constitutional and legal aspects of large language model development in the context of the digital divide and linguistic discrimination. The study concludes that, in relation to the development of large language models, the digital divide arises due to the uneven digitalization of languages, resulting in limited access to natural language processing technology.

**Keywords:** law, large language models, language discrimination, digital technologies, digital divide, artificial intelligence, natural language processing technology

Большие языковые модели (англ. Large Language Models, LLM) – это генеративные модели искусственного интеллекта используемые в технологии обработки естественного языка (англ. Natural language processing, NLP). Наличие таких моделей позволяет компьютеру эффективно обрабатывать текстовые данные, демонстрируя способность к «пониманию» текста на глубоком уровне, создавать связные и контекстуально релевантные ответы на запросы, осуществлять перевод текста между языками, а также генерировать текст, который соответствует определенным стилевым и содержательным требованиям [18. С. 24–34].

Большие языковые модели обучаются на обширных массивах языковых данных. Структура и репрезентативность, их объем и формат определяют процесс обучения и точность понимания контекста [21. С. 36–56], а наличие дефектов или недостаточность данных может приводить к некорректной работе модели и в целом препятствовать развитию технологии [20. С. 260]. Параметры обучающих данных будут зависеть от уровня цифровизации конкретного языка.

Цифровизация языка в широком смысле представляет собой процесс преобразования данных в соответствующие лингвистические корпуса. Для этого применяются текстовые данные (такие как файлы, транскрипции, аннотации), речевые данные (например, аудиозаписи, фонетические и интонационные аннотации) и мультимодальные данные, которые объединяют несколько типов информации, например видео с текстом, изображения с текстом и т. д. [12. С. 291]. Процесс цифровизации языка выполняет не только техническую функцию, способствуя созданию больших языковых моделей и развитию технологий обработки естественного языка, но и играет важную общественно-социальную роль, содействуя сохранению национальной и культурной идентичности [28. С. 126–139]. Например, цифровизация миноритарных языков может значительно помочь в сохранении культурного наследия малых народов.

Разные языки имеют различный уровень цифровизации, что может быть обусловлено рядом факторов, включая экономические, технические и правовые. Экономические факторы связаны с тем, что языки имеют разный экономический потенциал [6. С. 173; 32. С. 1–8], а процесс цифровизации требует значительных ресурсов, в том числе временных, финансовых и т. д. К техническим факторам может отнести ошибки при сборе данных, недостатки в конструкции корпусов и

ограничения существующих наборов данных, ошибки в метаданных и т. д. [39. С. 193–204; 14. С. 5751–5767; 30. С. 26–37]. Правовые факторы связаны с существованием нормативных барьеров на доступ к обучающим данным, связанных с необходимостью соблюдения соответствующего правового режима при использовании данных [21. С. 36–56; 1. С. 123–140; 22. С. 99–123; 23. С. 367–376; 24. С. 17–27; 25. С. 2–26]. Преодоление таких барьеров требует мер как на концептуальном уровне – устранения нормативных ограничений с учетом баланса частных и публичных интересов, так и на практическом – создания условий для обмена и распространения языковых данных. Среди таких мер можно выделить развитие института повторного использования данных, накопленных в государственных информационных системах, а также привлечение высших учебных заведений к созданию лингвистических корпусов и цифровизации языка.

Невозможность создания полноценной языковой модели для определенных языков или диалектов делает многие цифровые продукты недоступными для их носителей либо ухудшает их работу по сравнению с теми, что доступны для носителей языков с высоким уровнем цифровизации. Это приводит к цифровому неравенству, когда доступ к технологии распределяется неравномерно среди языковых сообществ, тем самым создавая риск дискриминации.

Национальная стратегия развития искусственного интеллекта на период до 2030 года подчеркивает, что защита прав и свобод человека является одним из основных принципов развития и использования технологии искусственного интеллекта, а «недискриминация» выделена в качестве одного из основного принципа развития нормативно-правового регулирования общественных отношений, связанных с развитием и использованием технологий искусственного интеллекта.

Статья 2 Всеобщей декларации прав человека (1948) устанавливает запрет на дискриминацию, в том числе, по языковому признаку. Аналогичное положение содержится и в статье 1 (3) Устава ООН, а также находит свое отражение в пункте 2 статьи 19 Конституции РФ, согласно которому государство гарантирует равенство прав и свобод человека и гражданина независимо от языка. В контексте создания больших языковых моделей представляется целесообразным толковать это понятие максимально широко, рассматривая языковую дискриминацию не только как необоснованные различия или ограничения, которые могут снижать или исключать возможность реализации прав на основе языковой принадлежности, но и как действия, которые могут препятствовать сохранению или развитию языков меньшинств.

Комитет ООН по правам человека неоднократно рассматривал проблему языковой дискриминации, однако его судебная практика недостаточно развита и не всегда обеспечивает надежной защиты языковых меньшинств [31. С. 27–56]. Например, дискриминация по признаку голоса часто остается незамеченной [7. С. 167–177], что может оказаться критичным при взаимодействии с технологией распознавания речи и голоса и связанных цифровых продуктов: систем интерактивного ответа и голосовых помощников. Анализ существующей практики позволяет выделить ряд ключевых критериев для определения языковой дискриминации. Во-первых, это численность носителей языка, поскольку степень дискриминации часто зависит от уровня распространенности языка в обществе

[29. С. 3–15]. Во-вторых, значимым критерием является уровень государственной поддержки многоязычия: активные государственные программы по обучению и использованию различных языков способствуют снижению риска языковой дискриминации [36. С. 39–53]. В-третьих, важен уровень использования языков меньшинств в общественной жизни, что также способствует более точной оценке случаев языковой дискриминации.

Однако, несмотря на возможность выделить критерии для оценки языковой дискриминации, правовая квалификация таких случаев в контексте цифровых технологий вызывает определенные трудности. Например, дискриминация в языковых моделях может быть вызвана как алгоритмической, так и человеческой предвзятостью. Алгоритмическая предвзятость возникает из-за искажений в данных, на которых обучается модель, в то время как человеческая предвзятость может проявляться на этапе разработки алгоритмов [5. С. 337–358]. Оба типа предвзятости могут существенно влиять на точность и справедливость принимаемых решений, что усугубляет социальное неравенство. Важно отметить, что данные формы предвзятости не всегда очевидны и могут проявляться на различных стадиях работы модели, что затрудняет их обнаружение и минимизацию. В связи с этим правовая квалификация таких ситуаций требует особого внимания, поскольку не всегда ясно, следует ли расценивать ошибки в языковых моделях как проявление дискриминации, и какие меры ответственности могут быть применимы к разработчикам и владельцам технологий.

### Список литературы

1. Ильин И. Г. Персональные данные в системах искусственного интеллекта: технология обработки естественного языка // *Journal of Digital Technologies and Law*. – 2024. – Т. 2, № 1. – С. 123–140.
2. Миронова М. В. Становление термина «языковая дискриминация» в современной социолингвистике // *New Language*. – New World. – New Thinking. – 2019. С. 555–558.
3. Мушаков В. Е. Конституционные права человека в контексте проблемы преодоления цифрового разрыва // *Вестник Санкт-Петербургского университета МВД России*. – 2022. – № 1(93). – С. 69–73.
4. Талапина Э. В. Обработка данных при помощи искусственного интеллекта и риски дискриминации // *Право. Журнал Высшей школы экономики*. – 2022. – № 1. – С. 4–27.
5. Харитонов Ю. С. Правовые средства обеспечения принципа прозрачности искусственного интеллекта // *Journal of Digital Technologies and Law*. – 2023. – Т. 1, № 2. – С. 337–358.
6. Alarcón A. A. The economics of language // *Catalan Sociolinguistics: State of the art and future challenges*. – 2022. – Т. 32. – С. 173.
7. Baugh J. Linguistic profiling across international geopolitical landscapes // *Dædalus*. – 2023. – Т. 152, № 3. – С. 167–177.
8. Bosco F. et al. Profiling technologies and fundamental rights and values: regulatory challenges and perspectives from European Data Protection Authorities // *Reforming European data protection law*. – 2015. – С. 3–33.

9. Browning M., Arrigo B. Stop and risk: Policing, data, and the digital age of discrimination // *American Journal of Criminal Justice*. 2021. T. 46, № 2. С. 298–316.
10. Chasalow K., Levy K. Representativeness in statistics, politics, and machine learning // *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*. – 2021. – С. 77–89.
11. Chilingaryan K., Meshkova I., Sheremetieva O. International legal protection of linguistic minorities // *International Journal of Psychosocial Rehabilitation*. – 2020. – T. 24, № 6. – С. 9750–9758.
12. Dash, N. S., & Arulmozi, S. History, features, and typology of language corpora. – Springer Singapore, 2018. – С. 1 – 291.
13. Devlin J. et al. Bert: Pre-training of deep bidirectional transformers for language understanding // *arXiv preprint arXiv:1810.04805*. – 2018.
14. Doğruöz A. S., Sitaram S., Yong Z. X. Representativeness as a forgotten lesson for multilingual and code-switched data collection and preparation // *arXiv preprint arXiv:2310.20470*. – 2023. – С. 5751–5767.
15. Drożdżowicz A., Peled Y. The complexities of linguistic discrimination // *Philosophical Psychology*. – 2024. – С. 1–24.
16. Egbert J, Biber D, Gray B. Approaches to Representativeness in Previous Corpus Linguistic Research. In: *Designing and Evaluating Language Corpora: A Practical Framework for Corpus Representativeness*. Cambridge University Press. – 2022. – С. 28–51.
17. Engel C., Linhardt L., Schubert M. Code is law: how COMPAS affects the way the judiciary handles the risk of recidivism // *Artificial Intelligence and Law*. – 2024. – С. 1–23.
18. Glauner P. Technical foundations of generative AI models. In: *Legal Tech – Zeitschrift für die digitale Anwendung des Nomos*. – С. 24–34.
19. Hacker P. A legal framework for AI training data—from first principles to the Artificial Intelligence Act // *Law, Innovation and Technology*. – 2021. – T. 13, № 2. – С. 257–301.
20. Hacker P. et al. Generative Discrimination: What Happens When Generative AI Exhibits Bias, and What Can Be Done About It // *arXiv preprint arXiv:2407.10329*. – 2024. – С. 1–51
21. Ilya, I. Progress in Natural Language Processing Technologies: Regulating Quality and Accessibility of Training Data // *Legal Issues in the digital Age*. – 2024. – № 2. – С. 36–56.
22. Ilya I. The Voice and Speech Processing within Language Technology Applications: Perspective of the Russian Data Protection Law // *Legal Issues in the digital Age*. – 2020. – № 1. – С. 99–123.
23. Ilin I. Legal Regime of the Language Resources in the Context of the European Language Technology Development // *Language and Technology Conference*. – Cham: Springer International Publishing, 2019. – С. 367–376;
24. Ilin I., Kelli A. The use of human voice and speech in language technologies: the EU and Russian intellectual property law perspectives // *Juridica Int'l*. – 2019. – T. 28. – С. 17–27.

25. Ilin, I., & Kelli, A. Natural Language, Legal Hurdles: Navigating the Complexities in Natural Language Processing Development and Application. *The Journal of the University of Latvia. Law.* – C. 2–26 (forthcoming 2024).
26. Ilin I., Dedova M. Academic Entrepreneurship in the Field of Language Resource Creation and Dissemination. *The ESU 2019 Conference and Doctoral Programme, Naples (Italy), 8–14 September 2019.* Ed. Angelo Riviezzo, Maria Rosaria Napolitano, Antonella Garofano. *Electronic Conference Proceedings.* – C. 193–200.
27. Jiang X. et al. Large Language Models in Healthcare Current Development and Future Directions // *Generative AI Research.* – 2023. № 2. – C.12
28. Kelli A. et al. Constitutional values as a basis for the limitation of copyright within the context of digitalisation of the estonian language // *Constitutional Values in Contemporary Legal Space II.* – 2017. – C. 126 – 139.
29. Kome D. Legal protection of linguistic minority under discrimination: the case of anglophone Cameroon. – 2023. – C. 3–15
30. Li X. et al. Corpuslm: Towards a unified language model on corpus for knowledge-intensive tasks // *Proceedings of the 47th International ACM SIGIR Conference on Research and Development in Information Retrieval.* – 2024. – C. 26–37.
31. Möller J. T. Case Law of the UN Human Rights Committee relevant to Members of Minorities and Peoples in the Arctic Region // *The Yearbook of Polar Law Online.* – 2011. – T. 3, № 1. – C. 27–56.
32. Monteith B. et al. Unleashing the Economic Potential of Large Language Models: The Case of Chinese Language Efficiency // *Authorea Preprints.* – 2023. – C. 1–8.
33. Morin S. L. AI Discrimination in Hiring // *Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology.* – IGI Global, 2024. – C. 64–74.
34. Orwat C. Algorithmic Discrimination From the Perspective of Human Dignity // *Social Inclusion.* – 2024. – T. 12. – C. 1–18.
35. Ozkul D. Artificial Intelligence and Ethnic, Religious, and Gender-Based Discrimination // *Social Inclusion.* – 2024. – T. 12. C. 1–3.
36. Page C. Academic language development and linguistic discrimination: Perspectives from internationally educated students // *Comparative and International Education.* – 2023. – T. 52, № 2. – C. 39–53.
37. Rogers S. E. Bridging the 21st century digital divide // *TechTrends.* – 2016. – T. 60, № 3. – C. 197–199.
38. Sohail A., Zhang L. Using large language models to facilitate academic work in psychological sciences. – 2024. – C. 2–21.
39. Solovyev V. D., Akhtyamova S. Linguistic Big Data: Problem of Purity and Representativeness // *DAMDID/RCDL.* – 2019. – C. 193–204.
40. Vaswani A. Attention is all you need // *Advances in Neural Information Processing Systems.* – 2017.
41. Yenduri G. et al. Generative pre-trained transformer: A comprehensive review on enabling technologies, potential applications, emerging challenges, and future directions // *arXiv preprint arXiv:2305.10435.* – 2023.

**А. А. Карцхия,**  
доктор юридических наук, профессор,  
Российский государственный университет нефти и газа  
(национальный исследовательский университет)  
имени И. М. Губкина

## ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В НОВОЙ ПАРАДИГМЕ

**Аннотация.** Переход общества к новой технологической основе через внедрение современных информационно-коммуникационных технологий может существенно преобразовать экономику и общественные отношения. Однако уникальные возможности передовых цифровых технологий, таких как искусственный интеллект, большие данные и облачные вычисления, несут в себе риски, способные поставить под угрозу общепринятые ценности. Эти новые цифровые возможности имеют глобальное значение и могут значительно изменить общественную жизнь. Поэтому особое внимание следует уделять вопросам ответственности и безопасности при использовании технологий искусственного интеллекта, а также защите прав и интересов людей, включая их персональные данные.

**Ключевые слова:** доверенный искусственный интеллект, интеллектуальная собственность, ответственность, безопасность искусственного интеллекта, угрозы и риски, связанные с технологией искусственного интеллекта, устойчивое развитие, интеллектуальная собственность, кибербезопасность

## ARTIFICIAL INTELLIGENCE TOWARDS A NEW PARADIGM

**Abstract.** The transition of society to a new technological basis through the introduction of modern information and communication technologies can significantly transform the economy and social relations. However, the unique capabilities of advanced digital technologies such as artificial intelligence, big data, and cloud computing carry risks that can compromise conventional values. These new digital opportunities are of global importance and can significantly change public life. Therefore, special attention should be paid to issues of responsibility and security when using artificial intelligence technologies, as well as the protection of people's rights and interests, including their personal data.

**Keywords:** trusted artificial intelligence, intellectual property, liability, artificial intelligence security, threats and risks of AI technology, sustainable development, intellectual property, cybersecurity

В настоящее время приобретает особое значение *современное понимание искусственного интеллекта*. Так, определение основано на концептуальном представлении об ИИ, подробно изложенном в книге С. Рассела и П. Норвига [1], где «искусственный интеллект представляет собой компьютерную систему, которая может для достижения заданного набора целей, определенных человеком, делать прогнозы, рекомендации или принимать решения, влияющие на ре-

альную или виртуальную среду. Системы искусственного интеллекта предназначены для работы с различным уровнем автономии».

Вместе в том по мере того как возможности искусственного интеллекта становятся все более мощными растущее использование систем искусственного интеллекта, по мнению аналитиков [2. С. 3–5], может привести к определенным изменениям ландшафта угроз, которые можно классифицировать следующим образом, разделив на три сферы безопасности:

- *цифровая безопасность*, характеризующаяся тем, что использование искусственного интеллекта позволяет существенно повысить эффективность проведения кибератак, что создаст новые угрозы с использованием уязвимостей человека виде фишинга, синтеза речи и образов (*deep fake*) или утечки данных.

- *физическая безопасность*, предполагающая использование беспилотных летательных (над- и подводных) аппаратов и других автоматизированных систем (в т. ч. автономных систем вооружения, рой микродронов и т. п.), а также атаки на киберфизические системы (на транспорте, в промышленности и др.) или критически важную инфраструктуру.

- *политическая безопасность*, при использовании искусственного интеллекта для сбора и анализа данных в целях целенаправленной пропаганды или манипулирование сознанием и общественным мнением путем вторжения в частную жизнь или анализа и манипулирования поведением, настроениями и убеждениями людей на основе имеющихся данных.

Современные базовые модели ИИ, лежащие в основе ChatGPT и подобных систем, работают во многом так же, как марковская модель. Но ChatGPT намного больше и сложнее, с миллиардами параметров, обучен на огромном объеме данных, по большей части общедоступного контента в Интернете. В этом огромном массиве текста, слова и предложения появляются в последовательностях с определенными зависимостями, что помогает модели ИИ понять, как разбить текст на статистические фрагменты, которые обладают некоторой предсказуемостью. ИИ изучает шаблоны таких блоков текста, используя эти знания, чтобы предложить определенное решение [11].

Появляются новые модели искусственного интеллекта – агентский искусственный интеллект, который является более гибкой системой, которая может обеспечить более высокую автоматизацию и производительность труда в определенных отраслях и помочь тем, кому не хватает цифровой грамотности. Агент искусственного интеллекта может взаимодействовать с приложениями или веб-сайтами, добавлять товары в корзину и оформлять заказ в соответствии с предварительно зарегистрированными предпочтениями и способами оплаты, заполнять и отправлять форму или отвечать на приглашения на мероприятия [3. С. 3].

В последние годы генеративный искусственный интеллект переживает стремительный рост, который сопровождается, в том числе, растущими проблемами охраноспособности результатов деятельности искусственного интеллекта в сфере интеллектуальной собственности. В настоящее время в разных странах активно идет процесс выработки правового режима авторства искусственного интеллекта и патентной защиты его технологий [4–7].

Быстрое развитие генеративного искусственного интеллекта, в частности, создало целый лабиринт новых проблем с авторским правом. Эти вопросы в первую очередь касаются способа обучения моделей искусственного интеллекта и того, являются ли результаты разработок этих моделей самостоятельным охраноспособным объектом, чтобы давать им право на защиту авторским правом. «Основной вопрос в сфере авторского права заключается в том, обладают ли произведения, созданные искусственным интеллектом, достаточно творческим началом, чтобы иметь право на защиту авторским правом. Одна из точек зрения заключается в том, что произведения, созданные с помощью текстовых подсказок и не требующие какого-либо дополнительного творческого вклада пользователя-человека, как в случае с генеративными инструментами искусственного интеллекта, не защищаются авторским правом, поскольку эти подсказки больше похожи на инструкции для художника, получившего заказ» [8. С. 7–9].

В этой ситуации возрастает значение комплексных исследований развития искусственного интеллекта, его новой парадигмы в т. ч. по правовым вопросам применения технологий искусственного интеллекта в цифровой экономике [9. С. 165; 10. С. 27–28].

Бурный рост цифровых технологий за последние годы привел к резкому увеличению интереса к искусственному интеллекту и другим передовым технологиям. Быстрая эволюция и практическое применение технологий искусственного интеллекта связаны с ожиданиями значительного увеличения производительности труда, стимулирования инноваций и предпринимательства, а также решения глобальных задач, включая социальные вызовы, такие как улучшение системы здравоохранения и борьба с изменением климата, что способствует достижению целей устойчивого развития.

В такой ситуации концепция доверенного (ответственного) искусственного интеллекта может стать базой для разработки универсальных международных рекомендаций по созданию и использованию технологий и моделей искусственного интеллекта. Это позволит сформировать правовые нормы в рамках национальных законодательств различных стран, основываясь на принципах защиты прав человека, конфиденциальности и безопасности данных, а также прозрачности, объяснимости, справедливости, подотчетности и безопасности искусственного интеллекта. Важным шагом на пути к достижению этой цели станет международная конвенция против использования информационно-коммуникационных технологий в преступных целях, проект которой был согласован специальным комитетом ООН в августе 2024 года.

Вместе с тем этот процесс порождает и новые угрозы и вызовы для человека, что служит особым фактором, который необходимо учитывать при стимулировании развития искусственного интеллекта.

Искусственный интеллект обладает потенциалом для решения наиболее сложных задач, стоящих перед человечеством. В этом контексте особенно важными становятся вопросы ответственности и надежности технологий искусственного интеллекта при их применении, а также гарантии защиты прав и интересов человека, включая защиту его персональных данных.

### Список литературы

1. Russell S., Norvig P. Artificial Intelligence: A Modern Approach / 3rd edition. – London: Pearson, 2009. [Электронный ресурс]. – URL: <http://aima.cs.berkeley.edu/>
2. Brundage M. [et al.] The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, 2018 [Электронный ресурс]. – URL: [https://www.eff.org/files/2018/02/20/malicious\\_ai\\_report\\_final.pdf](https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf)
3. Aggarwal, Rohit and Singh, Harpreet, Overcoming Limitations of Ai Agents: Integrating Tacit Knowledge Through Inferred Latent Themes (May 27, 2024). [Электронный ресурс]. – URL: <https://ssrn.com/abstract=4843878>
4. Юридическая концепция роботизации: монография / Н. В. Антонова, С. Б. Бальхаева, Ж. А. Гаунова и др.; отв. ред. Ю. А. Тихомиров, С. Б. Нанба. – М.: Проспект, 2019. – 240 с.
5. Карцхия А. А. Правовое регулирование и возможности современных биотехнологий // ИС. Промышленная собственность. – 2020. – № 8. – С. 33–46.
6. Рожкова М. А. Станет ли искусственный интеллект самостоятельным субъектом права? // Хозяйство и право. – 2021. – № 6. – С. 14–22.
7. Харитонов Ю. С., Савина В. С. Технология искусственного интеллекта и право: вызовы современности // Вестник Пермского университета. Юридические науки. – 2020. – Вып. 49. – С. 524–549. – DOI: 10.17072/1995-4190-2020-49-524-549
8. Hill M., Hackworth A. Copyright in the Age of AI, 2023. [Электронный ресурс]. – URL: <https://www.charlesrussellspeechlys.com/en/insights/quick-reads/102j7d1-copyright-in-the-age-of-ai/#page=1>
9. Доклад НИУ ВШЭ «Правовые аспекты использования искусственного интеллекта: актуальные проблемы и возможные решения» / отв. рук. В. Б. Наумов, С. А. Чеховская, А. Ю. Брагинцев, А. В. Майоров. – М.: Изд. ВШЭ, 2021.
10. Амелин Р. В., Чаннов С. Е. Эволюция права под воздействием цифровых технологий. Москва: НОРМА, 2023.
11. Zewe A. Explained: Generative AI. MIT News Publication Date: November 9, 2023. [Электронный ресурс]. – URL: <https://news.mit.edu/2023/explained-generative-ai-1109>

Д. С. Кийко,  
аспирант,  
Казанский инновационный университет  
имени В. Г. Тимирязова

## ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА О РОБОТОТЕХНИКЕ И ИСКУССТВЕННОМ ИНТЕЛЛЕКТЕ

**Аннотация.** В статье проводится анализ проблем и перспектив развития законодательства в сфере робототехники и искусственного интеллекта. Особое внимание уделяется определению правового статуса искусственного интеллекта, вопросам ответственности за его действия. Рассматриваются подходы к международному сотрудничеству и стандартизации, а также роль образования в подготовке специалистов, способных работать с технологическими и правовыми аспектами данной сферы. Подчеркивается необходимость создания комплексных законодательных норм, учитывающих междисциплинарный характер данной области. Исследование акцентирует внимание на необходимости системного подхода, который предполагает взаимодействие экспертов из различных областей, таких как юриспруденция, инженерия и общественные науки.

**Ключевые слова:** искусственный интеллект, робототехника, законодательство, ответственность, кибербезопасность, правовой статус, международное сотрудничество, стандартизация, защита данных

## PROBLEMS AND PROSPECTS FOR THE DEVELOPMENT OF LEGISLATION ON ROBOTICS AND ARTIFICIAL INTELLIGENCE

**Abstract.** The article analyses the problems and prospects for the development of legislation in the field of robotics and artificial intelligence, paying particular attention to the definition of the legal status of artificial intelligence, issues of responsibility for its actions. Approaches to international cooperation and standardization are considered, as well as the role of education in training specialists capable of dealing with the technological and legal aspects of this field. The study emphasizes the necessity for comprehensive legislation that considers the interdisciplinary nature of the field, and the importance of a systematic approach involving the interaction of experts from different fields, including law, engineering and the social sciences.

**Keywords:** artificial intelligence, robotics, legislation, responsibility, cybersecurity, legal status, international cooperation, standardization, data protection

Одним из ключевых вопросов, требующих решения, является определение правового статуса искусственного интеллекта. Необходимо четко установить, кто несет ответственность за действия роботов и интеллектуальных систем. Проблема заключается в том, что автономные системы принимают решения без непосредственного участия человека. Это затрудняет определение субъекта ответственности за возможные правонарушения. Кроме того, в настоящее время отсутствует единый подход к правовому регулированию систем искусственного

интеллекта. Как отмечает Райан Кало, профессор Вашингтонского университета, отсутствие единого мнения о правосубъектности искусственного интеллекта затрудняет разработку соответствующих законов. Он также подчеркивает важность комплексного подхода к регулированию, который должен учитывать как технологические, так и социальные аспекты. По его словам, право обычно предполагает разделение между людьми и инструментами. Сложность классификации роботов и тенденция рассматривать социальные технологии как людей могут нарушить это разделение и лежащие в его основе принципы [1. С. 513–564].

Говоря об ответственности, Е. Н. Агibalова предлагает применить комплексный подход, предполагающий различные уровни ответственности для различных роботов в зависимости от степени потенциальной опасности, которую они представляют для общества. В настоящее время искусственный интеллект обычно рассматривается как инструмент, находящийся в распоряжении человека, который является реальным нарушителем и исполнителем правонарушения [2. С. 21–24].

Для решения существующих проблем необходимо укреплять международное сотрудничество и разрабатывать единые стандарты. Представляется возможным говорить о том, что исследования Ника Бострома легли в основу формирования стратегий безопасного использования искусственного интеллекта. Он предлагает концепцию дифференцированного технологического прогресса, согласно которой общество должно замедлять развитие опасных и вредных технологий, особенно тех, которые увеличивают риск для человечества, и ускорять развитие полезных технологий, особенно тех, которые снижают риски, связанные с природными явлениями или другими технологиями. [3. С. 230].

Еще одним аспектом является разработка образовательных программ для специалистов в области искусственного интеллекта и права. Это необходимо для подготовки квалифицированных юристов, способных учитывать технические аспекты при разработке законодательных норм. В 2023 году в Гарвардском университете была запущена программа, которая объединяет изучение права и технологий. Она акцентирует внимание на новых задачах и перспективах для юридической сферы, связанных с развитием искусственного интеллекта. Это является примером подхода к подготовке специалистов в данной области. [4].

Еще одним возможным решением может стать формирование международных платформ для обсуждения вопросов, связанных с регулированием. В качестве иллюстрации можно привести проект «Альянс по управлению искусственным интеллектом», инициированный Всемирным экономическим форумом в 2023 году. Цель этого проекта заключается в обмене опытом и разработке рекомендаций для стран, внедряющих технологии искусственного интеллекта [5].

В настоящее время законодательство, регулирующее сферу робототехники и искусственного интеллекта, находится в стадии становления и не всегда соответствует вызовам современности, обусловленным стремительным технологическим прогрессом. Это создает потенциальные риски как для пользователей, так и для общества в целом. Для эффективного регулирования этой области необходимо учитывать ее междисциплинарный характер и привлекать специалистов из различных областей, таких как юриспруденция, инженерия, философия и граж-

данское общество. Исследования, проводимые учеными и экспертами в этой области, подчеркивают важность системного подхода, который позволит создать безопасные и эффективные условия для внедрения новых технологий. Оптимизация законодательства в области искусственного интеллекта и робототехники требует консолидации усилий научного сообщества, международного взаимодействия и активного участия общественности. Только такой подход позволит минимизировать потенциальные риски и использовать возможности этих технологий для повышения качества жизни.

### Список литературы

1. Calo R. Robotics and the Lessons of Cyberlaw // California Law Review. – 2015. – Vol. 103, No. 3. – Pp. 513–565.
2. Агibalова Е.Н. Юридическая ответственность при применении систем искусственного интеллекта // Государство, право и общество: вопросы теории и практики. – 2020. – С. 15–24.
3. Bostrom N. Superintelligence: Paths, Dangers, Strategies. – Oxford University Press, 2014. – 352 p.
4. Coyer C. Harvard Launches New Initiative to Better Understand – and Shape – the Future of AI // Legaltech news. 2023. – URL: <https://www.law.com/legaltechnews/2023/07/18/harvard-launches-new-initiative-to-better-understand-and-shape-the-future-of-ai/>
5. AI Governance Alliance // World Economic Forum. 2023. – URL: <https://initiatives.weforum.org/ai-governance-alliance/about>

Д. С. Кийко,

аспирант,

Казанский инновационный университет  
имени В. Г. Тимирязева

### ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ПРОИЗВОДСТВА И РАСПРОСТРАНЕНИЯ ВОЕННЫХ РОБОТОВ

**Аннотация.** В данной статье проводится анализ вопросов государственного регулирования создания и использования военных роботов и искусственного интеллекта в военных целях. В работе проводится исследование правовых, этических аспектов и вопросов безопасности, связанных с применением автономных систем. Автор рассматривает, как существующие пробелы в регулировании могут привести к увеличению рисков эскалации конфликтов и гонки вооружений.

**Ключевые слова:** военные роботы, искусственный интеллект, автономное оружие, международное гуманитарное право, этическое регулирование, государственная ответственность, гонка вооружений, человеческий контроль, глобальная безопасность

## STATE REGULATION OF THE PRODUCTION AND DISTRIBUTION OF MILITARY ROBOTS

**Abstract.** The article analyses the issues of state regulation of the creation and use of military robots and artificial intelligence for military purposes. It examines the legal, ethical and security issues associated with the use of autonomous systems. The author considers how existing gaps in regulation can lead to increased risks of conflict escalation and arms race.

**Keywords:** military robots, artificial intelligence, autonomous weapons, international humanitarian law, ethical regulation, state responsibility, arms race, human control, global security

Применение автономных военных роботов открывает новые перспективы в ведении военных действий. Беспилотные летательные аппараты и полностью автономные оружейные платформы предоставляют стратегические преимущества, учитывая высокую точность поражения целей и снижение риска для личного состава. Однако использование автономных военных роботов сопряжено с определенными рисками, такими как потенциальный ущерб гражданскому населению, проблемы с подотчетностью и определением их правосубъектности и возможность возникновения гонки вооружений. Для решения этих проблем необходим комплексный подход к регулированию, который позволит сбалансировать интересы национальной безопасности с этическими и правовыми аспектами.

Международное гуманитарное право (далее – МГП) представляет собой фундамент правовой системы, регулирующий вооруженные конфликты. Однако, как отмечают исследователи Кеннет Андерсон и Мэтью К. Ваксман в своей работе «Право и этика для роботов-солдат», существующие нормы МГП не всегда применимы к автономным военным роботам [1. С. 2].

В частности, нарушается принцип разграничения (*distinction*), требующий проведения границы между комбатантами и гражданскими лицами, когда автономные системы действуют в динамичной среде без прямого контроля человека. «Отсутствие четких правовых норм создает пробелы в системе ответственности за неправомерные действия с использованием автономных систем, которая может быть распределена между разработчиками, операторами и командирами. Исследование Роберта Спэрроу подчеркивает этические и правовые проблемы, связанные с определением ответственности за непредсказуемые действия машин» [2. С. 74]. Этот пробел подрывает соблюдение МГП и доверие общества к военным приложениям искусственного интеллекта.

В своем исследовании Ребекка Крутоф утверждает, что делегирование полномочий по принятию решений, сопряженных с вопросами жизни и смерти, автономным алгоритмам затрагивает проблемы, не предусмотренные существующим законодательством, регулирующим оборот оружия [3. С. 79]. Кроме того, это может привести к нарушению принципов человеческого достоинства и моральной ответственности. Применение автономных систем в военной сфере может снизить риск вооруженных конфликтов и уменьшить количество человеческих жертв и политических рисков. Однако использование таких технологий мо-

жет привести к эскалации конфликтов, поскольку государства и негосударственные субъекты стремятся получить преимущества, используя эти системы.

В Соединенных Штатах Америки и Китайской Народной Республике были разработаны национальные руководства, регламентирующие применение автономных вооружений и ИИ. Однако в этих документах стратегические цели зачастую ставятся выше этических и правовых норм, а также в них нередко прописываются специфические условия эксплуатации в военных целях, которые принимают во внимание разнообразные требования, стандарты, обстоятельства и способы применения. Такой фрагментарный подход препятствует формированию согласованных международных стандартов. Отсутствие единого международного регулирования способствует гонке вооружений, поскольку государства стремятся создать все более совершенные автономные системы. Такая конкуренция может привести к дестабилизации международной безопасности и повышению вероятности непреднамеренных конфликтов [4].

Эти документы должны охватывать ключевые аспекты, такие как механизмы подотчетности и принцип значимого человеческого контроля. Государства должны требовать от разработчиков прозрачности при создании и внедрении автономных систем. Это включает в себя требование к разработчикам документировать алгоритмы принятия решений и создавать механизмы для проверки соблюдения международного гуманитарного права. Организации, такие как ООН, должны возглавить усилия по развитию многостороннего сотрудничества, используя существующие платформы и соглашения, такие как Конвенция о «негуманном» оружии. Совместные инициативы могут способствовать гармонизации национальной политики государств и снижению рисков, связанных с гонкой вооружений.

Разработка и внедрение боевых роботов открывает новые перспективы, но также сопряжено с потенциальными угрозами для международной безопасности. Хотя автономные системы могут повысить результативность операций и уменьшить потери среди личного состава, их некорректное применение вызывает серьезные юридические и этические вопросы. Для урегулирования этих проблем требуется комплексная правовая основа, которая объединит международные законы, обеспечит прозрачность и взаимодействие между сторонами. Если государства будут действовать на опережение, они смогут гарантировать, что использование военной робототехники будет соответствовать принципам гуманизма и способствовать формированию стабильного и безопасного мирового порядка.

### Список литературы

1. Anderson K., Waxman M.C. Law and Ethics for Robot Soldiers // Policy Review. – 2012. – 19 p.
2. Sparrow R. Killer Robots // Journal of Applied Philosophy. – 2007. – Vol. 24, – № 1. – Pp. 62–77.
3. Crotoft R. Autonomous Weapon Systems and the Limits of Analogy // Harvard National Security Journal. – 2018. – Vol. 9. – Pp. 51–83.
4. Kahn L. How the United States Can Set International Norms for Military Use of AI // The Lawfare Institute. – 2024. – URL: <https://www.lawfaremedia.org/article/how-the-united-states-can-set-international-norms-for-military-use-of-ai>

**О. И. Ларина,**

кандидат экономических наук, доцент,  
Государственный университет управления

## **О ПЕРСПЕКТИВАХ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА**

**Аннотация.** В статье обозначены проблемные точки использования данной технологии, как в области рынка труда, так и в сфере конфиденциальности данных. Выделены и другие значимые факторы применения искусственного интеллекта: возможность социальной изоляции, отсутствие понимания юридической ответственности за решения. Сделан вывод о необходимости развития правовых норм, определяющих использование искусственного интеллекта в общественных системах.

**Ключевые слова:** цифровые технологии, машинное обучение, нормативно-правовое регулирование, этические аспекты, искусственный интеллект, социальные аспекты, риски искусственного интеллекта

## **ABOUT THE PROSPECTS OF LEGAL REGULATION APPLICATIONS OF ARTIFICIAL INTELLIGENCE**

**Abstract.** The article problematic points of using this technology are identified, both in the field of the labor market and in the field of data privacy. The author identifies other significant factors in the use of artificial intelligence: the possibility of social isolation, lack of understanding of legal responsibility for decisions. The conclusion is made about the need to develop legal norms that determine the use of artificial intelligence in public systems.

**Key words:** digital technologies, machine learning, regulatory and legal regulation, ethical aspects, artificial intelligence, social aspects, risks of artificial intelligence

Цель статьи – обозначить проблемные области в современном применении ИИ, затрагивающие социальную сферу, что требует, по мнению автора, скорейшего правового урегулирования.

Развитие и внедрение ИИ в различные направления человеческой деятельности и сферы жизни несет не только потенциальные преимущества, но и вызывает определенные опасения и негативные последствия. Беспрецедентная скорость, с которой развивается ИИ, повышает беспокойство относительно его воздействия на рабочую силу, приводя к утрате рабочих мест и увеличению неравенства разных групп населения. Также возникают вопросы относительно конфиденциальности данных и безопасности, особенно в условиях широкого применения алгоритмов машинного обучения, которое используется в основе ИИ.

Искусственный интеллект с его уникальными способностями становится неотъемлемой частью нашего повседневного опыта. Согласно исследованию почти 75 % опрошенных компаний признают искусственный интеллект ключевым фактором изменений в сфере бизнеса и трудоустройства [10]. Современная тех-

нология оказывает двойственное воздействие на рынок труда: с одной стороны, искусственный интеллект может способствовать созданию новых профессий (например, специалист по обучению ИИ) и рабочих мест в сфере технологий, но в то же время приводит к сокращению рабочей силы из-за автоматизации и внедрения нейросетей в производственные процессы. Так по прогнозам Федерального бюро статистики труда США, к 2030 году автоматизация сыграет важную роль в сокращении рабочих мест в 19 из 30 профессий, что может привести к увеличению числа безработных и, следовательно, к росту бедности. Люди, потерявшие свои рабочие места из-за автоматизации, столкнутся с финансовыми трудностями из-за снижения заработной платы. В том числе возрастет потребность в переквалификации для приобретения новых навыков, соответствующих требованиям изменяющегося рынка труда.

В современном мире, который все больше становится глобальным и технически передовым, межличностные связи сокращаются, что приводит к росту одиночества. По данным доклада Еврокомиссии около 13 % респондентов ответили, что чувствуют себя одинокими большую часть времени или на постоянной основе [6]. В условиях социальной изоляции и нехватки ресурсов для удовлетворения потребностей незащищенных слоев населения были разработаны искусственные роботы-компаньоны, которые обеспечивают компанию и поддержку людям, в частности престарелого возраста. Несмотря на положительные стороны данной разработки, существует ряд недостатков: утрата человеческих связей и деперсонализация отношений с машинами могут усилить чувство изоляции и ухудшить психологическое благополучие пользователей [5].

Другой важный аспект связан с конфиденциальностью данных. Например, по опубликованным данным в 2022 г. было утеряно 667,6 млн единиц персональных данных пользователей [3]. Данный факт свидетельствует о недостаточной защите личной информации в онлайн-среде, что ставит вопрос об эффективности использования ИИ, поскольку есть существенные затраты на его применение и убытки от потери данных. Эти факты могут вызывать недоверие общества к технологическим компаниям и инструментам на базе ИИ. Для пользователей важна уверенность, что все личные данные находятся в безопасности, в противном случае сознательное решение об ограничении применения ИИ в повседневной жизни становится неизбежным. В связи с этим ответственность компаний, а также регулирующих органов в обеспечении контроля и сохранности информации возрастает.

### Список литературы

1. Андреева Г. Н. Проблемы правового регулирования искусственного интеллекта в России // Россия: тенденции и перспективы развития. – 2021. – № 16–1. – С. 501–504.
2. Асадуллина А. В., Белоусов В. С. Регулирование технологий искусственного интеллекта на территории Европейского Союза // Российский внешне-экономический вестник. – 2022. – № 8. – С. 20–35.

3. Россия: утечки информации ограниченного доступа в 2022 г. // InfoWatch [Электронный ресурс]. – URL: <https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichenного-dostupa-v-rossii-za-2022-god.pdf>
4. Харитонов Ю. С., Савина В. С., Паньини Ф. Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права // Вестник Пермского университета. Юридические науки. – 2021. – № 53. – С. 488–515.
5. Berridge C., Zhou Y., Robillard J. M., Kaye J. Companion robots to mitigate loneliness among older adults: Perceptions of benefit and possible deception // Front. Psychol. – 2023. – Vol. 14. – DOI: <https://doi.org/10.3389/fpsyg.2023.1106633>
6. Loneliness and social connectedness: insights from a new EU-wide survey // European Commission. – URL: <https://publications.jrc.ec.europa.eu/repository/handle/JRC133351>
7. Obermeyer Z., Powers B., Vogeli C., Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations // Science. – 2019. – Vol. 366. – № 6464. – Pp. 447– 453. – DOI: 10.1126/science.aax2342
8. Personal Information Protection Law of the People's Republic of China // The National People's Congress of the People's Republic of China. – URL: [http://en.npc.gov.cn.cdurl.cn/2021-12/29/c\\_694559.htm](http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm)
9. Saniuk S., Grabowska S., Straka M. Identification of Social and Economic Expectations: Contextual Reasons for the Transformation Process of Industry 4.0 into the Industry 5.0 Concept. // Sustainability – 2022. – Vol. 14, № 3. – DOI: <https://doi.org/10.3390/su14031391>
10. The Future of Jobs Report 2023 // World Economic Forum. – URL: [https://www3.weforum.org/docs/WEF\\_Future\\_of\\_Jobs\\_2023.pdf](https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf)

**Д. О. Новиков,**  
частнопрактикующий юрист

## **ПРАВО И ЗАКОНОДАТЕЛЬСТВО ОБ ИСКУССТВЕННОМ ИНТЕЛЛЕКТЕ: ТЕОРЕТИКО-ПРАКТИЧЕСКАЯ ХАРАКТЕРИСТИКА И НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ**

**Аннотация.** Для регулирования искусственного интеллекта необходимо принять общий нормативный правовой акт – федеральный закон, краткая концепция и возможная структура которого приведена в настоящей статье. Также необходимы дополнения отраслевого законодательства, в представленной работе предложены некоторые нормы, которые могут быть внесены в ГК РФ, УК РФ и иные законы, а также определены направления совершенствования и развития законодательства об ИИ.

**Ключевые слова:** искусственный интеллект, законодательство об искусственном интеллекте, цифровые технологии, принципы искусственного интеллекта, правовой институт, совершенствование законодательства, концепция закона об искусственном интеллекте

## LAW AND LEGISLATION ON ARTIFICIAL INTELLIGENCE: THEORETICAL AND PRACTICAL CHARACTERISTICS AND DIRECTIONS OF IMPROVEMENT

**Abstract.** Of course, the desire to use artificial intelligence in order to facilitate some processes and make them more efficient is normal. However, in addition to the positive results from the use of artificial intelligence, there are certain risks, the abuse of artificial intelligence can lead to problems. An important aspect is the need for comprehensive regulatory regulation of the use of artificial intelligence, which is currently practically absent, which is a significant gap in the law. We believe that in order to regulate artificial intelligence, it is necessary to adopt a general regulatory legal act – a federal law, the brief concept and possible structure of which is given in this article.

**Keywords:** artificial intelligence, legislation on artificial intelligence, digital technologies, principles of artificial intelligence, legal institution, improvement of legislation, the concept of the law on artificial intelligence

Для анализа правовых и нормативных особенностей ИИ следует обратить внимание на содержание данного термина.

Из приведенного определения следует, что ИИ рассматривается с двух точек зрения – как научное направление и как свойство интеллектуальных систем. В приведенном издании термины «искусственный интеллект» и «машинный интеллект» рассматриваются как синонимы, равнозначные понятия, отдельно выделяется понятие «искусственный мозг», который определяется как повторение искусственными системами свойств, присущих мозгу человека.

Помимо понятия «искусственный интеллект» часто используются схожие термины «нейросеть», «робот» и иные, которые не являются синонимами. Например, роботы всегда обладают внешней оболочкой, некоторые роботы имеют ИИ, некоторые его не имеют. Нейросеть – это программа и инструмент, который может быть встроен в систему ИИ. Такие отличия свидетельствуют, что приведенные понятия, не являясь равнозначными, тем не менее тесно связаны между собой, могут пересекаться и дополнять друг друга.

Зарубежные исследователи отмечают, что искусственный интеллект, несомненно, является движущей технологической силой первой половины этого столетия, которая преобразит практически все отрасли, если не всю деятельность человека в целом [18. Р. 1]. Трудно спорить с данной мыслью, действительно, ИИ может существенно изменить мир, поэтому справедливым является обозначение современного периода как четвертой промышленной или технологической революции [16].

Социальная роль ИИ требует необходимости правового регулирования различных аспектов его разработки и использования.

**Право искусственного интеллекта: самостоятельная отрасль права или правовой институт?** Рост популярности ИИ, его использование во многих сферах деятельности, а именно в медицине, спорте, юриспруденции, в быту, ак-

туализируют проблему совершенствования нормативного регулирования и выявления статуса ИИ в юридической науке.

В настоящее время в юридической науке существуют два основных подхода к ИИ, в рамках которых он рассматривается либо как правовой институт, либо как предмет самостоятельной отрасли права. Существующие подходы всесторонне исследованы в работе Н. В. Мишиной [8. С. 62–62]. За рубежом существует самостоятельная отрасль права, регулирующая отношения, связанные с созданием и использованием ИИ, которая получила название робоправо. На наш взгляд, такое название значительно сужает предмет отрасли, поскольку ИИ и робот понятия смежные, пересекающиеся, но не синонимы.

Для ответа на вопрос, что же представляет собой право ИИ следует провести анализ с учетом признаков отрасли права, выделяемых в науке. М. Н. Марченко предлагает выделять два критерия отрасли права – предмет (основной критерий) и метод (вспомогательный критерий) [7. С. 443]. Л. Б. Тиунова исследует три критерия, позволяющих выделить самостоятельную отрасль права: объективная дифференциация общественных отношений, их государственно-правовая оценка, а также степень развитости соответствующей области правовых норм (консолидация норм и систематизация законодательства) [11. С.86].

Отсутствие официальных критериев деления права на отрасли приводит к научным дискуссиям со множеством взглядов на данную проблему. По-нашему мнению, можно выделить четыре признака отрасли права, которые позволят более подробно рассмотреть право ИИ.

Во-первых, признаком, выделяемым всеми исследователями, является особый предмет правового регулирования, под которым понимаются общественные отношения, регулируемые конкретной отраслью права. Искусственный интеллект, как технический инструмент и социальное явление формирует новые общественные отношения, связанные с особенностями его использования, ответственностью, границами и пределами использования. Можно сказать, что распространение ИИ формирует новые общественные отношения, анализируя которые, можно отметить, что ИИ – это не временное явление, в жизнь общества он вошел надолго, и его роль будет лишь усиливаться.

Во-вторых, в науке в качестве самостоятельного принципа выделяется наличие специфического метода правового регулирования. Отметим, что не все отрасли права имеют специфические методы. Любое нормативное регулирование строится на императивном, диспозитивном методе, либо на их сочетании. Например, в трудовом праве сочетаются императивный и диспозитивный методы, для уголовного права характерен преимущественно императивный метод. Проблемой метода правового регулирования ИИ является то, что его трудно определить. Нормативное регулирование ИИ крайне слабое, и это характерно не только для России, но и для многих государств мира. Искусственный интеллект больше изучается представителями технических наук, в общественных науках он изучен крайне слабо, какого-либо определенного метода регулирования нет. Однако, учитывая, что ИИ будет активно развиваться, то можно предположить, что его регулирование будет выстраиваться на сочетании императивного и диспозитивного методов. Наиболее целесообразным видится сочетание императивного,

рекомендательного и договорного способа правового регулирования, при этом для обеспечения безопасности приоритет следует отдать императивному методу, в пределах, которые не будут тормозить развитие ИИ.

В-третьих, следует выделить такой признак, как наличие специальных (отраслевых или межотраслевых) принципов. Как правило, во всех отраслях права правоотношения и их регулирование выстраиваются на ряде общих и специальных принципов. Например, к общим относятся законность, гуманизм, уважение прав и свобод человека и гражданина, они актуальны для всех отраслей права и всех видов правоотношений. Специальные принципы отражают специфику той или иной отрасли права. Например, в уголовном праве выделяют такие принципы, как неотвратимость ответственности, экономия мер государственного принуждения, в уголовном процессе специальными принципами являются – осуществление правосудия только судом, презумпция невиновности и пр. Многие из принципов носят межотраслевой характер, например принципы публичных отраслей права значительно пересекаются. Во многом схожи принципы процессуальных отраслей права. Очевидно, что принципы позволяют выделить самостоятельную отрасль права.

Принципы ИИ, как правило, содержатся в нормативных правовых актах, однако следует помнить, что в настоящее время они закреплены в подзаконном правовом акте. Отдельно можно уделить внимание развитию системы принципов, например, в качестве самостоятельного принципа обозначить необходимость нормативного определения границ и пределов использования ИИ и др.

В-четвертых, признаком отрасли права можно назвать наличие определенного массива правовых норм, позволяющих вести речь о самостоятельном характере отрасли права или наличие единого правового акта для регулирования общественных отношений, свойственных отрасли, например кодекса.

По нашему мнению, указанный признак, наряду с предметом правового регулирования, можно назвать одним из ключевых, позволяющих выделить нормы, регулирующие общественные отношения, в самостоятельную отрасль права. Как было указано выше, искусственный интеллект в настоящее время регламентируется крайне слабо, что является проблемой практически всех государств мира.

Учитывая, что достаточное нормативное регулирование ИИ в настоящее время отсутствует, то трудно говорить о праве ИИ, как о самостоятельной отрасли права.

Что касается единого, кодифицированного правового акта, как признака отрасли права, следует отметить, что его наличие является важным, но все-таки факультативным признаком. Многие отрасли права действительно имеют такой правовой акт. Однако следует помнить, что общество развивается и трансформируется, усложняются общественные отношения и многие отрасли права, появившиеся в последние 30 лет, носят комплексный характер – предпринимательское право, банковское право, транспортное право и не всегда имеют кодекс или специальный закон. В отечественной науке ведутся дискуссии о необходимости принятия отдельного кодекса, который бы регулировал предпринимательскую деятельность, но до настоящего времени в России такой кодекс не принят. Отметим, что такой кодекс принят в Казахстане [4]

Рассмотрение ИИ с точки зрения признаков, указанных выше, позволяет сделать вывод, что говорить о праве искусственного интеллекта, как о самостоятельной отрасли права, в настоящее время преждевременно, поскольку слабо разработано нормативное регулирование, в зачаточном состоянии находится определение специальных принципов и пр. Усиление роли искусственного интеллекта, его повсеместное использование, позволяет говорить о начале формирования соответствующего правового института.

Что касается появления новых отраслей права, следует отметить, что это не одномоментный процесс. Например, в настоящее время существует такая комплексная отрасль, как налоговое право. Однако после распада СССР и возникновения соответствующих общественных отношений, налоговое право было правовым институтом, подотраслью финансового права, а сейчас оно является самостоятельной отраслью права, хотя и не все исследователи это признают. До реформы научных специальностей ВАК в 2021, по которым присуждаются ученые степени кандидата и доктора наук, выделялась такая специальность, как «12.00.04 – «Финансовое право; налоговое право; бюджетное право», при этом ранее специальность «Финансовое право» входило в специальность 12.00.14 наряду с административным правом. Формирование отдельной научной специальности «Финансовое право; налоговое право; бюджетное право», показывает изменение государственного подхода к определению отраслей. После реформы научных специальностей в 2021 году все указанные отрасли стали фактически входить в специальность 5.1.2 Публично-правовые науки, что свидетельствует о повышении значимости комплексных научных исследований.

Рассматривая перспективы развития «права искусственного интеллекта», отметим, что в настоящее время оно формируется как комплексный правовой институт и требует полноты правового регулирования. Использование ИИ в различных сферах, его, безусловно, растущая роль в экономике, социальной сфере, позволяет предположить, что с течением времени может произойти формирование самостоятельной отрасли права – «права искусственного интеллекта». Трудно предположить, когда именно это может произойти, но тенденции развития ИИ позволяют сказать, что через 8–10 лет вопрос самостоятельности данной отрасли встанет в полный рост. Такой непродолжительный, на первый взгляд, срок до момента возможного формирования «права искусственного интеллекта» как самостоятельной отрасли права, отводится по причине ускорения темпа жизни, темпа технического и технологического развития, и ростом темпов интеграции ИИ в различные сферы жизни общества.

**Общее нормативное регулирование искусственного интеллекта и направления его совершенствования.** Выше было указано, что нормативное регулирование ИИ в настоящее время крайне слабое. В рамках данного раздела будет рассмотрено общее нормативное регулирование и разработаны направления совершенствования законодательства.

Отдельно отметим, что в настоящее время принят Кодекс этики в области ИИ, который подписан крупными компаниями – «Сбер» и «Яндекс», государственными корпорациями – «Росатом», инновационным центром «Сколково», научными и учебными учреждениями – МФТИ, ВШЭ, ИСП РАН и др. [14].

Таким образом, указанные выше документы носят подзаконный характер, являются стратегиями и концепциями в области развития ИИ, а Кодекс этики ИИ не имеет статуса официального нормативного правового акта.

В настоящее время ведутся дискуссии о том, может ли ИИ быть субъектом права? В некоторых государствах роботов с ИИ признали таковыми (например, робота София из Саудовской Аравии). Признание ИИ в качестве субъекта или квазисубъекта права, по нашему мнению, недопустимо и преждевременно, поскольку у них отсутствуют признаки, свойственные субъектам права, в частности, у них отсутствует воля. Признание в некоторых государствах роботов с ИИ в качестве субъектов права или гражданами государства не следует рассматривать всерьез. Чаще всего это является маркетинговым, рекламным и, в некоторой степени, политическим ходом, направленным на демонстрацию технологического преимущества.

Распространение ИИ требует разработки и принятия соответствующего федерального закона, закрепляющего основные понятия, принципы, общие вопросы ответственности разработчиков и пользователей ИИ и др. [9].

**Краткая Концепция Федерального закона «Об искусственном интеллекте» и его структура.**

**1. Основная идея, цели и предмет правового регулирования, круг лиц, на которых распространяется действие законопроекта, их новые права и обязанности, в том числе с учетом имеющихся.**

Основная идея заключается в необходимости регулирования общественных отношений в области ИИ, которые в настоящее время находятся на низком уровне. Большая часть нормативных актов в данной сфере носит подзаконный характер. Использование ИИ в различных сферах опирается лишь на общие принципы права, применение норм права в данной сфере связано с проблемами ответственности разработчиков и пользователей, границ и пределов использования и пр.

Распространение ИИ в различных сферах позволяет отметить, что помимо принятия общего закона, потребуются внесение изменений в отраслевые акты – ГК РФ, УК РФ и пр. Отраслевые положения должны соответствовать общим, которые и предлагается закрепить в Федеральном законе «Об искусственном интеллекте».

Единого закона, который бы регулировал указанные общественные отношения, в настоящее время нет, регулирование во многом носит обрывочный характер, что с учетом популяризации ИИ будет способствовать усилению проблем, накоплению вопросов о его разработке и применении в различных сферах.

Целью предлагаемого Федерального закона является формирование единой системы правового регулирования в области разработки и использования ИИ в России.

Предметом правового регулирования выступают правоотношения, которые возникают в связи с разработкой и использованием искусственного интеллекта.

Круг лиц, на которых распространяется действие предлагаемого закона широк, и включает в себя следующие группы:

- во-первых, организации, компании и индивидуальные разработчики программ и иных продуктов на основе искусственного интеллекта.
- во-вторых, органы государственной власти, местного самоуправления, и их должностные лица, а также коммерческие и некоммерческие организации, использующие программы и иные продукты на основе искусственного интеллекта в профессиональной деятельности;
- в-третьих, физические лица, использующие программы и иные продукты на основе искусственного интеллекта для решения бытовых задач (например, автомобили с автопилотом и другие).

Новые права и обязанности лиц, на которых распространяется действие закона. Предлагаемый закон направлен на регулирование общественных отношений, которые в настоящее время урегулированы крайне слабо, соответственно, у всех адресатов возникают новые права и обязанности. Например, при закреплении специальных принципов – человекоцентричность, установление границ и пределов использования ИИ и других, все участники будут обязаны соблюдать обязанности, обусловленные указанными принципами.

## **2. Место будущего закона в системе действующего законодательства.**

В соответствии с Классификатором правовых актов, утвержденным Президентом РФ, предлагается возможным указать, что предлагаемый закон будет относиться к разделу «Информация и информатизация» (120.000.000), подраздел 120.040.000 «Информатизация. Информационные системы, технологии и средства их обеспечения».

Для правовой системы России принятие закона положит начало формированию единой системы регулирования искусственного интеллекта, что позволит говорить о начале оформления ИИ, как правового института, который в перспективе может трансформироваться в самостоятельную отрасль права – «право искусственного интеллекта».

## **3. Общая характеристика и оценка состояния правового регулирования общественных отношений в сфере искусственного интеллекта.**

В настоящее время правовое регулирование ИИ крайне слабое, многие акты носят подзаконный характер, применение права об ИИ зачастую осуществляется по методу «аналогии права».

Предлагаемый закон станет фундаментальным, системообразующим актом в области разработки и использования ИИ.

## **4. Социально-экономические, политические, юридические и иные последствия реализации будущего закона.**

Принятие Федерального закона «Об искусственном интеллекте» позволит сделать сферу разработки и использования ИИ более регулируемой, будут устранены пробелы в праве в указанной сфере, и фактически будет положено официальное начало формированию правового института ИИ.

Законодательство всегда отстает от общественных и технологических тенденций, возникновение новых институтов и технологий приводит к тому, что они зачастую находятся в «серой зоне» по причине слабости правового регулирования. Отставание законодательства от современных тенденций, его устаревание – это

нормальный, естественный процесс, который не всегда связан с неэффективной работой органов законодательной власти.

Однако современное состояние и роль ИИ позволяют сказать, что необходимо активно заниматься разработкой нормативного регулирования данной сферы.

Важность определения статуса ИИ, его принципов, прав и обязанностей разработчиков и пользователей, и иных аспектов обусловлена ростом популярности, использованием в различных сферах – медицине, спорте и других.

Как было рассмотрено выше, изменения правовых норм при принятии предложенного закона не потребуются по простой причине – таких норм в федеральных законах нет.

**Структура Федерального закона «Об искусственном интеллекте» может быть следующей:**

Глава 1. Общие положения

В первой главе будут приведены цели и задачи правового регулирования, основные понятия, определен статус ИИ, как объекта права.

Глава 2. Принципы ИИ

Во второй главе будут приведены и раскрыты общие и специальные принципы разработки и использования ИИ.

Глава 3. Разработка ИИ

В третьей главе будут указаны субъекты, которые могут разрабатывать и ИИ, их права, обязанности, участие государства в разработке и поддержке ИИ.

Глава 4. Использование ИИ

В четвертой главе могут быть рассмотрены права и обязанности лиц, использующих ИИ, установлены запреты и ограничения.

Глава 5. Контроль и надзор за исполнением настоящего Федерального закона

В пятой главе необходимо закрепить особенности контроля и надзора за использованием ИИ при его разработке, а также при использовании в социально значимых сферах – в медицине, образовании, на транспорте и в других.

Глава 6. Заключительные и переходные положения

В заключительной главе необходимо закрепить порядок вступления Федерального закона в силу, указать какие нормативные акты требуют внесения изменений.

Предложенная выше структура законопроекта носит дискуссионный характер, и, следует помнить, что закон носит общий характер. Помимо разработки и принятия нормативного правового акта общего характера следует уделять внимание и отраслевым актам и иным федеральным законам, направления развития некоторых будут рассмотрены ниже.

*Нормативное регулирование искусственного интеллекта в различных отраслях права и направления его совершенствования*

Искусственный интеллект в настоящее время используется в общественных отношениях, относящихся к разным отраслям права.

Так, в гражданском праве ИИ может быть использован для автоматизации процессов и унификации юридических процедур, для составления договоров, анализа и обработки больших объемов данных [5. С.1294–1296]. Помимо этого,

ИИ в гражданском праве является объектом сделок, результатом интеллектуальной деятельности и пр.

Все указанные аспекты использования ИИ должны быть регламентированы законодательно, чего в настоящее время не наблюдается.

Отдельно в гражданском законодательстве должны найти отражение положения о том, что ИИ является объектом гражданского права.

В уголовном праве и уголовном процессе ИИ может быть использован различным образом, например, он может помогать в расследовании преступлений, анализируя огромные массивы данных, но его возможности могут быть направлены и в обратную сторону – для совершения преступлений. Не является секретом, что любые технологии, разработки могут быть использованы как во благо, так и во вред обществу, и ИИ, который может применяться для расследования и раскрытия преступлений, так и для их совершения, – яркий тому пример. Предлагаем дополнить ст. 63 УК РФ, посвященную обстоятельствам, отягчающим наказание, пунктом «у», который может звучать следующим образом:

Отягчающими обстоятельствами признаются: «совершение преступления с использованием технологий искусственного интеллекта, нейросетей, роботов, и иных современных технологических решений *(также необходимо раскрытие понятия «современные технологические решения, это можно сделать в законе об ИИ).*

Также можно дополнить УК РФ или его статьи новыми нормами, которые устанавливали бы повышенную ответственность за преступления, совершенные с помощью ИИ. Например, это актуально для преступлений, предусмотренных ст. 159 УК РФ (Мошенничество), 264 УК РФ (Нарушение правил дорожного движения и эксплуатации транспортных средств) и др.

В уголовном процессе ИИ можно применять для организации предварительного расследования, оценки доказательств, профилактики и выявления преступлений, проведении экспертиз [10. С. 481–497]. Например, зарубежные исследователи указывают на возможность выявлять с помощью ИИ киберпреступления [20]. Однако справедливо отмечается, что для ИИ характерна необъяснимость, возможна предвзятость, имеется недостаток ответственности [10. С. 481–497]. Это является проблемами, которые требуют внимательного использования ИИ в процессе расследования. Для минимизации рисков следует нормативно закрепить порядок и границы использования ИИ в уголовном процессе. Помимо нормативной регламентации использования ИИ следует уделять внимание технологическим возможностям и подготовке кадров. Однако не следует излишне оптимистично относиться к возможностям использования ИИ в уголовном процессе, поскольку его механизмы далеки от совершенства, его можно с осторожностью применять для анализа большого количества данных, что особенно актуально при расследовании экономических преступлений.

Вопросы использования ИИ в судопроизводстве также вызывают интерес в науке, и отмечается, что он может быть использован для информационной поддержки, автоматизации поиска решений, сбора судебной статистики и иных целей [13. С. 1365–1368]. Слабая урегулированность ИИ в целом, различные этические проблемы требуют разработки правовой основы для использования ИИ в

судопроизводстве. Например, в процессуальные законы (УПК РФ, ГПК РФ, АПК РФ, КАС РФ) могут быть включены соответствующие нормы о возможностях, границах и пределах использования ИИ в судебном процессе. Предложения по содержанию такой нормы приведем ниже:

«1. В процессе судопроизводства суд имеет право использовать искусственный интеллект, нейросети и иные современные технологические решения, в пределах, не нарушающих основные принципы судопроизводства.

2. В процессе судопроизводства могут быть использованы искусственный интеллект, нейросети и иные современные технологические решения, прошедшие обязательную сертификацию (в настоящее время обязательной сертификации нет, но имеется добровольная. Однако имеются планы Правительства РФ сделать сертификацию обязательной [15]), и допущенные к использованию Верховным Судом РФ.

3. Искусственный интеллект, нейросети и иные современные технологические решения не могут быть использованы для составления судебных актов (*решений, приговоров и иных*).

4. Контроль за использованием искусственного интеллекта, нейросетей и иных современных технологических решений осуществляется в порядке, определяемом Верховным Судом РФ.

5. При использовании искусственного интеллекта, нейросетей и иных современных технологических решений в процессе судопроизводства необходимо указание об этом в материалах дела.

Отдельно необходима разработка подробного нормативного акта, регламентирующего порядок использования искусственного интеллекта, нейросетей и иных современных технологических решений в судебной деятельности. Такой акт может быть разработан и принят Судебным департаментом при Верховном Суде РФ.

**Заключение.** Рассмотренные выше некоторые сферы деятельности и отрасли использования ИИ показывают, что отраслевое нормативное регулирование данных процессов в настоящее время отсутствует, однако проведенный анализ позволил сформулировать предложения по совершенствованию законодательства в гражданском и уголовном праве, а также в процессуальных отраслях.

Искусственный интеллект в настоящее время становится неотъемлемой частью жизни, он используется в различных сферах – предпринимательской деятельности, медицине, спорте и многих других. Однако нормативное регулирование ИИ находится на низком уровне, что создает определенные проблемы при его использовании, поскольку отсутствуют единые принципы и механизмы его применения. В такой ситуации многое зависит от моральных качеств, этичности, осознания ответственности лиц, его использующих.

В процессе исследования были сформулированы предложения по развитию нормативного регулирования в области ИИ – приведена краткая концепция Федерального закона «Об искусственном интеллекте», обозначена структура данного закона, также разработаны предложения по совершенствованию ГК РФ и процессуальных кодексов (ГПК РФ, АПК РФ и др.). Приведенные предложения позволяют обозначить контуры и направления развития законодательства

для того, чтобы сфера использования ИИ стала более регулируемой. Это позволит снизить риски от использования ИИ, позволит определить ответственность разработчиков и пользователей и решит другие актуальные проблемы, которые без должного нормативного регулирования будут лишь усиливаться.

### Список литературы

1. Федеральный закон от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // Собрание законодательства РФ. – 27.04.2020. – № 17. – Ст. 2701.
2. Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства РФ. – 14.10.2019. – № 41. – Ст. 5700.
3. Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // Собрание законодательства РФ. – 31.08.2020. – № 35. – Ст. 5593.
4. Предпринимательский кодекс Республики Казахстан от 29.10.2015 № 375-V ЗРК (ред. от 01.09.2024) // Казахстанская правда. – 03.11.2015. – № 210(28086).
5. Аненкова А. А., Гончарова С. Г. Место искусственного интеллекта в структуре гражданских правоотношений // Материалы конференции Весенние дни науки, Екатеринбург, 20–22 апреля 2023 года. – Екатеринбург: Издательский дом Ажур. – С. 1294–1296.
6. Арзамасов Ю. Г. Комплексный подход к определению искусственного интеллекта // Вестник Воронежского государственного университета. Серия: Право. – 2022. – № 3. – С. 242–262.
7. Марченко М. Н. Теория государства и права: учеб.-метод. пособие: Моск. гос. ун-т им. М. В. Ломоносова. Юрид. фак. – М.: Зерцало-М, 2001. – 623 с.
8. Мишина Н. В. Право искусственного интеллекта как новая сфера правового регулирования или новая отрасль права // Евразийский Союз Ученых. – 2020. – № 3. – С. 62–65.
9. Полякова Т. А., Камалова Г. Г. «Право искусственного интеллекта» и его место в системе информационного права // Правовое государство: теория и практика. – 2021. – № 3. – С. 133–145.
10. Спиридонов М. С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law. – 2023. – № 1. – С. 481–497.
11. Тиунова Л. Б. Системные связи правовой действительности: методология и теория. – СПб.: Изд-во СПбГУ. – 1991. – 133 с.

12. Толковый словарь по искусственному интеллекту / авт.-сост. А. Н. Аверкин, М. Г. Гаазе-Рапопорт, Д. А. Поспелов. – М.: Радио и связь, 1992. – 256 с.
13. Эберт Е. С., Эмищян Е. А., Шаблова Е. Г. Правосудие и искусственный интеллект: перспективы и проблемы // Материалы конференции Весенние дни науки, Екатеринбург, 20–22 апреля 2023 года. – Екатеринбург: Издательский дом Ажур. – С. 1365–1368.
14. Кодекс этики в сфере искусственного интеллекта (Альянс в сфере искусственного интеллекта) [Электронный ресурс]. – URL: <https://ethics.a-ai.ru/>
15. Правительство задумалось о сертификации ИИ-решений для поддержки внедряющих их компаний // Интерфакс [Электронный ресурс]. – 13.03.2024. – URL: <https://www.interfax.ru/russia/950230>
16. Fouad F. The Fourth Industrial Revolution is the AI Revolution A Business Prospective // International Journal of Information Technology. – 2019. – № 8. – P.12–23. DOI: 10.30534/ijisat/2019/01852019.
17. Frigerio I., Rashidian N. White paper: ethics and trustworthiness of artificial intelligence in clinical surgery // Intelligence & Robotics. – 2023. – № 3. – P.111–122. – DOI:10.20517/ais.2023.04.
18. Holmes W., Bialik M., Fadel C. Artificial Intelligence In Education Promises and Implications for Teaching and Learning. – 2019. – 37 p.
19. International Test and Evaluation Standards for Artificial Intelligence based on Networked Data-Information- Knowledge-Wisdom-Purpose (DIKWP) Model. – 2024. – July. – DOI:10.13140/RG.2.2.28549.56809
20. Kaur R., Gabrijelcic D., Klobucar T. Artificial intelligence for cybersecurity: Literature review and future research directions // Information Fusion. – 2023. – № 97. – DOI: 10.1016/j.inffus.2023.101804
21. Lukanova G. Robots, Artificial Intelligence and Service Automation // in HotelsIn book: Robots, Artificial Intelligence, and Service Automation in Travel, Tourism, and Hospitality. – 2019. – Pp.157–183. – DOI: 10.1108/978-1-78756-687-320191009

**В. С. Савина,**

доктор юридических наук, профессор,  
Российский экономический университет  
имени Г. В. Плеханова

## **АКТУАЛЬНЫЕ ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ТЕХНОЛОГИЙ ВИРТУАЛЬНОЙ И ДОПОЛНЕННОЙ РЕАЛЬНОСТИ**

**Аннотация.** Цель исследования составляет формирование комплексного представления о проблемах, возникающих в сфере правового регулирования технологий виртуальной и дополненной реальности. Новейшие цифровые технологии могут изменить нашу жизнь к лучшему, однако необходима адекватная оценка рисков их применения, а также разработка соответствующего правового

регулирования. В первую очередь оно должно быть направлено на решение вопросов безопасности, защиты персональных данных и иной конфиденциальной информации. В настоящее время возникает особая сфера правового регулирования, связанная с осуществлением различных видов прав человека в информационно-телекоммуникационных сетях, а также технологий виртуальной и дополненной реальности.

**Ключевые слова:** виртуальная и дополненная реальность, виртуальное пространство, киберправо, правовое регулирование

## CURRENT ISSUES OF LEGAL REGULATION OF VIRTUAL AND AUGMENTED REALITY TECHNOLOGIES

**Abstract.** The purpose is to examine the problems arising in the sphere of legal regulation of virtual and augmented reality technologies. The latest digital technologies can change our lives for the better, but an adequate assessment of the risks of their use is necessary, as well as the development of appropriate legal regulation. First of all, it should be aimed at solving issues of security, protection of personal data and other confidential information. It seems that at present a special sphere of legal regulation is emerging related to the implementation of various types of human rights in information and telecommunication networks, as well as virtual and augmented reality technologies.

**Keywords:** Virtual and augmented reality, virtual space, cyber law, legal regulation

Цифровые технологии помогают человеку преодолевать ограничения пространства, времени и физических возможностей. Для этого используются методы улучшения умственных способностей и изменения восприятия реальности. Примером является создание метавселенной (Meta<sup>1</sup> признана экстремистской организацией, ее деятельность запрещена в РФ), представляющей собой виртуальную социальную среду, доступную через цифровой аватар. Аватар – это виртуальная форма, которая может принимать различные облики и свободно перемещается в виртуальной среде [10].

«Сингапурские исследователи создали биомиметический материал из высокоэластичного полимера, имитирующий человеческую кожу. Он способен автономно самовосстанавливаться при механическом повреждении, имитировать осязание и определять приближение объектов... К настоящему моменту есть множество разработок, способных имитировать часть функций человеческой кожи» [10].

Технологии виртуальной и дополненной реальности можно использовать также в предпринимательской деятельности, для рекламных целей, в креативных индустриях, индустриях развлечений, а также в целях обучения. Основное их свойство – эффект реального присутствия. Например, компания GiveAR в 2014 году на одной из башен «Москва-Сити» установила виртуальное

---

<sup>1</sup> Мета – организация признанная экстремистской, ее деятельность запрещена на территории Российской Федерации.

10-метровое «Око Саурана», увидеть которое можно было через смартфон с помощью специального приложения [7].

В философском энциклопедическом словаре и Большом толковом словаре русского языка виртуальный (от лат. *virtus* – сила, способность) означает «возможный; такой, который может или должен проявиться при определенных условиях; условный, кажущийся (виртуальная реальность)» [2].

Для анализа правового регулирования технологий виртуальной и дополненной реальности обратим внимание в первую очередь на происхождение данных терминов. В переводе с латыни *virtus* означает потенциальный, возможный, мнимый, воображаемый, а *realis* – вещественный, действительный, существующий. Такое понимание виртуальности находит отражение в трудах многих ученых. Например, Кристофер Цифрино употребляет для обозначения виртуальной собственности термин «*elusive*», что означает в переводе с английского языка на русский «неуловимый», «уклончивый» [15].

Реальность в философии понимают как синоним бытия: «понятие бытия не обладает никакой двусмысленностью: оно однозначно и синонимично реальности вообще, взятой без разграничения на типы, т. е. предстает в виде многообразия форм и типов реальности, исторически доступной человеку» [12]. Тем самым значение слов «виртуальный» и «реальный» прямо противоположное, и тем не менее мы используем их в рамках единого термина.

Виртуальную реальность можно определить следующим образом: это «технически конструируемая при помощи компьютерных средств интерактивная среда порождения и оперирования объектами, подобными реальным или воображаемым, на основе их трехмерного графического представления, симуляции их физических свойств (объем, движение и т. д.), симуляции их способности воздействия и самостоятельного присутствия в пространстве, а также создания средствами специального компьютерного оборудования эффекта присутствия человека в этой объектной среде (чувство пространства, ощущения и т. д.), сопровождающегося ощущением единства с компьютером» [3].

Термины «виртуальная реальность» и «дополненная реальность» имеют сходное значение, однако с технической точки зрения между ними имеются и различия. Дополненная реальность предполагает интеграцию цифровых данных со средой пользователя в режиме реального времени. В отличие от виртуальной реальности (VR), где формируется полностью искусственная среда, использование AR осуществляется на основе реально существующей среды окружающего мира с наложением поверх нее сгенерированной информацией, воспринимаемой органами чувств человека. Сфера использования дополненной реальности – это визуальное изменение окружающей среды, либо предоставление пользователям дополнительной информации.

В основу технологий виртуальной и дополненной реальности положена концепция симуляции. Ж. Бодрийяр отмечал, что «симуляция – это... порождение моделей реального без оригинала и реальности: гиперреального. Таким образом, исчезновением реального, симуляция, наносит удар по установленному порядку... теперь невозможно отделить и процесс реального, или доказать реальность реального».

Термины «виртуальная реальность» (англ. virtual reality, VR), «дополненная реальность» (англ. augmented reality, AR) тесно связаны с понятиями «виртуальное пространство» и «киберпространство», которые известны цивилистике достаточно давно, и активно используются в ряде научных исследований [11]. В некоторых правовых исследованиях можно также встретить термин «гиперреальность» [6]. Эти термины применяются также во многих других областях научного знания: философии, социологии, истории, экономики, медицины и других наук. Тем не менее следует отметить, что до сих пор не сформировалось единого мнения относительно определений данных понятий.

В отличие от аналогового мира, в виртуальном мире коммуникации осуществляются на основе законов формальной логики и правил обработки, хранения и передачи информации, заданных человеком (разработчиком, программистом). Такой подход предполагает однозначную оценку явления. Поэтому далеко не всегда правовые средства, разработанные для реального мира, способны урегулировать отношения, складывающиеся в виртуальном (электронно-цифровом) мире.

А. В. Демин, анализируя влияние права на виртуальную реальность, отмечает, что и то, и другое явление представляют собой «символический мир идеальных образов, во многом условный и лишь с относительной достоверностью отображающий бытие объективного мира» [4]. В .Г. Земченкова и М. В. Никитина полагают, что «изменяя реальное видение объекта, автор промышленного образца отталкивается от своего восприятия формы изделия, которое, как правило, являясь условным идеальным его образом, в условиях виртуальной среды отражает субъективность эстетических взглядов автора» [5].

Ученые отмечают, что дихотомия «реальное – виртуальное» [8] должна быть воспринята правом.

Итак, новейшие цифровые технологии могут изменить нашу жизнь к лучшему, однако необходима адекватная оценка рисков их применения, а также разработка соответствующего правового регулирования. В первую очередь оно должно быть направлено на решение вопросов безопасности, защиты персональных данных и иной конфиденциальной информации. Как представляется, в настоящее время возникает особая сфера правового регулирования, связанная с осуществлением различных видов прав человека в информационно-телекоммуникационных сетях, а также технологий виртуальной и дополненной реальности.

### Список литературы

1. Бодрийяр Ж. Симулякры и симуляция [Электронный ресурс]. – URL: <http://exsistencia.livejournal.com/>
2. Большой толковый словарь русского языка / Сост. и гл. ред. С. А. Кузнецов. – СПб.: «Норинт», 1998.
3. Грицанов А. А., Галкин Д. В., Карпенко И. Д. Виртуальная реальность // Новейший философский словарь: 3-е изд., исправл. – Минск: Книжный Дом, 2003. – С. 171–173.

4. Демин А. В. Фикции в нормах налогового права // Финансовое право. – 2013. – № 4. – С. 24–30.
5. Земченкова В. Г., Никитина М. В. Комментарий к законодательству РФ о промышленных образцах [Электронный ресурс] // СПС «КонсультантПлюс».
6. Коляда А. В. Интеллектуальная собственность как системная правовая реальность // Юридический мир. – 2013. – № 4. – С. 40–45.
7. Око Саурана. Дополненная реальность. GiveAR // Комсомольская правда. – 13 дек. 2014 г. [Электронный ресурс]. – URL: <https://www.kp.ru/video/513613/>
8. Коротникова Н. В. Интернет как средство производства сетевых коммуникаций в условиях виртуализации общества // Социологические исследования. – 2007. – № 2. – С. 85–86.
9. Косарев А. С. Проблемы правового регулирования сделок в сфере электронной коммерции: дисс. канд. юридических наук: 12.00.03. – М., 2010.
10. Савина В. С. К вопросу о гражданско-правовой ответственности при использовании систем искусственного интеллекта для модификации человека // Ученые записки юридического факультета. – 2022. – № 4. – С. 60–62. – EDN CWSKUW.
11. Ситдикова Л. Б. Правовое регулирование отношений в сфере оказания информационных и консультационных услуг в Российской Федерации: дисс. доктора юридических наук: 12.00.03. – М., 2009.
12. Спиркин А. Г. Философия: учебник. 2-е изд. – М.: Гардарики, 2010.
13. Тарасов М. В. Субъекты и объекты гражданских правоотношений в информационно-коммуникационных сетях: проблемы теории и практики: дисс. канд. юридических наук: 12.00.03. – М., 2014.
14. Философский энциклопедический словарь / под ред. Губского Е.Ф. и др. – М.: ИНФРА-М, 2001.
15. Christopher J. Ciffrino. Virtual Property, Virtual Rights: Why Contract Law, Not Property Law, Must be the Governing Paradigm in the Law of Virtual Worlds // Boston College Law Review. – 2014. – № 235. – С. 235–264.

**И. А. Филипова,**

кандидат юридических наук, доцент,  
Национальный исследовательский  
Нижегородский государственный университет  
имени Н. И. Лобачевского

### **СРАВНЕНИЕ ПОДХОДОВ К РЕГУЛИРОВАНИЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА (НА ПРИМЕРЕ РОССИИ, КИТАЯ, ЕВРОПЕЙСКОГО СОЮЗА И США)**

**Аннотация.** Работа направлена на сопоставление разнообразных методов регулирования искусственного интеллекта, которые формируются в разных странах и регионах мира. Сравнительный анализ различных подходов позволяет сделать выводы о предпочтительности использования или неиспользования

определенных правовых конструкций в создаваемом сегодня российском правовом регулировании в сфере искусственного интеллекта.

**Ключевые слова:** правовое регулирование, искусственный интеллект, система искусственного интеллекта, риск-ориентированность, сегментирование, системный подход, антропоцентризм

## COMPARISON OF APPROACHES TO THE REGULATION OF ARTIFICIAL INTELLIGENCE (ON THE EXAMPLE OF RUSSIA, CHINA, THE EUROPEAN UNION AND THE UNITED STATES)

**Abstract.** The work is aimed at comparing the various methods of artificial intelligence regulation that are being formed in different countries and regions of the world. A comparative analysis of various approaches allows us to draw conclusions about the preference of using or not using certain legal structures in the Russian legal regulation in the field of artificial intelligence that is being created today.

**Keywords:** legal regulation, artificial intelligence, artificial intelligence system, risk-based approach, segmentation, systems approach, anthropocentrism

**Введение.** Искусственный интеллект (далее – ИИ) быстро развивается, а его возрастающее влияние на общество способствует формированию национального и международно-правового регулирования.

**Основная часть.** Процесс создания регулирования ИИ в России мы можем разделить на несколько этапов (хотя подобное деление на этапы является весьма условным). Первый этап (2016–2019 годы) был заключен в подготовке программных документов, которые определили российские национальные политики в области ИИ. Второй этап включает в себя создание определенных правовых основ и разработку будущих российских законов (2020–2024 годы). Следующий третий этап в перспективе завершится созданием полноценной системы регулирования ИИ (2025–2030 годы). Деление на перечисленные выше этапы соответствует плану, содержащемуся в Национальной стратегии развития ИИ, утвержденной Указом Президента Российской Федерации № 490 от 10 октября 2019 года, и обновленной в 2024 году. Тем самым Россия создает свой собственный подход к регулированию ИИ, и особенности этого подхода постепенно проявляются в российском законодательстве. Принципы регулирования можно увидеть в Концепции развития регулирования отношений в сфере технологий ИИ и робототехники на период до 2024 года, одобренной Правительством Российской Федерации в Распоряжении от 19 августа 2020 года № 2129-р. Основными особенностями российского подхода к регулированию ИИ являются следующие:

- цель регулирования состоит в том, чтобы способствовать развитию искусственного интеллекта, устраняя барьеры различного свойства, включая правовые;
- поставленная задача – минимизировать риски (контролируя их уровень);
- учет и использование лучшего зарубежного опыта.

Сравним российский подход с иными подходами, складывающимися в других странах или группах стран. Сегодня разные страны и регионы разраба-

тывают свои подходы к регулированию ИИ. Особенно интересны с точки зрения сравнительного анализа европейский и китайский подходы, так как два этих подхода являются наиболее устоявшимися, ведь Европейский Союз и Китай конкурируют за право первыми в мире создать регулирование ИИ. Начнем с Европейского союза.

Европейский подход к регулированию ИИ является риск-ориентированным и «жестким», демонстрирующим серьезные ограничения. Положительной стороной этого подхода является акцент на правах человека (хотя некоторые исследователи утверждают, что этот акцент выражен явно недостаточно) [3. С. 1], еще один плюс – системность правового регулирования, европейское регулирование выстраивается горизонтально, наиболее широко рассматривая сферу ИИ. Но не стоит оставлять без внимания то, что строгие ограничения, присутствующие в европейском законодательстве по ИИ, станут барьерами для развития ИИ, поэтому российское регулирование, хоть и будет развиваться на основе риск-ориентированного подхода, не будет таким строгим.

Хотя в России уже есть несколько законов, касающихся использования ИИ, но нет акта, подобного Европейскому регламенту об ИИ. Увидим ли мы такой закон в ближайшие годы? На этот вопрос трудно ответить однозначно. К примеру, проект Цифрового кодекса Российской Федерации уже обсуждался в российском парламенте и планируется к обсуждению в доработанном варианте в 2025–2026 годах, кроме того, готовится или уже обсуждается целый ряд законопроектов, среди них: проекты о внесении изменений в Гражданский кодекс Российской Федерации и иные нормативные правовые акты. Предлагаемые поправки касаются защиты человеческого голоса, интеллектуальной собственности на произведения, создаваемые с использованием ИИ, маркировки контента, сгенерированного нейронными сетями, применения ИИ в предвыборной агитации и так далее.

Вторым из наиболее сформированных подходов к регулированию ИИ является китайский. К преимуществам этого подхода следует отнести:

- гибкость, как следствие сегментации регулирования, вместо системности;
- умеренность в ограничениях, которая не станет препятствием для развития ИИ, тем самым нацеленность на максимальную реализацию потенциала искусственного интеллекта.

В то же время наименования китайских нормативных правовых актов в сфере ИИ указывают на регулирование достаточно узких вопросов, и в этом китайский подход схож с российским. Впрочем, в Китайской Народной Республике уже обсуждается законопроект об ИИ [2. С. 46–73], собственно, как и в России – проект Цифрового кодекса, что указывает на общую тенденцию к горизонтальному регулированию, изначально характерную для европейского подхода. «Увеличение количества сфер, в которых происходит использование ИИ, все больше заставляет задуматься о необходимости системного подхода к построению модели регулирования ИИ» [1. С. 10].

Пока же по степени антропоцентризма европейский подход не имеет конкурентов. Принципиальным различием в стратегиях развития искусственного

интеллекта Китайской народной Республики и Европейского союза является то, что в Европе политические дискуссии по поводу регулирования ИИ были вызваны прежде всего его широким распространением и желанием контролировать вероятные вредные последствия от использования [4. С. 505–528], в Китае же отправной точкой послужило желание реализовать потенциал ИИ, то есть, если Европейский союз изначально заботило снижение возможного вреда, то Китай – перспективы инноваций [5. С. 1441–1459].

Итак, российский подход ближе к китайскому, нежели европейскому, за счет гибкости и отсутствия горизонтальности регулирования. Гибкость подхода присутствует еще и потому, что российское регулирование ИИ – это в основном этические правила. Впрочем, этические нормы в этой области разработаны и в Китае, США, Европе. Общеизвестно, что недостатком этического регулирования является отсутствие юридической ответственности за игнорирование этических норм. К примеру, в США подход к регулированию ИИ сформирован в значительно меньшей, чем в Китае и Европейском союзе, до настоящего времени сохраняется значительная фрагментарность правового регулирования, в основном принимаются законы отдельных штатов по узким вопросам (например, по распознаванию лиц с помощью систем ИИ), но увеличение количества предлагаемых в этой области законопроектов на федеральном уровне позволяет прогнозировать перенос риск-ориентированности, свойственной европейскому регулированию, и на американскую «почву», как это уже происходит с Китаем. В России, как уже упоминалось, риск-ориентированность изначально заявлена как один из принципов создаваемого регулирования.

Как будет дальше развиваться регулирование ИИ в России? Фактически российский национальный подход еще ближе, чем к китайскому, к подходу США и Великобритании, предпочитающих не устанавливать никаких жестких ограничений, во избежание торможения в развитии ИИ, так что жесткие ограничения в ближайшие годы в российском законодательстве по искусственному интеллекту мы вряд ли обнаружим.

Вернемся к правительственной «Концепции развития регулирования отношений в сфере технологий ИИ и робототехники на период до 2024 года», а точнее к основным принципам регулирования ИИ в России, в ней заявленным. Первый из принципов – стимулирование развития технологий как основа – близок к китайскому (а также американскому) подходу. Второй заявленный принцип – риск-ориентированность и междисциплинарность – тяготеет к европейскому подходу. Третий принцип – расширение использования инструментов саморегулирования, создание этических правил – также больше подходит американскому подходу.

**Заключение.** Международный подход, без сомнения, будет складываться в итоге с учетом наработок уже формирующихся сегодня национальных и региональных подходов. Каким он будет? Риски от развития ИИ возрастают, включая экзистенциальные риски для всего человечества. Скорее всего, придется создавать не только этические нормы, но и нормы права, которые защищают человека и человеческое общество в целом, которое все больше будет ощущать противостояние между ИИ и людьми. И подобную проблему невозможно урегулировать.

ровать законодательными ограничениями только в одной стране или группе стран, поиск решения этой задачи станет необходимым в ближайшие несколько лет для всего мирового сообщества. От того, насколько хорошо будет решена данная задача, зависит общее будущее людей.

### Список литературы

1. Перспективные направления правового регулирования искусственного интеллекта: монография / под ред. А. В. Минбалева. – Саратов: Амирит. – 2023. – 442 с.
2. Филипова И. А. Правовое регулирование искусственного интеллекта: опыт Китая // Journal of Digital Technologies and Law. – 2024. – Т. 2, № 1. – С. 46–73.
3. Arnold L. How the European Union’s AI Act Provides Insufficient Protection Against Police Discrimination // Journal of Law and Social Change. – Online first. – May 14, 2024.
4. Cath C., Wachter S., Mittelstadt B., Taddeo M., Floridi L. Artificial intelligence and the “good society”: The US, EU, and UK approach // Science and Engineering Ethics. – 2018. – Vol. 24 – Iss. 2. – Pp. 505–528.
5. Zeng J. Artificial intelligence and China’s authoritarian governance. International Affairs. – 2020. – Vol. 96. – Iss. 6. – Pp. 1441–1459.

**В. Н. Шельменков**

старший преподаватель,  
Университет имени О.Е. Кутафина (МГЮА)

### LEGAL TECH РЕВОЛЮЦИЯ: КАК ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ МЕНЯЕТ ЮРИДИЧЕСКУЮ СФЕРУ

**Аннотация.** Статья посвящена Legal Tech революции и ее влиянию на юридическую сферу. Цель статьи – проанализировать, как искусственный интеллект меняет работу юристов, какие новые возможности и проблемы возникают в связи с этим. В результате исследования выявлены основные тенденции развития Legal Tech, его перспективы и последствия для юридической практики.

**Ключевые слова:** искусственный интеллект, информационные технологии, информационные системы, база данных, программы для ЭВМ, Legal Tech, автоматизация процессов, прогнозирование

### LEGAL TECH REVOLUTION: HOW ARTIFICIAL INTELLIGENCE IS CHANGING THE LEGAL FIELD

**Abstract.** The article is devoted to the Legal Tech revolution and its impact on the legal sphere. The purpose of the article is to analyze how artificial intelligence is changing the work of lawyers, what new opportunities and problems arise in this regard. The research methodology includes the analysis of scientific articles, reports and other sources of information on the topic of Legal Tech. As a result, of the work, the

main trends in the development of Legal Tech, its prospects and consequences for legal practice will be revealed.

**Keywords:** artificial intelligence, information technology, information systems, database, computer programs, Legal Tech, process automation, forecasting

**Введение.** В современном мире технологии развиваются с невероятной скоростью, и юридическая сфера не является исключением. Искусственный интеллект (ИИ) становится все более важным инструментом для юристов, помогая им автоматизировать рутинные задачи, анализировать большие объемы данных и принимать обоснованные решения. Это явление получило название Legal Tech – революция в юридической сфере, которая меняет традиционные подходы к работе юристов и адвокатов.

Развитие LegalTech построено на внедрении новых технологий в юридическую деятельность как в процессе правотворчества, так и правоприменения, юридического консалтинга, а также осуществления правосудия.

В настоящий момент, законодательство, которое дает возможность развиваться отрасли LegalTech, находится в недостаточном состоянии. В связи с этим необходимо законодательно зафиксировать гарантии соблюдения прав и свобод человека и гражданина в процессе использования технологий LegalTech.

Направлением данной работы является исследование влияния искусственного интеллекта в области юридических наук, а также определение перспектив развития Legal Tech.

Актуальность темы обусловлена необходимостью адаптации юридической сферы к новым технологическим реалиям и определения наиболее эффективных способов использования искусственного интеллекта для повышения качества юридических услуг и оптимизации рабочих процессов.

Результаты работы позволят оценить текущее состояние Legal Tech и определить направления его дальнейшего развития.

**Основная часть.** Вхождение в цифровую эпоху [1, С.11], эпоху четвертой промышленной революции, несомненно, отражается на нашей повседневной жизни и жизни общества в целом. С каждым годом технологии становятся все более неотъемлемой составляющей нашего бытия, а технологический прогресс влияет на все сферы общества, в том числе правовую.

Влияние технологического прогресса на юридическую деятельность проявляется в развитии популярного направления Legal Tech (правовые технологии). «Legal Tech – это разнообразные платформы, программы, продукты и инструменты, специально разработанные для упрощения и оптимизации процессов, составляющих профессиональную деятельность юристов» [2]. Это понятие включает в себя и применение искусственного интеллекта для юридических вопросов.

По мнению А. В. Минбалеева, «Legaltch это совокупность идей, технологий, решений, позволяющих реализовать, оптимизировать юридическую деятельность с использованием различных информационных технологий, решений и продуктов» [3].

Современное российское законодательство дает легальное определение этому понятию. В соответствии со статьей 2 Федерального закона № 123-ФЗ от 24.04.2020 «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных"», искусственный интеллект представляет собой совокупность технологических решений, которые позволяют имитировать когнитивные способности человека, включая способность к самостоятельному обучению и поиску решений без заранее заданного алгоритма действий, и достигать результатов, сопоставимых с результатами интеллектуальной деятельности человека при выполнении конкретных задач [4].

Сильный искусственный интеллект – это программы, которые отождествляются с сознанием человека и осознают себя как самостоятельные субъекты деятельности. В отличие от слабого искусственного интеллекта сильный наделен способностью мыслить абстрактно, способностью решать не только узкоспециализированные задачи, но и выходить за рамки этих задач. Этот вид искусственного интеллекта еще не создан и, по оценкам специалистов, он вряд ли появится в ближайшее время. По мнению экспертов, сильный искусственный интеллект появится только к 2075 году [5].

Слабый искусственный интеллект – это программы и сервисы, которые направлены на решение узкопрофильных задач. Это понятие включает в себя голосовых ассистентов, систему распознавания лиц, рекламу в социальных сетях и многое другое. Именно слабый искусственный интеллект на данный момент стоит рассматривать в качестве технологии, способной решать правовые задачи.

Слабый искусственный интеллект действует на основе датасетов – обработанной и структурированной в табличном виде информации. Датасеты являются основой машинного обучения искусственного интеллекта. В этом и заключается одна из основных проблем использования слабого искусственного интеллекта применительно к российской юриспруденции. Несмотря на это крупные юридические компании предпринимают попытки создания таких датасетов на основе имеющихся внутренних документов для решения правовых задач.

Существует множество вариантов применения слабого искусственного интеллекта в области Legal Tech. Основные из них:

- 1. Технологии по созданию правовых документов и актов.** Такие программы позволяют создавать типовые юридические документы, используя лишь входные данные пользователя. К примеру, американская компания LegalZoom [6] может создать черновой вариант завещания, пользователю лишь остается внести информацию о своем имуществе и о том, как пользователь хотел бы им распорядиться. В перспективе такие сервисы, используя уже существующую технологию блокчейн в качестве защищенного реестра хранения и передачи информации, смогут сделать услуги нотариуса более доступными для людей, так как для получения услуги даже не придется выходить из дома.

**2. Технологии по систематизации нормативных правовых актов и судебной практики.** В нашей стране представителями этой отрасли Legal Tech выступают справочно-правовые системы «Гарант», «Консультант», «Кодекс» и иные.

В России активно развивается «Единый портал государственных и муниципальных услуг» [7] – интернет-портал, содержащий справочную информацию.

Председатель Совета судей России Виктор Момотов сообщил о предстоящем запуске суперсервиса «Правосудие-онлайн» [8]. Судебный департамент при Верховном суде РФ уточнил, что разработка суперсервиса близится к завершению и скоро начнется тестирование [9].

**3. Технологии по распознаванию образов,** лиц, которые используются в правоохранительных органах. В 2021 году Россия вышла на второе место по темпу подключения видеокамер и уверенно удерживает третье место по общему количеству камер видеонаблюдения в мире [10]. Большое количество камер видеонаблюдения и использование слабого искусственного интеллекта позволило создать систему распознавания лиц и образов в крупных городах России, которая помогает обнаружить людей, находящихся в розыске. Так же искусственный интеллект с возможностью машинного обучения применяется в сочетании с камерами видеофиксации дорожных правонарушений, что позволяет не только наказывать недобросовестных водителей за нарушение правил скоростного режима, но и выявлять не пристегнутые ремни безопасности, использование мобильного телефона во время вождения автомобиля и другие правонарушения.

**4. Технологии, позволяющие анализировать правовые документы и на основе этих правовых документов осуществлять прогнозирование правовых результатов разбирательства.** В США команда политологов создала модель Верховного Суда США на базе искусственного интеллекта, которая на основе анализа прошлых решений вышеупомянутой судебной инстанции способна предсказывать с высокой вероятностью исходы дел [11]. Подобные модели были созданы для прогнозирования решений Европейского суда по правам человека, модель прогнозировала решения суда с 79 % точностью [12], а также для прогнозирования исходов патентных споров в судах США [13].

С учетом рассмотренного можно сделать вывод, что слабый искусственный интеллект уже успешно применяется в юридической деятельности, а перспективы его использования ограничиваются лишь техническим прогрессом. Закон Мура, лежащий в основе развития компьютерных технологий, говорит о том, что число транзисторов в интегральной схеме удваивается примерно каждые 18–24 месяца, что дает нам право предполагать, что уже в ближайшие годы появятся новые способы использования искусственного интеллекта в качестве правовой технологии.

Одним из таких направлений можно считать внедрение искусственного интеллекта в процесс судопроизводства. Автоматизировать судопроизводство полностью и заменить судью в этом процессе с учетом специфики слабого искусственного интеллекта предполагается невозможным.

Другим перспективным направлением является использование в юридической деятельности ставшего популярным за последние несколько ме-

саяцев алгоритма обработки естественного языка GPT-3,5, а точнее чат-бота ChatGPT, работающего на основе этого алгоритма. Данный чат-бот позволяет в диалоговом режиме отвечать на запросы, задаваемые пользователем. Функционал ChatGPT предоставляет возможность задать вопрос о перспективах его использования в юридической деятельности. По мнению ChatGPT, он как искусственный интеллект может быть полезен в юридической деятельности для решения ряда задач:

1. Обработка крупных объемов информации за короткий срок времени.
2. Проведение юридических консультаций и подготовка юридических документов.
3. Мониторинг изменений в законодательстве.
4. Помощь юристу в проведении консультаций.
5. Автоматизация рутинных процессов, такие как проверка сроков, подача документов.
6. Оказание поддержки в других задачах, связанных с работой юриста.

Важно отметить, что ChatGPT не видит себя в качестве замены квалифицированного юриста, отмечая, что его главная цель как одной из разновидностей LegalTech является помощь юристу в повышении эффективности его деятельности, оптимизации рутинных задач и повышении качества работы юриста.

Дополнительно стоит выделить еще одну перспективную сферу развития искусственного интеллекта в юридической деятельности. Искусственный интеллект позволит перейти от поиска, по ключевым словам, к смысловому поиску, который будет давать более точную информацию. Следующей за этим ступенью развития поиска информации в сети Интернет является интеграция чат-бота, например, ChatGPT, в поисковую систему. Это даст возможность получать не просто ссылки на соответствующую информацию, а сформулированные фразы, напоминающие реакцию живого человека на вопрос. Применительно к юридической деятельности это позволит более быстро и эффективно искать юридическую практику, нормы права, а также позволит получать ответы на интересующие обывателя юридические вопросы, которые будут сформулированы на понятном для пользователя языке.

Таким образом, анализируя представленную информацию, можно сделать вывод о том, что в ближайшие несколько лет слабый искусственный интеллект в качестве правовой технологии будет применяться для автоматизации большего количества правовых задач. Но юридические задачи, которые требуют умения мыслить абстрактно и наличия эмоционального интеллекта, скорее всего, не под силу автоматизировать при текущем уровне развития технологий искусственного интеллекта. Поэтому роль юриста в современном мире будет меняться. Юристам придется развивать творческие способности, чтобы находить решения для нестандартных задач, а искусственный интеллект будет использоваться в сочетании с этими навыками для оптимизации рутинных процессов.

### **Список литературы**

1. Корнев А. В. Дигитализация права: проблемы и перспективы // Актуальные проблемы российского права. – 2019. – № 6. – С. 11.

2. Рожкова М. А. LegalTech и LawTech – что это такое и в чем их значимость для права? // Закон.ру. 2020. 14 февраля. – URL: [https://zakon.ru/blog/2020/02/14/legaltech i lawtech %C2%A0что это такое i v c hem ih znachimost dlya prava](https://zakon.ru/blog/2020/02/14/legaltech_i_lawtech_%C2%A0что_это_такое_i_v_c_hem_ih_znachimost_dlya_prava)
3. Информационно-технологическое обеспечение юридической деятельности (LegalTech): учебник (коллектив авторов; под ред. д.ю.н., доц. А.В. Минбалева). – М.: «Проспект», 2022. – 368 с.
4. ФЗ от 24.04.2020 № 123 «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» // «Собрание законодательства РФ», 27.04.2020, № 17, ст. 2701.
5. Berruti F., Nel P. and Whiteman R. An executive primer on artificial general intelligence // McKinsey & Company April 29, 2020. – URL: <https://www.mckinsey.com/capabilities/operations/our-insights/an-executive-primer-on-artificial-general-intelligence>
6. LegalZoom // URL: <https://www.legalzoom.com/>
7. Госуслуги. – URL: <https://www.gosuslugi.ru/superservices>
8. Госуслуги. – URL: <https://www.gosuslugi.ru/superservices>
9. DIGITAL. – URL: <https://rg.ru/2023/03/20/posporim-na-gadzhetah.html>
10. Серебров Ю. TelecomDaily: Россия вышла на второе место по темпам подключения видеокamer // Telecom Daily 30 июня 2021 г. – URL: <https://telecomdaily.ru/news/2021/06/30/telecomdaily-rossiya-vyshla-na-vtoroe-mesto-po-tempam-podklyucheniya-videokamer>
11. Ruger T. W. et al. The Supreme Court Forecasting Project: Legal and Political Science Approaches to Predicting Supreme Court Decisionmaking // COLUM. L. REV., 2004, Vol. 104, p. 1150.
12. Aletras N., Tsarapatsanis D., Preotiuc-Pietro D., Lamos V. Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective. / PLOS ONE – №12 -Stanford. – 18 p.
13. Harbert T. Lex Machina Arms Corporate Leaders and Patent Attorneys with Predictive Analytics, DataInformed, 2012, June 6. – URL: <http://data-informed.com/lex-machina-arms-corporate-leaders-and-patent-attorneys-with-predictive-analytics/>

## ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВА ЧЕЛОВЕКА

**Е. С. Алехина,**

кандидат экономических наук, доцент,  
Донской государственный технический университет

**С. В. Надтока,**

кандидат юридических наук, доцент,  
Донской государственный технический университет

### ЦИФРОВИЗАЦИЯ ГУМАНИТАРНОЙ ДЕЯТЕЛЬНОСТИ В СИСТЕМЕ РАЗВИТИЯ ПРАВ ЧЕЛОВЕКА

**Аннотация.** Применение цифровых технологий в области гуманитарной помощи представляется значительным вкладом в развитие прав человека. Целью работы является изучение международного опыта цифровизации гуманитарной деятельности с выявлением проблемных аспектов. Анализ актуальных информационных технологий, онлайн-платформ и приложений, используемых в данной области, подтверждает эффективность достижений современности, однако наряду с этим возникают риски правонарушений в сфере обеспечения безопасности, конфиденциальности, здравоохранения и т. д. Решение выявленных проблем представляется возможным только за счет международного сотрудничества, открытого диалога и обсуждения с привлечением всех участников процесса гуманитарной деятельности.

**Ключевые слова:** гуманитарная помощь, права человека, цифровизация, устойчивое развитие, планирование, логистика, государственное регулирование

### DIGITALIZATION OF HUMANITARIAN ACTION IN THE HUMAN RIGHTS DEVELOPMENT SYSTEM

**Abstract.** The use of digital technologies in the field of humanitarian assistance seems to be a significant contribution to the development of human rights. The aim of this work is to study international experience of digitalization of humanitarian activities with the identification of problematic aspects. Analysis of current information technologies, online platforms and applications used in this area confirms the effectiveness of modern achievements but at the same time there are some risks of violation in the field of security, privacy, health care, etc. It is possible to solve the identified problems only through international cooperation, open dialogue and discussion with the involvement of all participants of the humanitarian process.

**Keywords:** humanitarian aid, human rights, digitalization, sustainable development, planning, logistics, governance

**Введение.** Цифровое развитие общества затрагивает все фундаментальные сферы деятельности человеческой жизни, трансформируя социум, культуру, политику, экономику и право. Гуманитарная активность не является исключением, поскольку применение цифровых технологий предоставляет огромные возможности для повышения эффективности гуманитарной практики, направленной на спасение жизней людей и содействие пострадавшим от вооруженных конфликтов, экономических кризисов, экологических бедствий и других условий.

Тема цифровизации гуманитарной деятельности является как никогда актуальной по нескольким причинам: глобальная неустойчивость в политических отношениях государств, отставание в социальноэкономическом развитии стран третьего мира, катастрофические проблемы окружающей среды и ряд иных факторов, провоцирующих потоки мигрантов и беженцев, ухудшающих здоровье людей и благополучие.

По своей природе гуманитарная деятельность направлена на защиту прав и свобод человека, однако в эпоху цифровизации эти процессы обнаруживают ряд вопросов, связанных с рисками и угрозами для всех членов цифрового мира.

В этой связи целью исследования является изучение международного опыта цифровизации гуманитарной деятельности с выявлением проблемных аспектов.

К задачам работы относится:

1. Выявить наиболее эффективные цифровые технологии, обеспечивающие гуманитарную помощь.
2. Обозначить влияние цифровизации на развитие системы защиты прав человека.
3. Изучить возможности решения проблем глобальной цифровизации.

На мировом уровне трансформация гуманитарной практики приводит к изменениям в способах оказания гуманитарной помощи [5]. Активно внедряется использование приложений для гуманитарной работы, социальных сетей, медиа-платформ и мобильных денег [3, С. 1], направленных на поддержку нуждающихся.

Однако, предоставляя новые возможности для общения и помощи в сложных ситуациях, цифровые технологии остаются недоступными для многих гуманитарных и волонтерских организаций, не обладающих соответствующими стандартами или согласованиями на международном уровне [3. С. 1].

**Основная часть.** Гуманитарное сообщество мирового масштаба всегда нуждалось в развитии и структуризации по нескольким причинам. Во-первых, количество людей, страдающих от различных бедствий и кризисов по всему миру, беспрестанно растет, что требует больших ресурсов и усилий со стороны регулятивных институтов. Во-вторых, координация деятельности гуманитарных организаций требует упорядочивания, выделения центра управления, четкого распределения полномочий и иных механизмов структуризации [1. С. 14–15].

Решением этих проблем является применение цифровых технологий, адаптация которых под волонтерские нужды помогает организовать иерархически сложенный процесс гуманитарной помощи.

Внедрение информационных систем, таких как гуманитарные приложения, способствует решению различных проблем в рассматриваемой области. Среди наиболее эффективных программ можно назвать следующее:

- Приложение 4w's (who, what, where, when) [3. С. 2] представляет собой геолокационное планирование для предоставления информации по организации гуманитарной помощи. Посредством данной программы возможно отслеживание лиц, оказывающих гуманитарную помощь и решение критических вопросов (кто, что, где и когда);

- Платформа KoBoToolbox [6] позволяет собирать, обрабатывать и хранить гуманитарную информацию с мобильных устройств и сетевых приложений;

- Приложение MigApp для помощи мигрантам, предоставляет бесплатный доступ к информации, программам и услугам, значимым в процессе миграции [3. С. 28].

- Платформа TraceRx может использоваться для налаживания цепочки поставок гуманитарной помощи при чрезвычайных ситуациях [3. С. 2].

- Мессенджеры (WhatsApp, Viber, WeChat, Kakao Talk и т. д.) позволяют пользователям практически при любых условиях отправлять и получать данные в более широком объеме, чем посредством мобильной связи [3. С. 2].

Обозначенные инструменты предоставляют пользователям современные и оперативные решения в области гуманитарной деятельности, а также «способствуют координации реагирования и коммуникации между пострадавшими сообществами, волонтерами и работниками по оказанию помощи, чтобы обеспечить интегрированную цифровую среду для прозрачной и своевременной гуманитарной помощи» [3. С. 2].

Однако для решения комплексных задач, включающих в себя логистику, системы снабжения, предотвращение и ликвидация разного рода бедствий, в дополнение с общими информационными системами, требуются специальные структуры материально-технического обеспечения [5. С. 263].

С целью принятия стратегических решений и усиления логистического кластера в международной гуманитарной практике реализуются такие технологические инструменты, как UN-OCHA LogIK Tool [5. С. 268], предоставляющий информацию о том, какие вещи и продукты были доставлены в необходимое местоположение, чтобы поставщики могли отслеживать гуманитарные потоки.

Применение информационных технологий, распространяющих данные об основных узлах и линиях распределения, запросах на гуманитарное обслуживание и другие операционные процедуры, является ключевым элементом в выстраивании гуманитарной системы. Указанная информация передается посредством Reliefweb или Humanitarian Response [5, С. 268] и иных информационных платформ, предоставляющих доступ к инфографике и отчетности о гуманитарной деятельности.

Использование беспилотных летательных аппаратов или дронов отличается широким спектром действий: доставка посылок и предметов первой необходимости в труднодоступные локации, мониторинг и оценка ущерба, отслеживание экологических катастроф в кризисных зонах, поиск пострадавших лиц и т. д. [3. С. 3].

По своей сути применение обозначенных технологических инструментов направлено на развитие доступности гуманитарной помощи, оповещение общественности и усовершенствование подотчетности путем предоставления данных, документации, функций мониторинга и отслеживания. Кроме того, предоставление конкретных задач по принятию решений, поддержки системы управления (например, маршрутизация и навигация), материально-техническому снабжению, а также планированию местоположения или распределения заданий невозможно без использования цифровых технологий и аппаратов.

Как отмечалось выше, гуманитарная практика является частью более широкой системы защиты прав и свобод человека, в связи с чем, развитие данного сектора имеет значительное влияние на всю правовую систему.

В качестве основного требования к обеспечению прав и интересов граждан выдвигается поддержание безопасности, здравоохранения, благоприятной окружающей среды, культурной идентичности и конфиденциальности. К сожалению, стремительное технологическое развитие не всегда способствует этому.

В этом контексте возникают вопросы о защите личных данных и информации, передаваемой посредством приложений и онлайн-платформ, а также метаданных, реализуемых в рамках гуманитарной деятельности.

«Все стороны, участвующие в оказании гуманитарной помощи, должны понимать важность необходимости предотвращения утечки персональных данных и нарушений неприкосновенности частной жизни, поскольку потенциальные негативные последствия для жизни и прав людей являются значительными» [3. С. 5].

Наиболее эффективным решением в данном случае является международное обсуждение проблемы гуманного использования цифровых технологий в реализации гуманитарной активности с целью развития принципов терпимости, нейтралитета и беспристрастности в отношении частной жизни других людей и сообществ.

**Заключение.** Исследование международного опыта применения цифровых технологий в гуманитарной деятельности позволяет выявить как преимущества, так и недоработанные аспекты, которые могут приводить к значительным нарушениям в области прав человека.

Игнорирование этих вопросов, как и отказ от технологических инноваций, представляет угрозу в процессе жизнеобеспечения миллионов людей, страдающих от разного рода кризисов. Поэтому современное включение цифровых инструментов в гуманитарную активность и защиту прав граждан должно сопровождаться активной поддержкой политиков, обсуждениями между мировыми лидерами и гуманитарными организациями, активным участием представителей различных структур (поставщики услуг, волонтеры, представители общественности, социальные организации и т. д.) с целью формализации нормативных требований, поддержания безопасности и предотвращения киберугроз.

### Список литературы

1. Борисов А. В. Гуманитарная система ООН: кризис, возможности и позиция России // Мировая политика. – 2023. – № 1. – URL: <https://cyberleninka.ru/article/n/gumanitarnaya-sistema-onn-krizis-vozmozhnosti-i-pozitsiya-rossii>
2. Гайнутдинова Е. И. Роль ООН в цифровизации информации и гуманитарных услуг для мигрантов во всем мире // Горизонты гуманитарного знания. – 2020. – № 5. – URL: <https://cyberleninka.ru/article/n/rol-onn-v-tsifrovizatsii-informatsii-i-gumanitarnyh-uslug-dlya-migrantov-vo-vsem-mire>
3. Akhmatova Dz. M., Akhmatova M. S. Promoting digital humanitarian action in protecting human rights: hope or hype // Journal of International Humanitarian Action. – 2020. – № 5. – DOI:10.1186/s41018-020-00076-2.
4. Casswell J., Hamilton Z. Navigating the shift to digital humanitarian assistance. 2019. – URL: <https://www.rescue.org/resource/navigating-shift-digitalhumanitarian-assistance>
5. Comes T., de Walle B. V. Information systems for humanitarian logistics. Supply chain management for humanitarians: tools for practice // Kogan Page. – London. – 2016. – Pp. 257–284.
6. Olajide V. Data Collection with KoboToolbox. – 2019. – URL: [https://www.researchgate.net/publication/335147345\\_Data\\_Collection\\_with\\_KoboToolbox](https://www.researchgate.net/publication/335147345_Data_Collection_with_KoboToolbox)

**К. О. Беляков,**

Российский государственный художественно-промышленный  
университет имени С. Г. Строганова,  
Национальный исследовательский  
Томский государственный университет

**Е. Н. Ирискина,**

студент,  
Национальный исследовательский  
Томский государственный университет

### КЛАССИФИКАЦИЯ КОЛОНИАЛЬНЫХ ОБЩЕСТВ ПО ТИПАМ ФОРМИРУЕМЫХ ЗАВИСИМОСТЕЙ И ВОПРОСЫ ДЕЛЕГИРОВАНИЯ СУБЪЕКТНЫХ ПРАВ ЦИФРОВЫМ ДВОЙНИКАМ

**Аннотация.** В связи со стремительным развитием искусственного интеллекта, усилением зависимости людей от платформ с искусственным интеллектом, уходом жизни в виртуальный мир, появляется много проблем технического и этического характера, в том числе все более актуальной становится угроза появления новых форм и типов колониализма. В статье показаны пути «мягкого, безболезненного» понуждения и формирования зависимостей с добровольной передачей субъектных прав граждан, а также способы и возможные пути предотвращения с использованием существующих юридических механизмов.

**Ключевые слова:** метавселенная, искусственный интеллект, интеллектуальные роботы, автономные роботы, интеллектуальные помощники, интеллектуальные импланты, неокOLONиализм, колониализм

## CLASSIFICATION OF COLONIAL SOCIETIES BY TYPES OF FORMED DEPENDENCIES AND ISSUES OF DELEGATING SUBJECT RIGHTS TO DIGITAL COUNTERPARTS

**Abstract.** Due to the rapid development of artificial intelligence, the increasing dependence of people on artificial intelligence platforms, and the withdrawal of life into the virtual world, many technical and ethical problems are emerging, including the threat of new forms and types of colonialism. The authors show ways of “soft, painless” coercion and the formation of dependencies with the voluntary transfer of subjective rights of citizens, as well as methods and possible ways of prevention using existing legal mechanisms.

**Keywords:** metaverse, artificial intelligence, intelligent robots, autonomous robots, intelligent assistants, intellectual implants, neocolonialism, colonialism

**Введение.** Впервые слово «метавселенная» было упомянуто писателем Нилом Стивенсоном в 1992 году в литературном произведении «Лавина» [1]. Под «метавселенной» Нил Стивенсон понимал следующую стадию развития Интернета, а именно «...общий цифровой мир, объединяющий физическую, дополненную и виртуальную реальности...» В настоящее время понятие «метавселенная» получило широкую популярность и употребляется довольно часто и встречается почти во всех сферах жизни общества. Крупные корпорации, такие как Meta<sup>2</sup> – запрещенные организации в Российской Федерации) Microsoft, заявляют о своем видении метавселенной, ее создании и развитии. Метавселенная от Meta уже расширилась в 100 странах [2]. Виртуальный мир входит как в жизнь общества, так и в жизнь каждого отдельного человека.

**Основная часть.** В метавселенной проходят выступления артистов, например, 29 августа 2022 года Snoop Dogg и Eminem выступили в метавселенной The Otherside Metaverse, используя своих цифровых двойников [3].

Банки уже уверенно вошли в метавселенную. Согласно анализу Citi [4], к 2030 году экономика метавселенной может вырасти до \$13 трлн. А Goldman Sachs и Morgan Stanley заявили, что у метавселенной есть рыночные возможности вырасти на \$8 трлн, в то время как JPMorgan считает, что у «метаверс» есть ежегодный потенциал роста на \$1 трлн. В настоящее время банки предлагают потребителям огромный выбор универсальных услуг в виртуальном мире, поскольку виртуальная сфера продолжает сливаться с физическим миром, имитируя повседневные потребности от покупок и игр до финансовых практик и государственных услуг. В августе 2022 года Decentraland запустил первый банкомат в своей метавселенной [5]. В партнерстве со студией Metaverse Architects и платежным шлюзом Transak потребители могут воспользоваться банкоматом для

<sup>2</sup> Мета – организация признанная экстремистской, ее деятельность запрещена на территории Российской Федерации.

покупки криптовалюты в метавселенной, как в физическом мире. Владельцы недвижимости в Decentraland имеют возможность добавить банкомат на свою виртуальную землю для легкого доступа к криптовалюте – так же, как учреждение в физическом мире.

Банк открыл [6] виртуальный зал ожидания в Decentraland – Onyx Lounge, названный в честь платежной системы JPMorgan, работающей на блокчейне. JPMorgan стал первым банком, открывшим офис в метавселенной. «Метавселенная, вероятно, проникнет в каждый сектор в ближайшие годы, а рыночные возможности оцениваются в более чем \$1 триллион годового дохода, а также подчеркивается, что уже потрачено \$54 млрд в год на виртуальные товары – это в 2 раза больше суммы, потраченной на покупку музыки», – согласно отчету JPMorgan [6]. В документе JPMorgan отмечается, что средняя стоимость виртуальной земли подорожала в 2 раза с \$6000 до \$12 000 в период с июня по декабрь 2021 года, и прогнозируется, что к 2027 году расходы на внутриигровую рекламу достигнут \$18,4 миллиарда в год. JPMorgan определил стремление отдельных авторов использовать Web3 для монетизации своей работы новыми способами как движущую силу новой экономики, строящейся в метавселенной. «Эта экономика собственности в сочетании с возможностью взаимодействия может открыть огромные возможности, благодаря которым цифровые товары и услуги больше не будут привязаны к одной игровой платформе или бренду». JPMorgan отметил, что все более широкое внедрение метавселенной также обусловлено интересом со стороны крупных брендов, сославшись на шаг Adidas и Nike по созданию NFT, а также открытие Samsung магазина метавселенной в качестве огромного шага вперед в этом направлении [7]. Крупнейший банк Великобритании HSBC, сразу после JPMorgan, купил участок виртуальной земли в метавселенной Sandbox для взаимодействия с поставщиками финансовых услуг и привлечения спортивных сообществ [8].

На уровне всемирной организации интеллектуальной собственности обсуждаются вопросы регистрации товарных знаков в метавселенной [9, 10]. В марте 2022 года American Express зарегистрировала товарные знаки для виртуального рынка и криптоуслуг в метавселенной. Цифровой банк Quontic предлагает банковские услуги в своих виртуальных офисах. Их дебетовая карта, выпущенная в апреле, предлагает счета в BTC в дополнение к наличным и текущим счетам с высокой процентной ставкой. Через банкомат посетители могут открыть банковский счет, чтобы принять участие в вечеринке мета-пула и получить бесплатный NFT. Другой цифровой банк, Cogni, купил этим летом коллекцию NFT у яхт-клуба Bored Ape и создает дебетовую карту Bored Ape для новых сервисов Web3 для клиентов [11].

Правительство Китая планирует контролировать метавселенную вплоть до развития собственной парадигмы – так называемой «метавселенной Китая» или Chinaverse [12].

Метавселенная становится искусственно созданным пространством, где биологический человек приравнен по правам в метавселенной к своему цифровому двойнику и взаимодействует как субъект с другими цифровыми двойника-

ми и искусственными ботами, цифровыми субъектами, созданными искусственным интеллектом (далее – ИИ).

Эти взаимоотношения и взаимозависимости в виртуальных пространствах становятся новой реальностью для жизнедеятельности людей, и с одной стороны – новыми возможностями, а с другой – новыми вызовами и опасностями.

В статье предпринята очень краткая попытка исследования взаимодействия человека в современном мире с возможностями «существования и ограниченной жизнедеятельности» в виртуальных пространствах с делегированием субъектных прав своим цифровым двойникам и на основании этих исследований дана попытка классифицировать типов колониализма выделив четыре типа.

**Биологический интеллект и искусственный интеллект.** Согласно теории триединого мозга Пола Маклина, биологический мозг человека условно состоит из трех частей: древний глубинный мозг рептилий, мозг млекопитающих – «лимбическая система» и неокортекс, отвечающий за биологический интеллект [13]. Таким образом, мозг человека имеет функционал: безусловного автомата – инстинкты в мозге ящеров, автомата с условиями – работает как функция от множества аргументов, творческий – долго ищет соответствия и может принять нетривиальное креативное решение.

Теория триединого мозга имеет непосредственную связь с метавселенной. Метавселенная, вернее технологии, применяемые в киберпространстве, ожидаемо будут работать с человеком ориентируясь на его инстинкты желаний и обходить встроенные инстинкты опасностей – фактически вводя человека в состояние «живой функции» – работая на свои потребности, эксплуатируя человека.

Ожидаемо для технологий управления – использовать и работать именно с глубинным мозгом человека, работая с инстинктами, «неконтролируемыми» или «мало осознаваемыми» реакциями человека. История взлета и падения компании Cambridge Analytica, вплоть до осуждения, запрета и банкротства – это только один из публичных примеров работы технологий ИИ с инстинктами человека [14; 15].

Мэтью Болл, закрепивший за собой звание идеолога метавселенной выделил весь спектр основных черт, которые отличают метавселенную от Интернета и онлайн-игр [16]: бесконечное существование; существование в реальном времени и независимость от внешних факторов; нет ограничений по количеству человек; существование экономики внутри; объединение физическое и виртуального мира в единый целый мир; совместимость данных; наполненность контентом и опытом.

Метавселенные – это современные площадки взаимодействия человека с новым для себя пространством с неизведанными для биологического человека новыми свойствами и возможностями, одновременно угрозами и опасностями.

**Колониализм.** Общеизвестно, что по типу управления, заселения и хозяйственного развития в истории колониализма выделилось три основных вида колоний:

1. Переселенческие колонии.
2. Сырьевые колонии (или эксплуатируемые колонии).
3. Смешанные (переселенческо-сырьевые колонии).

Введем классификацию колониальных обществ по типам формируемых зависимостей: переселенческие и сырьевые, финансовые, технологические, правовые.

**Колониальное общество 1.0.** Колониальное общество версии 1.0 представляет собой эксплуатацию колоний метрополиями. Достаточно глубоко исследовано, в том числе постколониальной теории (постколониализм) и неокOLONиализма.

«Неоколониализм – система подчинения и эксплуатации развитыми капиталистическими государствами молодых неразвитых стран и экономик, в том числе недавно освободившихся из колониальной политической зависимости, с помощью неравноправных экономических и прямых военно-политических отношений и договоров в связи с полной несостоятельностью прежней колониальной системы и краха колониальных империй как результата возникновения и развития СССР и стран социалистического лагеря» [17]. Вторично «расцвел» после «разгрома соцстран» (Ф. Кастро) и Советского Союза в 1990-е и нулевые годы [18].

Эгоистическое отношение бывших метрополий по отношению к бывшим своим колониям – никуда не может исчезнуть, если отношения формируются не на равных условиях и в неравном соотношении к технологическому и экономическому уровню.

Как и глобальное разделение труда с признаками неравного соотношения технологического и экономического уровней государств в построении неравных отношений, так и «колонизаторский опыт» бывших метрополий создают условия появления и проявления признаков эксплуатации в формате неокOLONиализма.

Разрыв в технологическом уровне с поддержкой экономических ресурсов формирует отношения, позволяющие эксплуатировать «технологические и сырьевые колонии» более мягкими способами, иногда для эксплуатируемых выглядящие как благо «высших цивилизаций».

**Псевдоколониальное общество 2.0.** Современное финансовое управление (Бреттон-Вудское, а следом – Ямайское соглашение финансового управления) сформировали условия добровольной передачи суверенных прав государственных финансовых механизмов на уровень «финансовой метрополии», которая обязалась быть «справедливым финансовым институтом» для всех участников.

В результате благодаря юридической передаче части суверенных прав государства легитимно и собственной воле лишились права быть на равных по отношению к вышестоящему по рангу институции, структуре власти в иерархии. Сформировались отношения, которые позволяют манипулировать и управлять, формируя тем самым возможность эксплуатировать финансовыми ресурсами «экономических колоний».

Текущая ситуация ярко показывает два элемента:

1. Суверенную добровольную передачу прав по обстоятельствам. И нам будет полезно изучить эти обстоятельства и как они возникают на примере не только государств, но и на уровне граждан.

2. Мягкую эксплуатацию с помощью части переданных субъектных прав другому, когда такая эксплуатация выглядит как благо. Но по сути является инструментом эксплуатации «финансового или технологического суверена».

Для целей настоящей статьи под «субъектным правом» будем понимать право принимать решения от имени своего, нотариально, либо иным способом закрепленные, то есть некое эксклюзивное делегирование полномочий. Авторами предлагается разделять субъективные права известные юридической науке и субъектное право. В частности, Л. И. Глухарева «под субъективными правами понимает специальную юридическую категорию, которая выражает формально закрепленные, т. е. прошедшие надлежащую правотворческую процедуру и поэтому гарантированные государством, полномочия физических и юридических лиц; эти полномочия открывают не потенциальные, а реальные (гарантированные) возможности действовать определенным образом и добиваться желаемых целей и благ» [17]. Несмотря на то, что по общему правилу права человека неотчуждаемы, их нельзя купить или передать по наследству, человек может осуществить «отчуждение» прав, попав в полную зависимость.

На данном этапе искусственный интеллект является слабым, виртуальные помощники используются для простейших функций, а роботы используются как инструменты.

**Колониализм 3.0.** Колониализм 3.0 – это технологическая несuverенность цифровых колоний по национальному и территориальному принципу.

Развитие искусственного интеллекта идет быстрыми темпами, а развитие креативных способностей современного человека замедляется. Человек все больше и больше становится зависимым от цифровых систем, таких как виртуальные помощники, цифровые ассистенты, которые берут на себя все более сложные функции.

Вторые со временем становятся уязвимыми и зависимыми от первых. В процессе технологического разрыва не способны на организационном уровне, поддерживать уровень знаний, способный понимать и осознавать суть происходящего. И в конечном счете, становятся подконтрольными сообществами, управляемыми, – становятся в ранг «технологических колоний».

Формирование таких «технологических метрополий» и «технологических колоний» формирует принципы «колониализма 3.0» – колониализма, основанного на технологическом несuverенитете подконтрольных сообществ, компаний, государств, территориальных объединений.

**Колониализм 4.0.** На текущем уровне развития общество находится на этапе развития, когда не человек говорит виртуальному ассистенту, что делать, а виртуальный ассистент, анализирует поведения человека, «диктует» человеку, что ему стоит делать.

На данном этапе происходит делегирование полномочий с целью обеспечения комфорта и уход в метавселенную.

Первоначально, человек имеет желание делегировать только часть своих полномочий умному ассистенту, чтобы облегчить свою жизнь. Это может быть контроль оплаты подписок или услуг ЖКХ. Затем искусственный интеллект сам начинает подбирать подписки и настойчиво предлагать человеку подписаться или даже подписывать человека на какие-то сервисы, в зависимости от предоставленных ему полномочий. В подобной ситуации, человек, его права и свободы, находятся под угрозой колонизации, возникает угроза Колониализма 4.0.

Происходит в тот момент, когда человек передает свои права и полномочия в принятии решений **«сервисам с технологиями искусственного интеллекта»**. На этом этапе развития отношений искусственный интеллект начинает управлять людьми, передавших ему свои субъектные права. Человек добровольно лишает себя своих прав на принятие решений от имени себя.

Процесс передачи простых функций от человека к интеллектуальному персональному помощнику происходит уже сейчас. Мы легко соглашаемся на передачу рутинных задач своим ассистентам. Процесс передачи происходит на условиях доверия. Но кто из граждан оформил эти отношения юридическим путем? Какие из прав переданы легально, и можно ли их отозвать на законных основаниях? И если ваш персональный ассистент с технологиями искусственного интеллекта на протяжении нескольких лет исправно выполнял порученные ему функции, возложенные на него обязательства, то в мире экономических отношений и технологий ваш цифровой двойник имеет более высокий статус доверия, нежели гражданин, передавший эти права. Возникают условия, при которых доверитель попадает в зависимость от ведомого, но уполномоченного цифрового двойника – интеллектуального ассистента. При передаче прав в пограничных условиях накопленным итогом – возникает опасность потери субъектности гражданина по отношению к субъектности его цифрового ассистента с возложенными на него правами.

Говоря о субъектности, мы говорим о человеке как о субъекте права, а также о цифровом ассистенте как о субъекте права, что пока является не признанным на законодательном уровне, несмотря на наличие публикаций о субъектности сильного искусственного интеллекта [20]. По мнению авторов Д. Б. Абушенко, К. Л. Брановицкий, С. К. Загайнова, «применительно к человеку субъектность, как правило, обосновывается либо дескриптивно – через атрибутивные свойства человеческого сознания (воля, способность к мышлению, к автономному принятию решений, самосознание), либо посредством аксиологического подхода – через репрезентацию в праве системы ценностей, во главе которой стоит человек» [21]. Д. И. Степанов рассматривает субъектность в смысле самостоятельной воли, разума, устремлений и предпочтений [22].

Для многих людей принятие оферты становится рутинной, и они не изучают соглашения, передавая свое субъектное право. Для примера разберем «Условия использования голосового помощника «Алиса»» [23].

Потребитель должен постоянно самостоятельно отслеживать изменения в соглашении. «Яндекс» вправе внести изменения в любой момент, без уведомления потребителя.

Ассистент, основанный на искусственном интеллекте, и самообучается. За любое такое обучение «Яндекс» ответственности не несет. Потребитель пользуется голосовым помощником и обучает его под свою ответственность.

Таким образом, «Яндекс» предоставляет потребителю искусственный интеллект и не несет никакой ответственности за совершение сделок от имени потребителя.

Стандартное ограничение ответственности.

Таким образом, соглашение, содержащее условия использования голосового помощника, не предусматривает возможности согласования условий, выбора тех или иных полномочий для передачи, ограничений таких полномочий,

а также не предусматривает ответственности правообладателя интеллектуального ассистента за действия ассистента. Потребитель не уделяет должной заботливости и осмотрительности при заключении такого соглашения и делает первый шаг в отчуждение своих субъектных прав.

Это **признаки мягкого колониализма нового, четвертого уровня**. Происходит модификация человека искусственным интеллектом. Человек отказывается от потребления в физическом мире, переходя к потреблению в мире виртуальном. «В будущем физический труд станет выбором», – сказал Илон Маск на Tesla AI day, добавив, что когда-нибудь это приведет к всеобщему базовому доходу [24].

Что заставляет человека передавать часть своих суверенных прав?

1. Удобство сервисов.
2. Недостаток времени на выполнение рутинных функций.
3. Необходимость освобождения свободного времени.
4. Псевдодоверие или условная надежность цифровых интеллектуальных помощников.
5. Лень.
6. Оптимизация ресурсов.

Как происходит передача прав, где граница, за которой человек принимает решение о добровольной передаче своих прав своему искусственному помощнику?

Где грань добровольного процесса передачи? Или принудительного процесса – что является инструментом для вынужденной передачи прав? или понуждения к передаче? Почему соглашения об использовании персональных ассистентов заключаются в форме акцепта оферты и не дают возможность выбора и согласования условий? Потребитель должен помнить о своих правах, внимательно изучать соглашения, размещенные в сети интернет для использования интеллектуальных помощников, пытаться согласовать их на приемлемых для него условиях или вовсе отказываться от заключения таких соглашений. В случае массового отказа от заключения таких сделок правообладатели начнут составлять взаимные соглашения, основанные на принципах права. Пока пользователи заключают соглашения на кабальных для себя условиях, правообладатели будут пользоваться положением сильной стороны и принуждать к заключению таких соглашений.

Необходимо ввести критерии и пороговые значения в таблицу с градацией степени передачи субъектных прав и, соответственно, зависимостей человека от искусственного интеллекта.

Авторы статьи считают необходимым подготовить основу для правоприменения законодательных актов об обязательности включения «возможности отзыва полномочий и переданных прав» от интеллектуальных сервисов и персональных ассистентов. Законодательно обязать разработчиков предусмотреть техническую возможность при наступлении волеизъявления субъекта прав вернуть переданные права от ассистентов к гражданину, не расторгая при этом соглашения об использовании персонального ассистента.

Авторами статьи предлагается вариативная (изменяемая во времени и введением новых типов зависимостей) таблица, в которой ввести в использование условной градации степени зависимости человека от правового ограничения «управляющей системы» от переданных субъектных/субъективных прав.

| Степень зависимости человека | Мотивация человека передать субъектные права                               | Вариативный набор переданных прав                                              | Условная зависимость, % | Перечень инструментов в выходе из зависимости                                                         |
|------------------------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------|-------------------------|-------------------------------------------------------------------------------------------------------|
| Полная свобода               | Все делать самому                                                          | Ничего не передавать                                                           | 0                       | Не требуется                                                                                          |
| Условная свобода 1 рода      | Удобство                                                                   | Право на совершение оплаты услуг ЖКХ, регулярных сервисов                      | 10                      | Заявление человеком об отзыве переданных полномочий «простым кликом» оператору услуг                  |
| Условная свобода 2 рода      | Недостаток времени                                                         | Право на оплату подписок и услуг ЖКХ, регулярных сервисов оплат и действий     | 20                      | Заявление человеком об отзыве переданных полномочий «простым кликом» оператору услуг                  |
| Условная свобода 3 рода      | Необходимость освобождения свободного времени                              | Право на оплату подписок, услуг мобильной связи и услуг ЖКХ                    | 30                      | Заявление человеком об отзыве переданных полномочий                                                   |
| Условная зависимость 1 рода  | Лень, оптимизация ресурсов                                                 | Передача регулярных сервисов оплат и действий                                  | 40                      | Заявительная форма отказа от соглашений по переданным правам путем простого заявления оператору услуг |
| Условная зависимость 2 рода  | Оптимизация ресурсов                                                       | Передача регулярных сервисов оплат и действий, регулярных сторонних транзакций | 50                      | Заявительная форма отказа от соглашений по переданным правам путем простого заявления оператору услуг |
| Условная зависимость 3 рода  | Оптимизация ресурсов, желание оградить от рутинных процессов               | Передача всех сервисов оплат и сторонних действий                              | 60                      | Заявительная форма отказа от соглашений по переданным правам путем простого заявления оператору услуг |
| Зависимость 1 рода           | Псевдодоверие или условная надежность цифровых интеллектуальных помощников | Право выбора некоторого количества услуг, товаров, частичное заключение сделок | 70                      | Заявительная форма отказа от соглашений по переданным правам в государственные судебные инстанции     |

| Степень зависимости человека | Мотивация человека передать субъектные права                                                                                        | Вариативный набор переданных прав                                                                                            | Условная зависимость, % | Перечень инструментов в выходе из зависимости                                                                                                             |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Зависимость 2 рода           | Нежелание думать                                                                                                                    | Право выбора всех услуг, товаров, частичное заключение сделок                                                                | 80                      | Заявительная форма отказа от соглашений по переданным правам в государственные судебные инстанции с возможностью только частичного отзыва переданных прав |
| Зависимость 3 рода           | Нежелание думать, выбирать, принимать решения                                                                                       | Право выбора всех услуг, товаров, заключение всех сделок                                                                     | 90                      |                                                                                                                                                           |
| Полная зависимость           | Полный уход в правовую зависимость от технологически х компаний верхнего управляющего уровня (метавселенную правового колониализма) | Полное право принимать все решения за человека, заключать все сделки, соглашения и обеспечивать все функции жизнеобеспечения | 100                     | Невозможность вернуться на уровень субъекта.                                                                                                              |

Предлагается разделить на три условных больших уровня «Условная свобода», «Условная зависимость» и «Зависимость» человека, каждый из которых подразделяется на уровни 1–3 рода (которые, в свою очередь, можно разделять на более мелкие или частные случаи), которые можно будет рассмотреть в дальнейших работах или последователями этой статьи.

«Условная свобода» – интервал, когда человек пользователь легко может отказаться от сервисов оператора услуг и отозвать переданные полномочия «условным кликом» или указанием соответствующей «галочки» в приложении оператора услуг.

«Условная зависимость», в этом интервале формируется условная зависимость человека от работы с виртуальными помощниками и сервисами, – на этом уровне у человека формируется часть зависимостей, от которых он легко может избавиться, приняв личное решение начать отказываться от делегирования своих полномочий внешним сервисам.

«Зависимость» – в этом диапазоне уровней у человека возникают сложности с отзывом делегированных прав и человек попадает в критическую зависимость от действий по отношению к нему самому и к другим субъектам сообще-

ства людей и инфраструктуры, институтов власти государства – этот интервал зависимости человека крайне критичен, вплоть до стапроцентной зависимости – т. е. потери субъектности человека.

**Заключение.** Предложенные авторами варианты мотивации человека передавать субъектные права, а также набор переданных прав приведены в качестве примера, являются дискуссионными и могут меняться в зависимости от одного субъекта права к другому.

Таким образом, в работе показаны предпосылки:

- 1) создания форм технологических и экономических инструментов подчинения и эксплуатации развитыми государствами по отношению к менее развитым государствам и сообществам;
- 2) создания форм технологических и экономических инструментов подчинения и эксплуатации технологическими платформами интеллектуальных сервисов по отношению к гражданам.

### Список литературы

1. Стивенсон Н. Лавина. – М.: Fanzon: 2019. – 544 с.
2. Метавселенная Цукерберга сегодня расширилась в 100 странах: Африки, Азиатско-Тихоокеанского региона, Ближнего Востока и США [Электронный ресурс]. – URL: <https://t.me/blockchainRF/6640>
3. Все о блокчейн, мозге и WEB 3.0 в России и мире [Электронный ресурс]. – URL: <https://t.me/blockchainRF/6637>
4. METAVERSE AND MONEY Decrypting the Future March 2022 [Электронный ресурс]. – URL: <https://ir.citi.com/gps/x5%2BFOJIT3BoHXVu9MsqVRoMdiws3RhL4yhF6Fr8us8oHaOe1W9smOy1%2B8aaAgT3SPuQVtwC5B2%2Fc%3D>
5. Banking in the metaverse, August 15, 2022. [Электронный ресурс]. – URL: [https://www.wundermanthompson.com/insight/banking-in-the-metaverse?j=112774&sfmc\\_sub=37402851&l=65\\_HTML&u=6724445&mid=110005021&jb=11004](https://www.wundermanthompson.com/insight/banking-in-the-metaverse?j=112774&sfmc_sub=37402851&l=65_HTML&u=6724445&mid=110005021&jb=11004)
6. \$1T opportunity: JPMorgan becomes first major bank in the metaverse [Электронный ресурс]. – URL: <https://cointelegraph.com/news/1t-opportunity-jpmorgan-becomes-first-major-bank-in-the-metaverse>
7. JPMorgan стал первым крупным банком в метавселенной [Электронный ресурс]. – URL: <https://t.me/blockchainRF/5435>
8. HSBC to Become The First Global Financial Services Provider to Enter The Sandbox [Электронный ресурс]. – URL: <http://bit.ly/TSBxHSBC>
9. ВОИС Журнал 1/2022 Товарные знаки в метавселенной [Электронный ресурс]. – URL: [https://www.wipo.int/wipo\\_magazine/ru/2022/01/article\\_0006.html](https://www.wipo.int/wipo_magazine/ru/2022/01/article_0006.html)
10. ВОИС Журнал 2/2022 Метавселенная, NFT и права ИС: регулировать или не регулировать? [Электронный ресурс]. – URL: [https://www.wipo.int/wipo\\_magazine/ru/2022/02/article\\_0002.html](https://www.wipo.int/wipo_magazine/ru/2022/02/article_0002.html)
11. Банки вошли в метавселенную с уверенностью [Электронный ресурс]. – URL: <https://t.me/blockchainRF/6602>

12. Метавселенная в Китае подвергнется государственному контролю [Электронный ресурс]. – URL: <https://www.sostav.ru/publication/metaverse-vs-chinaverse-55760.html>
13. Маклин, Пол Д. Трехединый мозг в эволюции: роль в палеоцеребральных функциях/ Пол Д. Маклин. – Springer Science & Business Media: 1990. – 672 с.
14. Как Cambridge Analytica «взламывала выборы» по всему миру [Электронный ресурс]. – URL: <https://tass.ru/mezhdunarodnaya-panorama/5048632>
15. Компания Cambridge Analytica [Электронный ресурс]. – URL: [https://ru.wikipedia.org/wiki/Cambridge\\_Analytica](https://ru.wikipedia.org/wiki/Cambridge_Analytica)
16. The Metaverse: What It Is, Where to Find it, and Who Will Build It [Электронный ресурс]. – URL: <https://www.matthewball.vc/all/themetaverse>
17. НеокOLONиализм [Электронный ресурс]. – URL: <https://ru.wikipedia.org/wiki/НеокOLONиализм>
18. Ломагин Н. А., Сутырин С. Ф. НеокOLONиализм [Электронный ресурс]. – URL: <https://bigenc.ru/economics/text/2259736>
19. Глухарева Л. И. Субъективные права, основные права, права человека: единство и различия // Вестник РГГУ. Серия «Экономика. Управление. Право». – 2009. [Электронный ресурс]. – URL: <https://cyberleninka.ru/article/n/subektivnye-prava-osnovnye-prava-prava-cheloveka-edinstvo-i-razlichiya-1>
20. Спицин И. Н., Тарасов И. Н. Использование искусственного интеллекта при отправлении правосудия: теоретические аспекты правовой регламентации (постановка проблемы) // Актуальные проблемы российского права. – 2020. – № 8. – С. 96–107.
21. Актуальные проблемы гражданского и административного судопроизводства / Д. Б. Абушенко, К. Л. Брановицкий, С. К. Загайнова [и др.]; под ред. В. В. Яркова. – М.: Статут, 2021. – 460 с.
22. Степанов Д. И. Недействительность корпоративных решений: статьи по проблемным вопросам. – М.: Статут, 2021. – 284 с.
23. Условия использования голосового помощника «Алиса» [Электронный ресурс]. – URL: [https://yandex.ru/legal/alice\\_termsofuse/](https://yandex.ru/legal/alice_termsofuse/)
24. Все о блокчейн, мозге и WEB 3.0 в России и мире [Электронный ресурс]. – URL: <https://t.me/blockchainRF/4481>

**И. И. Бунова,**

кандидат юридических наук, докторант,

Академия управления

Министерства внутренних дел

Российской Федерации

## **УГОЛОВНО-ПРАВОВАЯ ОХРАНА ПРАВА ЧЕЛОВЕКА НА СВОБОДУ СОВЕСТИ И ВЕРОИСПОВЕДАНИЯ В СОВРЕМЕННЫХ УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

**Аннотация.** Актуальность рассмотренного в статье вопроса обусловлена глубиной назревшей проблемы и перспективой масштабных негативных общественно-опасных последствий, которые может повлечь нарушение незыблемости уголовно-правовой охраны права на свободу совести и вероисповеданий в современных условиях цифровизации. Целью исследования видится анализ современного состояния, сложившихся предпосылок и последствий совершения деяний, предусмотренных ст. 148 УК РФ, изучение эффективности уголовно-правовых и криминологических мер противодействия преступлениям, нарушающим права человека на свободу совести и вероисповеданий в современных условиях цифровизации. Сформировано видение в необходимости особого подхода не только в плане уголовно-правового запрета, но и обеспечении профилактики данного вида преступлений.

**Ключевые слова:** цифровизация, верификация, свобода совести и вероисповеданий, уголовно-правовая охрана права, публичность, несовершеннолетние, профилактика преступлений

## **CRIMINAL-LEGAL PROTECTION OF THE HUMAN RIGHT TO FREEDOM OF CONSCIENCE AND RELIGION IN THE MODERN CONDITIONS OF DIGITALIZATION**

**Abstract.** The relevance of the issue considered in the article is due to the depth of the pressing problem and the prospect of large-scale negative socially dangerous consequences that may result from a violation of the inviolability of the criminal-legal protection of the right to freedom of conscience and religion in the modern conditions of digitalization. The purpose of the study is to analyze the current state, existing prerequisites and consequences of committing acts provided for in Art. 148 of the Criminal Code of the Russian Federation, to study the effectiveness of criminal-legal and criminological measures to counteract crimes that violate human rights to freedom of conscience and religion in the modern conditions of digitalization. A vision has been formed of the need for a special approach not only in terms of criminal-legal prohibition, but also in ensuring the prevention of this type of crime.

**Key words:** digitalization, verification, freedom of conscience and religion, criminal law protection of rights, publicity, minors, crime prevention

**Введение.** Российская Федерация является многоконфессиональной страной, народы которой имеют свою религию и традиции, свободны в выборе религиозных убеждений. Вместе с тем в последние годы складывается негативная тенденция, имеющая манипулятивный характер публичного воздействия отдельных лиц на неограниченную аудиторию слушателей, призывающая к насилию, дискриминации, провокационным действиям нетерпимости к иным религиям, имеющая разрушающий характер и влекущая к крайне негативным последствиям.

**Основная часть.** Уголовным законом Российской Федерации охраняется право верующих на свободу совести и вероисповеданий (ст. 148 УК РФ), однако в последнее время можно отметить негативную тенденцию роста преступлений данной направленности (2013 г. – 6; 2023 г. – 47).

Разумно было бы возразить, что представленные цифры незначительны на общем фоне числа зарегистрированных преступлений, однако публичный характер и социальные последствия, к которым может привести растущая динамика данных преступлений, имеет весьма критические перспективы.

Если ранее акцентировалось внимание на совершении преступных действий в общественном месте, прилюдно, то в последнее время на первый план выходит аспект обязательного «использования средств массовой информации либо информационно-телекоммуникационных сетей (далее – ИТС), включая сеть «Интернет» [6].

Публичное оскорбление чувств верующих, «посягательство на священные каноны церкви, надругательство над объектами культа вызывают негативную реакцию у верующих, которая может привести к массовым протестам, насилию и другим тяжким последствиям» [7. С. 21].

В этой связи можно обозначить деяния, предусмотренные ст. 148 УК РФ, совершенные в текущем 2024 году, повлекшие значительный общественный резонанс.

Так, в мае 2024 г. трое жителей Ставропольского края демонстративно сожгли книгу «Новый завет», фиксируя свои действия на камеру телефона, после чего выложили видеозапись в мессенджере [9]; в июне Елене Суликовой (она же Алена Полын) было предъявлено обвинение по пункту «а» ч. 2 ст. 282, ч. 1 ст. 148 УК РФ за распространение экстремистской литературы, в которой содержались призывы к совершению насилия в отношении священнослужителей Русской православной церкви, а также за публикацию в сети «Интернет» видео с высказываниями, оскорбляющими чувства верующих [8]; в июне 2024 г. двое мигрантов мусульман в православном храме в Южном Бутово г. Москвы целенаправленно затушили свечи, после чего применили насилие к прихожанке, сделавшей им замечание. Свои действия фиксировали на камеру телефона [3]; в июле 2024 г. в сети «Интернет» появился ролик, в котором Хавьер Ярмагомедов, блогер из Дагестана, оскорбительно выражался в адрес христиан, при этом осквернял нательный крест, топтал его [2].

Совершенные деяния были широко освещены в средствах массовой информации, вызвав негативную реакцию общественности, и привели к увеличению числа религиозных конфликтов, подпадающих под действие уголовного закона.

И в данном аспекте, в каждом отдельном случае, практическую значимость имеет заключение эксперта, которое позволяет квалифицировать деяние лица по ст. 148 УК РФ. Ключевым является определение экспертом в ходе проведения судебной лингвистической экспертизы, наличие (отсутствие) объекта, непосредственно предназначенного для богослужений и проведения религиозных обрядов (церемоний), их конфессиональной принадлежности. И, главное, содержатся ли в действиях лица признаки оскорбления (осквернения), выражения явного неуважения по отношению к религии, культу или другому конфессиональному вероучению (доктрине).

Исследование научно-теоретических источников и судебной практики о преступлениях, предусмотренных ст. 148 УК РФ, позволяет говорить об их схожести с преступлениями экстремистской направленности, которая заключается не только в оскорблении религиозных чувств верующих, но, главное, в публичном характере их совершения.

Неотъемлемыми составляющими публичности в этой связи является не только распространение лицом информации на открытых цифровых платформах, доступ к которым возможен неограниченного круга лиц, но и заведомо умышленное адресование ее широкому кругу лиц, подписанному на определенный контент, либо имеющих к нему доступ.

Речь, в большей степени, идет о сложившейся в последнее время негативной тенденции провокационной демонстрации отдельными, радикально настроенными личностями (блогерами), имеющими свой блог или контент, размещенный на определенной цифровой платформе, пренебрежительного, в большей степени, оскорбительного отношения к религии, призывы к совершению насилия, массовым беспорядкам на религиозной почве. Осуществление манипулятивной деятельности с целью формирования у внешней целевой аудитории канала одобрительного отношения к своим преступным действиями, поиск последователей и единомышленников.

Не следует забывать, что зачастую основной целевой аудиторией блогеров являются несовершеннолетние, которые наиболее подвержены восприятию деструктивного контента, циркулирующего в информационно-коммуникационной сети.

В этой связи нельзя не согласиться с автором, утверждающим, что «интернет наделяет большей силой и стимулирует рост доверия к людям, носителям тех или иных идей, которых мы не знаем лично, но именно эти «лидеры мнений» формируют новые тренды, создают моду на те или иные идеи, вещи, ценности» [4. С. 148].

Такие действия могут быть продиктованы не только желанием повысить свой рейтинг в сети, монетизировать свою деятельность, но и применением информационно-психологического воздействия, направленного на побуждение аудитории к агрессивным и иным асоциальным действиям, нарушающим общественный порядок и разрушающим традиции и ценности государства.

Разделяем мнение авторов, считающих, что «развитие цифровых технологий позволило киберпреступности не считаться с национальными государственными интересами и прочно обосноваться в информационном и экономическом пространстве» [10. С. 229].

Существенным обстоятельством является то, что личности блогеров, которые вещают в виртуальном пространстве, не всегда известны, как правило, они маскируются под псевдонимом или «ником».

На законодательном уровне проработан вопрос о деанонимизации блогеров, имеющих свои интернет-каналы и регулярных подписчиков, численностью не менее 10 000 человек, распространяющих информацию на территории России. Вместе с тем решение вопроса о верификации блогеров с меньшей целевой аудиторией, позволит не только в короткие сроки установить лиц, занимающихся пропагандой насилия в отношении священнослужителей, оскорбляющих чувства верующих, тем самым нарушая их право на вероисповедание, но и создать условия для блокировки их интернет-контента, предотвращая совершение этими лицами новых преступлений.

В этой связи нами полностью разделяется мнение ученых, утверждающих, что «требуется особый подход не только в плане уголовно-правового запрета, но и профилактики преступлений, которая должна осуществляться с учетом сведений о состоянии и динамике преступности», а также скрытом потенциале «возможностей ее появления, диктующем потребность в профилактике» [1. С. 108–109; 5. С. 72].

Обращая внимание на вовлечение в совершение преступлений, предусмотренных ст. 148 УК РФ несовершеннолетних, учитывая возраст, с которого наступает уголовная ответственность за данные преступления, необходимым элементом профилактики видится проведение с несовершеннолетними учащимися государственных бюджетных учреждений, информационной работы сотрудниками органов внутренних дел (далее – ОВД), о недопущении их вовлечения и участия в указанных деяниях.

Более того, установление систематического взаимодействия ОВД с главами религиозных объединений на предмет доведения до верующих информации, направленной на сохранение спокойствия, исключения агрессии в условиях происходящего информационного воздействия и провокационных действий со стороны преступного элемента, способствующих разжиганию религиозных конфликтов.

Резюмируя, следует заключить, вопрос религиозной толерантности и правильного диалога между традиционными конфессиями не просто крайне важен, он необходим. Цифровизация не изменила, а лишь обнажила те слабые стороны, которые не позволяют в полной мере спрогнозировать и создать полноценные условия реализации нормы права по уголовно-правовой охране прав человека на свободу совести и вероисповедания.

Исследуя современное состояние уголовно-правовой охраны права человека на свободу совести и вероисповедания в современных условиях цифровизации, следует сказать о неготовности уголовного закона в полной мере обеспечить данное законом право человека. Общественная опасность данного деяния стала гораздо выше с учетом трансформации преступности, изменения способов, средств, направленных на нарушение прав верующих на свободу совести и вероисповеданий, они носят массовый агрессивный характер, направлены на разжигание религиозных конфликтов, ненависти и вражды.

По факту преступления, совершенные по ч. 1 и ч. 2 ст. 148 УК РФ, нарушают права не одного конкретного лица, а неограниченного числа лиц, испове-

дующих определенную религию, сопряжены с нарушением общественного порядка. Используя информационно-телекоммуникационные сети лицо, совершающее преступление, охватывает огромную аудиторию, информация имеет высокую скорость передачи и распространения, как следствие, влечет негативные, порой непредсказуемые, последствия и массовые беспорядки, совершение иных, более тяжких преступлений.

**Заключение.** Видится разумным проработка на законодательном уровне вопроса о верификации блогеров, имеющих свои интернет-каналы и регулярных подписчиков, вне зависимости от их количества, что позволит в короткие сроки установить личность преступника, заблокировать интернет-канал, предотвратить совершение этими лицами новых преступлений.

Комплексной организации профилактической работы ОВД, заключающейся:

- в информационном просвещении несовершеннолетних начиная с 15-летнего возраста, обучающихся в государственных бюджетных учреждениях, о недопущении фактов их вовлечения и последствиях участия в совершении преступлений, предусмотренных ст. 148 УК РФ;
- организации взаимодействия с официальными представителями религиозных организаций различной конфессиональной принадлежности, направленное на проведение главами религиозных организаций в культовых местах, предназначенных для отправления религиозных нужд (церквях, мечетях, синагогах), разъяснительных бесед среди прихожан о возможных информационных провокациях, применении средств информационно-психологического воздействия в целях массового влияния на сознание людей противоположными сторонами, влекущих проявление нетерпимости к другим религиям, способствующим развязыванию религиозных конфликтов, провоцирующим массовые беспорядки и трагические последствия.

### Список литературы

1. Бабаев М. М., Пудовочкин Ю. Е. Российская уголовная политика и уголовный закон: опыт критического анализа: монография. – М.: Юрлитинформ. – 2017. – 693 с.
2. В Москве возбуждено уголовное дело против растоптавшего православный крест блогера // Российская газета (rg.ru). [Электронный ресурс]. – URL: <https://rg.ru/video/2024/07/17/v-moskve-vozbuzhdeno-ugolovnoe-delo-protiv-rastoptavshego-pravoslavnyj-krest-blogera.html?ysclid=lyx1v12e44346879072>
3. В Москве иностранец потушил свечи в церкви и напал на прихожанку // Известия. [Электронный ресурс]. – URL: <https://iz.ru/1714705/2024-06-19/v-moskve-inostranec-potushil-svechi-v-tserkvi-i-napal-na-prikhozhanku>
4. Гавриленко О. В. Цифровые технологии социального контроля: перспективы и социальные последствия их внедрения // Вестник Московского университета. Сер. 18. Социология и политология. – 2022. – Т. 28, № 1. – С. 145–163.
5. Пинкевич Т. В. Противодействие преступлениям, совершаемым в сфере конкуренции: постановка проблемы // Труды Академии управления МВД России. – 2019. – № 4(52). – С. 70–75.

6. Постановление Пленума Верховного Суда Российской Федерации от 28.06.2011 № 11 (ред. от 28.10.2021) «О судебной практике по уголовным делам о преступлениях экстремистской направленности» // Сайт Верховного Суда Российской Федерации [Электронный ресурс]. – URL: <https://www.vsrp.ru>

7. Сичкаренко А. Ю. Публичность как признак преступного нарушения права на свободу совести и вероисповеданий // Вестник Краснодарского университета МВД России. – 2019. – № 4 (46). – С. 21–25.

8. Следственный комитет обвиняет ведьму Алену Полынь в экстремизме и оскорблении религиозных чувств // LIFE. [Электронный ресурс]. – URL: <https://life-ru.turbopages.org/life.ru/s/p/1663970>

9. Суд вынес приговор по делу о ролике с сожжением «Нового завета» // РАПСИ. [Электронный ресурс]. – URL: [https://rapsinews.ru/judicial\\_news/20240905/310221668.html?ysclid=m0qiplti2k713374436](https://rapsinews.ru/judicial_news/20240905/310221668.html?ysclid=m0qiplti2k713374436)

10. Шалагин А. Е., Идиятуллов А. Д. Трансформация преступности в XXI веке: особенности предупреждения и противодействия // Вестник Казанского юридического института МВД России. – 2021. – Т. 12, № 2 (44). – С. 227–235.

**А. В. Воронин,**

магистр права, адвокат,

Тверская областная коллегия адвокатов

«Линия защиты»

## **АКТУАЛИЗАЦИЯ ПРАВОЗАЩИТНОГО РЕГУЛИРОВАНИЯ КОНСТИТУЦИОННОГО ПРАВА НА ПОСМЕРТНОЕ ТВОРЧЕСКОЕ БЫТИЕ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

**Аннотация.** Цифровизация детерминирует формирование новых форм и практик человеческой коммуникации и влечет изменение содержания конституционных прав человека и гражданина. В этой связи целью настоящего исследования является формулирование предложений по совершенствованию механизма правозащитного регулирования конституционного права на посмертное творческое бытие в условиях цифровизации и общественных отношений, связанных с его реализацией. На основе анализа норм позитивного права, материалов правоприменительной и судебной практики, данных научных источников обосновывается необходимость введения гражданско-правового субинститута охраны (защиты) «аватара» и воссозданного с помощью искусственного интеллекта человеческого голоса, установлении юридической (административной и уголовной) ответственности за нарушение установленных законом требований в сфере обработки биометрических персональных данных, а также за хищение чужого имущества с использованием технологии дипфейка.

**Ключевые слова:** право, посмертное творческое бытие, правозащитное регулирование, цифровизация, цифровые технологии, искусственный интеллект, нейронная сеть

## ACTUALIZATION OF REMEDIAL REGULATION OF CONSTITUTIONAL RIGHT TO POSTHUMOUS CREATIVE EXISTENCE IN THE CONTEXT OF DIGITALIZATION

**Abstract.** Digitalization determines the creation of new forms and practices of human communication and entails changes in the constitutional rights of human and citizen. In this regard the purpose of this study is to formulate proposals for improving the mechanism of remedial regulation of constitutional right to posthumous creative existence in the context of digitalization and public relations associated with its implementation. Based on the analysis of positive law, materials of law enforcement and court practice, data from scientific sources, the need to introduce a civil-law sub-institution for the protection (defense) of the "avatar" and the human voice recreated with the help of artificial intelligence, establishing legal liability (administrative and criminal) for violating the requirements established by law in the field of processing biometric personal data, as well as for theft of someone else's property using deepfake technology.

**Keywords:** law, posthumous creative existence, remedial regulation, digitalization, digital technologies, artificial intelligence, neural network

**Введение.** Институциональная модернизация правовых систем современности, обусловленная различными вызовами времени, в числе которых цифровизация, предполагает качественное обновление содержания основных прав и свобод человека и гражданина. Для правовой системы Российской Федерации разрешение вопроса о такого рода обновлении имеет решающее значение в связи с цифровым наследием «ковидного кризиса», актами сетевой манифестации «культуры отмены» в отношении России, деструктивными последствиями распространения «фейков» и инсинуаций по общедоступным цифровым каналам коммуникации. Между тем восприятие новых коммуникативных форм и практик порождает необходимость не только конституционно-правового осмысления, но и опосредования правопользования, прежде всего, в форме правового регулирования. В полной мере изложенное относится к эксклюзивным сюжетам творческого «воскрешения» умерших людей, ставшим востребованными в свете цифровизации. Как следствие актуализирован вопрос о необходимости правозащитного регулирования конституционного права на посмертное творческое бытие в означенных условиях.

**Основная часть.** Указанное во введении к настоящей работе конституционное полномочие каждого ранее жившего лица на продолжение своего творческого пути после собственной физической смерти с использованием цифровых технологий [3. С. 21] онтологически базируется на положениях ч. 1 ст. 20, ч. 1, 2 ст. 44 Конституции Российской Федерации (закрепляющих конституционное право на жизнь, конституционную свободу творчества и конституционное право на участие в культурной жизни [10]; далее – Конституция РФ), истолковываемых в их системной взаимосвязи. В качестве наглядных иллюстраций соответствующего правопользования, предполагающего формат коммуникативного присутствия, то есть нахождения почившего лица в конкретном месте и в определенное время при помощи конкретной цифровой технологии (а именно за счет digital-

трансформации человека в так называемого «аватара»), распоряжения имевшимися при жизни субъекта права творческими способностями, другими словами, опосредованного участия в культурной жизни, можно рассматривать следующие. Это извлечение голоса (вокала) рок-музыканта В. Р. Цоя из фонограмм и последующее создание нейронной сетью а капелла [13], а также реализация иных инициативных проектов по формированию целостного чувственно воспринимаемого и не лишенного способности к реагированию образа указанного лица на новогоднем концерте в Ижевске [2], возвращение к «жизни» актера Ю. В. Никулина для съемок в кинофильме «Манюня: Приключения в Москве» [4], который в настоящее время вышел в прокат, певицы Ж. В. Фриске для целей проведения «Премии МУЗ-ТВ 2024» [11].

Использование цифровой технологии, именуемой как «дипфейк» (англ. deepfake от deep learning «глубинное обучение» + fake «подделка»), не ограничивается одной лишь территорией Российской Федерации. «Несколько лет назад благодаря дипфейку Одри Хепберн прорекламовала шоколад. А Кэрри Фишер появилась в новой части «Звездных войн» уже после смерти. <...> К юбилею Сальвадора Дали флоридский музей художника решил оживить сюрреалиста. Посетители смогли пообщаться с самим Дали» – приводит сетевое издание "Metarating" [6].

Кроме того, в октябре 2023 года стало известно, что польская компания «CD Projekt RED», занимающаяся разработкой игрового проекта «Cyberpunk 2077», воспользовалась нейронной сетью для воссоздания голоса умершего польского актера дубляжа Милогоста Речека (Miłogost Reczek), участвовавшего в создании основной части компьютерной игры и не дожившего до выхода дополнения ("Phantom Liberty") к ней [25].

Таким образом, указанные практики обрели широкий масштаб распространения. Вместе с тем, как отмечалось ранее, до настоящего времени именно в Российской Федерации не нашла своего разрешения (в первую очередь законодательного) проблема правозащитного регулирования конституционного права на посмертное творческое бытие, а равно возникающих в связи с его реализацией общественных отношений.

Согласно данным социологического опроса, озвученным генеральным директором АНО «Диалог Регионы» В. Г. Табаком в рамках сессии «Украденная личность. Правовые аспекты регулирования дипфейков и подделок голоса» на XII Петербургском международном юридическом форуме, состоявшемся в 2024 году, 54 % респондентов из России считают, что регулировать дипфейки необходимо на законодательном уровне [24].

В настоящее время началось формирование судебной практики по вопросу использования дипфейка. Показательным примером в этом отношении является решение Арбитражного суда г. Москвы от 30.11.2023 по делу № А40-200471/2023. Из содержания данного судебного акта следует, что технология дипфейк (в приведенном примере за счет ее использования был создан «аватар» актера Киану Ривза (Keanu Reeves)) представляет собой дополнительный инструмент обработки (технического монтажа) видеоматериалов, используемый моушн-дизайнером [16]. Такое понимание исследуемого феномена является результатом судебного казуального

толкования норм гражданского законодательства. Вместе с тем единый законодательный подход к определению понятия «дипфейк», его правового режима, а также правовых последствий его использования на данный момент отсутствует. Одновременно применительно к заданной теме исследования важно также учесть следующее обстоятельство. Несмотря на то, что в рамках вышеназванного судебного дела не рассматривался вопрос о необходимости выражения человеком, «аватар» которого создается, согласия (несогласия) на подобного рода цифровую трансформацию, по нашему мнению, один лишь факт формирования судебной практики по вопросу использования дипфейков уже сам по себе свидетельствует о необходимости формулирования предложений, направленных на усовершенствование механизма правозащитного регулирования права на посмертное творческое бытие. Тем более в совокупности с приведенными ранее примерами, в которых речь напрямую идет о творческом «воскрешении» (при помощи вышеуказанной цифровой технологии) умерших людей.

В продолжение вышесказанного отметим, что инициатива правовой регламентации общественных отношений, связанных с использованием дипфейков, породила бурную дискуссию как среди представителей общественности, так и среди депутатов Государственной Думы Федерального Собрания РФ. В средствах массовой информации еще летом 2023 года сообщалось о грядущем «появлении» официального понятия «дипфейк» в российском правовом поле, однако спустя год законопроект по-прежнему находится в разработке в связи с особым – этическим – характером рассматриваемой проблемы [7].

Развивая соответствующий нарратив, полагается возможным заметить следующее. Как справедливо подчеркивает В. И. Крусс, регулировать – значит упорядочивать, направлять динамику процесса пользования конституционным полномочием, но без изменения и без «вторжения» в пространство его сущностной статики (с учетом того, что природа конституционных прав проявляется в свойствах *относительного* (выделено нами – А. В.) постоянства их содержания и неумалваемости по мере пользования) [19. С. 293].

Так, в результате конституционной реформы 2020 года текст п. «и» ст. 71 Конституции РФ был дополнен указанием на информационные технологии [8]. С момента внесения соответствующих изменений таковые находятся в ведении Российской Федерации, в связи с чем уместно вести речь о формировании правового фундамента для опосредования вышеназванного конституционного полномочия каждого.

Следует отметить, что «точечное» (элементарное) правозащитное регулирование рассматриваемой базовой возможности имеет место на уровне актов текущего законодательства.

Пленум Верховного Суда РФ в своем постановлении от 15.06.2010 № 16 «О практике применения судами Закона Российской Федерации «О средствах массовой информации» (далее – ПП ВС № 16) обращает внимание на то, что к общественным интересам следует относить не любой интерес, проявляемый аудиторией, а, например, потребность общества в обнаружении и раскрытии угрозы демократическому правовому государству и гражданскому обществу, общественной безопасности, окружающей среде (абз. 3 п. 25 ПП ВС № 16) [14].

Не вдаваясь в дискуссию о корректности используемой данным органом публичной власти терминологии (в особенности об отождествлении категорий «интерес» и «потребность»), отметим следующее. По нашему мнению, фактические данные о наличии (отсутствии) общественного интереса подлежат верификации в соответствии с положениями ч. 3 ст. 55 Конституции РФ, в которой перечисляются те фундаментальные конституционные ценности, меры правовой защиты которых являются универсальными вне зависимости от конкретных жизненных ситуаций отдельно взятых людей.

Вследствие этого можно выдвинуть предположение, согласно которому в отсутствие иного правозащитного регулирования случаи творческого «воскрешения» не могут подпадать под действие п. 1 ст. 152<sup>1</sup> ГК РФ в части, в которой выражение согласия на использование образа человека является необязательным.

В то же время следует обратить особое внимание на содержание абз. 1 п. 44 ПП ВС № 16. В соответствии с данным разъяснением без согласия гражданина обнародование и использование его изображения допустимо в силу подп. 1 п. 1 ст. 152<sup>1</sup> ГК РФ, то есть когда имеет место публичный интерес, в частности, если такой гражданин является публичной фигурой (занимает государственную или муниципальную должность, играет существенную роль в общественной жизни в сфере политики, экономики, искусства, спорта или любой иной области), а обнародование и использование изображения осуществляется в связи с политической или общественной дискуссией или интерес к данному лицу является общественно значимым. Такой подход представляется оправданным и, безусловно, конституционно значимым [23. С. 50].

И все же смоделируем такую ситуацию. Есть некоторая «публичная фигура», например, В. Р. Цой. Безусловно, он сыграл существенную роль в общественной жизни, по меньшей мере, в сфере искусства, став своего рода «символом эпохи». Однако творческое «воскрешение» В. Р. Цоя в соответствии с избранным нами дискурсом не сопряжено с какими-либо дискуссиями, а предполагает коммуникативное присутствие как формат реализации конституционного права каждого на посмертное творческое бытие. Одновременно Пленум Верховного Суда РФ в приведенном разъяснении отсылает к категории общественно значимого интереса к конкретному лицу. Вместе с тем на содержание такого «стремления» указано в приведенном ранее абз. 3 п. 25 ПП ВС № 16. Вследствие этого образуется герменевтический круг.

Таким образом, формально из вышеизложенного можно сделать вывод, что согласие на такого рода использование изображения требуется в любом случае. Однако применительно к данной позиции в абз. 2 п. 44 ПП ВС № 16 приводится следующее толкование. Если речь идет о возможности использования изображения в ситуации, связанной с извлечением прибыли, оно допускается строго при наличии согласия запечатленного лица. Соответственно, если инициаторы творческого «воскрешения» (например, группа «Кино» и сын В. Р. Цоя А. В. Цой) при той степени условности вышеописанных ситуаций извлекают в связи с таким «воскрешением» прибыль, логично заключить, что согласие человека в действительности требуется. Однако возникает вопрос о том, как следует

поступить, если «при прочих равных» творческое «воскрешение» осуществляется исключительно в благотворительных целях.

В связи с вышеизложенным представляется оправданным выдвинуть следующий тезис. По конституционно-правовому смыслу (определенному на основе системного толкования нормоположений ст. 2, ч. 1, 2 ст. 17, ст. 18, ч. 1 ст. 21, ч. 1 ст. 23, ч. 1 ст. 44, ч. 1, 2 ст. 45, ч. 1 ст. 55, ч. 3 ст. 67<sup>1</sup> Конституции РФ) положений п. 1 ст. 152<sup>1</sup> ГК РФ соответствующее регулирование направлено исключительно на защиту изображения (фотографии, видеозаписи, произведения изобразительного искусства) как некоторого статичного с точки зрения диалектики общественной жизни объекта, своего рода «следа» человека. Творческое же «воскрешение» предполагает формат не автоматического воспроизведения, а коммуникативного присутствия соответствующего лица (при этом такое присутствие обеспечивается за счет использования цифровых технологий и не ограничивается пространственно-временными пределами).

В этой связи, по нашему убеждению, требуется урегулирование соответствующих отношений путем дополнения ГК РФ статьей, посвященной вопросам правовой охраны (защиты) «аватара», созданного с помощью искусственного интеллекта.

Так, о постепенном «вхождении» социальных, экономических, духовно-культурных прав «в зону риска» под влиянием цифровых технологий и о необходимости принятия дополнительных мер по правовой защите таких возможностей пишут и другие авторы, например И. А. Умнова-Конюхова, Е. В. Алферова, И. А. Алешкова [22. С. 75].

В соответствии с предлагаемой нами моделью правозащитного регулирования субъект конституционного права на посмертное творческое бытие в случае наличия у него намерения реализовать указанное право должен при жизни добровольно в письменной форме выразить согласие на собственную цифровую трансформацию. При этом соответствующая односторонняя сделка, с нашей точки зрения, подлежит обязательному нотариальному удостоверению, что также надлежит урегулировать путем внесения дополнений в Основы законодательства РФ о нотариате (утв. ВС РФ 11.02.1993 № 4462-1) [12].

Одновременно представляется разумным введение законодательного запрета на предоставление третьим лицам права пользоваться «аватаром» в отсутствие четко и недвусмысленно выраженной воли умершего в той мере, в какой это будет отвечать требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Данный запрет с точки зрения внутреннего структурирования системы российского законодательства разумно отобразить в статье ГК РФ, посвященной вопросам правовой охраны (защиты) «аватара». При этом важно понимать, что «аватар» не является ни объектом, ни субъектом права. Это форма цифрового «дополнения» человека. И такое дополнение используется строго в целях обеспечения надлежащей реализации конституционного права каждого на посмертное творческое бытие в форме правопользования.

Наряду с этим «точечным» образом урегулированы общественные отношения, связанные с охраной человеческого голоса. Так, по смыслу ч. 1 ст. 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, в том числе сведения о голосе человека (на что содержится прямое указание в п. 1 Постановления Правительства РФ от 01.04.2024 № 408 «О видах биометрических персональных данных, на которые распространяется действие Федерального закона «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» [15]), являются биометрическими персональными данными [21].

Данный вектор развития правового регулирования видится нам избранным верно. Вместе с тем, поскольку в рассматриваемом аспекте голос, воспроизводимый при помощи нейронной сети, так же, как и «аватар», является формой цифрового «дополнения» человека, важно подчеркнуть следующее.

Для цели реализации идеи творческого «воскрешения» посредством цифровой трансформации отдельно взятого лица также необходимо внесение дополнений в действующее законодательство Российской Федерации, ведь согласно позиции Д. В. Бахтеева, с которой нет оснований не согласиться, чтобы создать систему искусственного интеллекта (цифровой объект), способную оказать положительное воздействие на физическую реальность, требуется сначала оцифровать фрагмент этой реальности [1. С. 73]. Поскольку использование голоса по своей сути аналогично использованию «аватара», по нашему мнению, имеются основания для урегулирования соответствующих общественных отношений в том же порядке, что и общественных отношений, связанных с использованием «аватара». Причем соответствующее правозащитное регулирование допустимо осуществлять одновременно. Так, не имеется каких-либо препятствий объективного и субъективного порядков для дополнения ГК РФ статьей, посвященной вопросам правовой охраны (защиты) человеческого голоса, воссозданного с помощью искусственного интеллекта. Ведь, как справедливо отмечают А. В. Корнев, И. С. Барзилова, С. В. Липень, О. В. Танимов, Д. В. Шепелев, А. А. Арнаутова, на законодательном уровне не всегда закреплены гарантирующие средства для использования цифровых технологий, неправильное сочетание отдельных видов норм и обеспечивающих их средств довольно часто приводит к изменению цели, изначально поставленной в самой норме нормативного правового акта [17. С. 134]. Такое регулирование с позиции юридической техники возможно в рамках одной статьи, что позволит избежать перегруженности вышеназванного законодательного акта близкими по своим смыслу и значению нормами, а также будет служить целям обеспечения надлежащего правоприменения. При этом в связи с тем, что ч. 2 ст. 11 Закона о персональных данных содержит специальное указание на то, что согласие на их обработку не требуется в случаях, предусмотренных законодательством Российской Федерации о нотариате, в момент состав-

ления согласия на собственную цифровую трансформацию субъекту надлежит указывать объемы таковой, и в случае разрешения воспроизводства человеческого голоса при помощи искусственного интеллекта факт обработки данных о голосе человека будет презюмироваться, дополнительная обработка биометрических персональных данных не потребуется.

Описанную выше правотворческую инициативу надлежит рассматривать в контексте приведения в гармонию цифровых технологий и права. Е. В. Скурко в этой связи пишет следующее: «Это может быть достигнуто как путем адаптации закона к технологии, так и посредством приспособления технологии к закону» [18. С. 81]. Поскольку правовая материя является в достаточной степени «гибкой», в рамках настоящего исследования допустимо вести речь именно об ее адаптировании под требования цифровой эпохи.

Полноценное гарантирование соответствующих прав немыслимо без введения юридической ответственности за их нарушение. В соответствии с данным подходом такая ответственность может быть гражданско-правовой, административной и уголовной. В этой связи полагается необходимым вновь обратиться к положениям ГК РФ.

Механизм реализации гражданско-правовой ответственности является достаточно проработанным. Так, ст. 152<sup>1</sup> ГК РФ предусмотрены два способа защиты изображения человека: изъятие из оборота по решению суда и уничтожение без какой бы то ни было компенсации экземпляров материальных носителей, содержащих изображение, полученное или используемое с нарушением требований закона; удаление распространенного в информационно-телекоммуникационной сети «Интернет» изображения, а также пресечение или запрещение дальнейшего его распространения.

Думается, что второй способ подлежит адаптации под специфику охраняемого (защищаемого) конституционного права на посмертное творческое бытие. Так, представляется реальным полное удаление «аватара» и воссозданного при помощи нейронной сети голоса человека из соответствующей базы данных, а также пресечение действий, создающих угрозу нарушения права в дальнейшем. При этом правотворческая инициатива, по нашему мнению, должна быть оформлена тем же (аналогичным) образом, что и ранее выдвинутая нами. В частности, по нашему мнению, дополнение ГК РФ указанием на данный способ защиты возможно в тексте статьи, которая посвящена вопросам правовой охраны (защиты) «аватара» и человеческого голоса.

Относительно возможности введения административной ответственности отметим следующее. Действующий Кодекс РФ об административных правонарушениях (далее – КоАП РФ) содержит специальную статью, которой предусмотрена административная ответственность за нарушение требований в области размещения биометрических персональных данных [9]. Однако в диспозиции данной статьи отсутствует указание на действия, содержащие признаки нарушения требований ч. 2 ст. 11 Закона о персональных данных. Вследствие этого видится целесообразной дополнительная правовая регламентация с определением вида и размера административного наказания за обозначенное нами административное правонарушение.

Аналогичным образом необходимо дополнить статью об уголовной ответственности за нарушение вышеназванных требований, повлекшие существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, Уголовный кодекс РФ (далее – УК РФ) [20].

Одновременно с этим можно предположить, что создание «аватара» и воссоздание человеческого голоса при помощи нейронной сети может послужить целям и интересам лиц, стремящихся к незаконному присвоению чужих благ. Так, с учетом изложенного представляется необходимым дополнить положения КоАП РФ об ответственности за совершение мелкого хищения, положения УК РФ об ответственности за совершение кражи, мелкого хищения, совершенного лицом, подвергнутым административному наказанию, мошенничества, присвоения или растраты, соответствующим квалифицирующим признаком – совершение административного правонарушения, преступления с использованием технологии дипфейка.

Дополнение указанных выше законодательных актов «пакетным образом» позволит обеспечить полноту и всесторонность соответствующего реформирования, усовершенствовать механизм правозащитного регулирования конституционного права на посмертное творческое бытие и возникающих в связи с его реализацией общественных отношений.

**Заключение.** На основании изложенного представляется возможным сформулировать следующие итоговые выводы.

Во-первых, наличие значительного числа практик творческого «воскрешения» человека с использованием цифровых технологий, реальной (наличной) потребности личности, общества и государства в усовершенствовании механизма правозащитного регулирования конституционного права на посмертное творческое бытие как закономерной реакции на вызовы цифровой эпохи, отсутствие единого законодательного подхода к определению понятия «дипфейк», его правового режима, а также правовых последствий его использования обусловили необходимость анализа норм позитивного права и разработки соответствующей правотворческой инициативы в рамках настоящего исследования.

Во-вторых, для целей обеспечения надлежащего правопользования видится необходимым введение в действующее гражданское законодательство Российской Федерации нового субинститута охраны (защиты) «аватара» и воссозданного с помощью искусственного интеллекта человеческого голоса, а также введения специальной нотариальной процедуры предоставления человеком в письменной форме добровольного согласия на его цифровую трансформацию.

В-третьих, для выполнения государством основной конституционной обязанности по признанию, соблюдению и защите прав и свобод человека и гражданина представляется целесообразным установление административной и уголовной ответственности за нарушение требований ч. 2 ст. 11 Закона о персональных данных, а также за хищение чужого имущества с использованием технологии дипфейка.

Практическая значимость настоящей работы сводится к формулированию правотворческой инициативы по усовершенствованию механизма правозащитно-

го регулирования обозначенного базового полномочия каждого. Вместе с этим представляется, что эвристический потенциал изучения данной проблематики не исчерпывается рамками настоящего исследования. И в дальнейшем целесообразно проведение конституционно-компаративистских, юридико-технических, философско-правовых и иных научных изысканий.

### Список литературы

1. Бахтеев Д. В. Искусственный интеллект: этико-правовые основы: монография. – М.: Проспект, 2023. – 176 с.
2. В Ижевске сгенерированный нейросетью Цой исполнит песню на удмуртском языке // Национальный акцент. Медиапроект гильдии межэтнической журналистики. – URL: <https://nazaccent.ru/content/41667-v-izhevsk-sgenerirovannyj-nejrosetyu-coj-ispolnit-pesnyu-na-udmurtskom-yazyke/>
3. Воронин А. В. Право на творческую жизнь после смерти: фикция или реальность? // Бакалавру.net: альманах научно-исследовательского клуба по актуальным проблемам права «Бакалавру.net». – Тверь: Издательство Тверского государственного университета. 2023. – С. 21–24.
4. «Воскрешенный» Юрий Никулин появится в фильме «Манюня: Приключения в Москве» // Regions.ru. – URL: <https://regions.ru/kultura/voskresshenyy-yuriy-nikulin-poyavilsya-v-filme-manyunya-priklyucheniya-v-moskve>
5. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 08.08.2024) // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_5142/](https://www.consultant.ru/document/cons_doc_LAW_5142/)
6. Жизнь после смерти: нейросети воскрешают мертвых артистов // Сетевое издание «Metarating». – URL: <https://cybersport.metaratings.ru/articles/zhizn-posle-smerti-neyroseti-voskreshayut-mertvykh-artistov/>
7. Заинтересованные в лицах: в России обсуждается закон о дипфейках // Известия. – URL: <https://iz.ru/1674806/katerina-alabina/zainteresovannye-v-litcakh-v-rossii-obsuzhdaetsia-zakon-o-dipfeikakh>
8. Закон РФ о поправке к Конституции РФ от 14.03.2020 № 1-ФКЗ «О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_346019/](https://www.consultant.ru/document/cons_doc_LAW_346019/)
9. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 08.08.2024) // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_34661/](https://www.consultant.ru/document/cons_doc_LAW_34661/)
10. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_28399/](https://www.consultant.ru/document/cons_doc_LAW_28399/)
11. «Ожившая» Жанна Фриске на премии Муз-ТВ довела ее отца до слез // 2x2.su. – URL: <https://2x2.su/news/shou-biznes/ozhivshaya-zhanna-friske-na-premii-muz-tv-dovela-eye-ottsa-do-slyez.html>

12. Основы законодательства Российской Федерации о нотариате от 11.02.1993 №4462-1 (ред. от 08.08.2024) // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_1581](https://www.consultant.ru/document/cons_doc_LAW_1581)

13. Попробуй спеть вместе со мной: как нейросеть воссоздала голос Виктора Цоя // РБК. – URL: <https://trends.rbc.ru/trends/industry/60b9f5729a7947830db7d491?from=copy>

14. Постановление Пленума Верховного Суда РФ от 15.06.2010 № 16 (ред. от 09.02.2012) «О практике применения судами Закона Российской Федерации «О средствах массовой информации» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_101401/](https://www.consultant.ru/document/cons_doc_LAW_101401/)

15. Постановление Правительства РФ от 01.04.2024 № 408 «О видах биометрических персональных данных, на которые распространяется действие Федерального закона «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_473908/](https://www.consultant.ru/document/cons_doc_LAW_473908/)

16. Решение Арбитражного суда г. Москвы от 30.11.2023 по делу № А40-200471/2023 // Картотека арбитражных дел [Электронный ресурс]. – URL: [https://kad.arbitr.ru/Document/Pdf/4d7f0305-69af-44fe-8841-a59e84aa7deb/8dedc372-21f6-4751-ab3c-8a320fe435ce/A40-200471-2023\\_20231130\\_Reshenija\\_i\\_postanovlenija.pdf?isAddStamp=True](https://kad.arbitr.ru/Document/Pdf/4d7f0305-69af-44fe-8841-a59e84aa7deb/8dedc372-21f6-4751-ab3c-8a320fe435ce/A40-200471-2023_20231130_Reshenija_i_postanovlenija.pdf?isAddStamp=True)

17. Система права и система законодательства: современное состояние и перспективы развития в цифровую эпоху: монография / под науч. ред. А. В. Корнева. – М.: Проспект, 2023 – 176 с.

18. Скурко Е. В. «Электронное правительство», «цифровой гражданин», «цифровая личность» искусственного интеллекта: новые подходы в цифровой государственной политике и юридической науке // Право, цифровые технологии и искусственный интеллект: сб. ст. / отв. ред. Е. В. Алферова. М.: ИНИОН РАН, 2021. С. 69–86.

19. Крусс В. И. Теория конституционного правопользования. – М.: Норма, 2007. 752 с.

20. Уголовный кодекс Российской Федерации от 13.06.1996 # 63-ФЗ (ред. от 08.08.2024) // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_10699/](https://www.consultant.ru/document/cons_doc_LAW_10699/)

21. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) «О персональных данных» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](https://www.consultant.ru/document/cons_doc_LAW_61801/)

22. Цифровое развитие и права человека: монография / И. А. Умнова, Е. В. Алферова, И. А. Алешкова / под общ. ред. И. А. Умновой-Конюховой. М.: ИНИОН РАН, 2021. 174 с.

23. Эбзеев Б. С. Личность и государство в России: взаимная ответственность и конституционные обязанности / Б. С. Эбзеев. М.: Норма, 2008. 384 с.

24. 54 % россиян считают, что регулировать дипфейки необходимо на законодательном уровне // dialog.info. – URL: <https://dialog.info/54-rossiyan-schitajut-chto-regulirovat-dipfejki-neobhodimo-na-zakonodatelnom-urovne/>

25. CD Projekt Red использовала нейросеть для создания голоса умершего актера озвучки // i2HARD. – URL: <https://i2hard.ru/publications/33825/>

**И. С. Иксанов**

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

### **ЦИФРОВОЕ ГРАЖДАНСТВО И НАРОДНЫЙ СУВЕРЕНИТЕТ: ПРОБЛЕМЫ РЕАЛИЗАЦИИ**

**Аннотация.** Идеи народного суверенитета широко представлены в отечественной науке. Они проанализированы с разных позиций и являются основой современного российского демократического общества. Взаимосвязь между цифровым гражданством и народным суверенитетом крайне важна, поскольку цифровые технологии и Интернет коренным образом изменили способ участия граждан в общественно-политических процессах. Интернет определил новые возможности для людей с целью выражения своего мнения и взаимодействия с другими представителями гражданского общества не только в масштабах одной страны, но и мира в целом. Трансграничность современных правоотношений в области народного суверенитета ставят вопрос о защите от искажения воли народа в цифровой среде, о преодолении цифрового разрыва и формировании современного пространства, защищенного в цифровой среде не менее надежно, чем в реальной.

**Ключевые слова:** цифровое гражданство, народный суверенитет, цифровая среда, цифровизация, цифровой разрыв

### **DIGITAL CITIZENSHIP AND PEOPLE'S SOVEREIGNTY: PROBLEMS OF IMPLEMENTATION**

**Abstract.** The ideas of national sovereignty are widely represented in Russian science. They are analyzed from different perspectives and are the basis of modern Russian democratic society. The relationship between digital citizenship and popular sovereignty is extremely important, as digital technologies and the Internet have radically changed the way citizens participate in socio-political processes. The Internet has identified new opportunities for people to express their opinions and interact with other representatives of civil society, not only on the scale of one country, but also the world as a whole. The cross-border nature of modern legal relations in the field of national sovereignty raises the question of protecting the distortion of the will of the people in the digital environment, bridging the digital divide and forming a modern space protected in the digital environment no less reliably than in the real one.

**Keywords:** digital citizenship, popular sovereignty, digital environment, digitalization, digital divide

**Введение.** В современном правовом демократическом государстве суверенная воля народа, воплощенная в народном суверенитете, выступает в качестве главной основы для реализации демократических ценностей. Надлежащее осознание сущности и содержания реализации суверенитета считается одним из необходимых условий для поддержания и развития народом России собственного государства.

**Основная часть.** Прежде чем сформироваться в сравнительно целое учение, иметь свое отражение в законодательной базе и выступить в качестве главной основы государственного строительства, идейные положения о суверенитете прошли процесс существенной трансформации и подверглись определенным сложностям в развитии.

Так, М. Ш. Шарифов указывает на тот момент, что первые упоминания о возникновении суверенности народа прослеживаются с античных времен. Однако возникновению непосредственного мышления в области народного суверенитета способствовало становление Вестфальской системы международных отношений. После принятия Вестфальского мира появились так называемые «восходящие теории» о нации-народе.

«Восходящие теории» – это перераспределение суверенитета от суверенов (например, монархов, государей) с укреплением таких важных характеристик, как единство, верховенство и безграничный суверенитет [16].

На сегодняшний день современное юридическое и политическое пространство имеет много интерпретаций понятию «народный суверенитет», при этом его часто сравнивают с демократией и народовластием [15].

Далее рассмотрим научные подходы отечественных конституционалистов в области народного суверенитета.

По мнению Б. С. Эбзеева, народный суверенитет – это в первую очередь особые качества народной власти, это не сама власть, а особенный принцип конституционного государственного строя, путем которого обеспечивается народное всевластие.

Народный суверенитет выходит далеко за рамки государственных пределов: провозглашает цели и принципы, устанавливает государственные организационные основы и закрепляет их в Конституции РФ, выступает не только в качестве субъекта непрерывного источника власти, но и в качестве уникальной личности государственно-правовой направленности [1].

Говоря о народном суверенитете, необходимо учитывать то обстоятельство, что он имеет определенную политическую сущность, правовую форму реализации, по мнению Б. Эбзеева, политическая сущность выступает итогом развития различного рода отношений людей, к примеру, экономических, политических, духовных и иных.

Стоит отметить, что государство напрямую оказывает правовое воздействие не только на суверенитет, распространенный в его пределах, но и в целом на народный, тем самым не препятствуя его распространению [17].

Таким образом, в конституционализме всевластие народа имеет исключительно правовую основу, а государство и государственная власть исходят от воли народа.

По мнению А. В. Зиновьева, народный суверенитет – это главная инстанция, так называемая база всего, что формируется в пределах государства, которой подчиняются все регуляторы власти общественных отношений [7].

По мнению С. А. Авакьяна народный суверенитет – это обширное понятие, состоящее из трех элементов, – всевластие народа внутри одного государства, народное право выбора власти и объединение граждан одной страны без привязки к национальности и расовой принадлежности [2].

По мнению Д. В. Дегтевой, А. В. Корниенко и коллег, народный суверенитет – это власть народа, зависящая от конституционного строя конкретного государства, частично отождествленная с определенными полномочиями власти, а также рассматриваемая как организационно-политическая система положений государственной конституции. Только при таких условиях можно говорить о какой-либо гарантии народного всевластия. К такому определению ученые пришли, исследуя актуальные подходы в области толкования понятия народного суверенитета [1].

По мнению В. В. Комаровой, такие конституционные понятия, как «народный суверенитет» и «источник власти», – это единое целое. Кроме того, эти явления и понятия имеют органическую связь, и их конституционное закрепление является выражением демократической природы Российского государства. Как отмечает автор, суверенность народа является конституционным принципом организации и деятельности народной власти; народ, являясь сувереном во всех сферах жизни, сам решает, как ему организовать свою непосредственную власть с помощью Конституции [10].

По мнению А. В. Безрукова, А. Н. Кокотовой и М. И. Кукушкиной, народный суверенитет – это безграничные властные полномочия народа, реализуемые практически во всех сферах жизнедеятельности граждан, с учетом закрепленных Конституцией и иными законодательными актами организационно-правовых форм [5].

Народный суверенитет и народовластие – общепризнанные конституционные ценности, важнейшей государственной и общественной стратегической задачей которых является построение демократического государства [9]. Сегодня в любом демократическом государстве в Конституции закреплены основные положения в области суверенитета народа и государства.

Следует отметить, что народный суверенитет – это своеобразный абсолют неделимости, при котором по законам логики власть безгранична [1]. Еще такие ученые, как Гоббс и Локк отмечали, что народ «хоть и является источником политической власти, но он лишен полновластия».

В рамках исследований в области народного суверенитета нами были выявлены две основные сложности: в практической (реализация идей и положений суверенитета) и теоретической (осмысление и понимание концепции суверенитета) частях.

В настоящий момент по-прежнему происходят бурные дискуссии в сфере толкования значения понятия «народ», что предопределяет невозможность в наиболее полной форме ответить на данный вопрос. В профессиональном общении юристов, политологов и социологов данная проблема носит название «парадокс народного суверенитета» [13].

Таким образом, анализ положений Конституции Российской Федерации показывает, что существует как минимум два определения слова «народ».

С политической точки зрения нация – это определенная группа людей, живущая на определенной территории и имеющая точно такие же права, как и другие этнические группы, говорящие на том же языке.

В то же время с точки зрения политико-правовой дееспособности народ представляет собой единый неделимый субъект, обладающий всемогуществом и законодательной властью.

Позиция нашего исследования аналогична мнению П. А. Астафичева. Он рассматривает народ как основной субъект власти, создающий политико-правовую способность каждого гражданина.

Согласно современной правовой действительности, не все граждане политически дееспособны. Это связано с разными причинами [4].

В настоящее время законом определены категории граждан РФ, не имеющие права участвовать в выборах или избираться в госорганы. К таким категориям относятся недееспособные граждане (недееспособность должна быть признана судом) и тюремные заключенные.

По мнению Д. А. Авдеева, правильный источник власти – это не все население, а лишь его часть, имеющая реальный статус избирателя. Ученый, таким образом, проводит параллели между понятиями «нация» (обладает определенной властью) и «электорат» (обладает действующим избирательным правом) [3].

На современном этапе развития граждане имеют право участвовать в общественно-политических процессах, т. е. народ имеет полноценное право голоса в контексте деятельности органов государственного управления.

Цифровое гражданство имеет решающее значение в этом контексте, поскольку оно содействует облегчению политического взаимодействия и участия населения в ходе процесса управления страной при помощи применения цифровых средств [8].

Однако пространственное поле цифровой среды также может служить источником дезинформации, которая способна подорвать народный суверенитет. В данном контексте цифровое гражданство имеет решающее значение для развития медиаграмотности и навыков критического мышления, позволяя гражданам определять достоверный характер информации, с которой они сталкиваются в Интернете.

В целом цифровое гражданство и народный суверенитет взаимосвязаны между собой и дополняют друг друга в современном демократическом обществе.

Взаимосвязь между цифровым гражданством и народным суверенитетом крайне важна, поскольку цифровые технологии и Интернет коренным образом изменили способ участия граждан в общественно-политических процессах. Интернет определил новые возможности для людей с целью выражения своего

мнения и взаимодействия с другими представителями гражданского общества не только в масштабах одной страны, но и мира в целом [7].

Кроме того, цифровое гражданство помогает защитить индивидуальные права граждан и неприкосновенность частной жизни в условиях цифрового пространства, что необходимо для народного суверенитета. Когда граждане осознают риски, связанные с обменом личной информацией в Интернете, и предпринимают определенные меры для своей защиты, у них появляется больше возможностей для участия в политических процессах.

На сегодняшний день, в эпоху цифрового развития, процесс формирования тесных взаимосвязей в рамках цифрового гражданства и народного суверенитета сталкивается с рядом определенных проблем.

В качестве основной мы выделяем проблему цифрового разрыва или цифрового неравенства, подразумевающую под собой неравный доступ к цифровым технологиям и Интернету в целом. Это может привести к ограничению возможности граждан участвовать в общественно-политической жизни с помощью применения цифровых технологий и препятствовать проявлению гражданской активности.

Преодоление проблемы цифрового разрыва оказывает непосредственное влияние на процесс продвижения цифрового гражданства и народного суверенитета [11].

Кроме того, существуют проблемы, связанные с быстрыми темпами развития и распространения цифровых технологий, что влечет за собой такое явление, как технологический прогресс. Например, развитие социальных сетей создает новые проблемы, связанные с распространением информации, неприкосновенностью частной жизни и кибербезопасностью, которые требуют постоянного внимания и адаптации граждан.

Нами было выделено несколько путей решения проблем, представленных выше, с помощью осуществления внедрения цифрового гражданства и народного суверенитета. Рассмотрим некоторые из них.

Преодоление проблемы цифрового неравенства. Система органов государственной власти и различного рода организации вполне могут осуществлять инвестиционную деятельность, то есть заниматься вложением инвестиций в дальнейших целях получения прибыли или иного полезного эффекта. Можно инвестировать в расширение доступа к Интернету и технологической инфраструктуре в недостаточно обслуживаемых территориях, что подразумевает создание общедоступных сетей Wi-Fi или сотрудничество с определенными компаниями в рамках расширения широкополосного доступа в труднодоступных районах.

Совершенствование способов функционирования политической системы напрямую зависит от развития современных цифровых технологий. Органы государственной власти, политические партии и общественно-политические организации могут содействовать в вопросах разработки стандартов и принципов современных цифровых технологий по мере их появления. В свою очередь, это может помочь включить создание целевых и экспертных групп в оценку этических-правовых последствий новых технологий.

В наши дни определенный круг исследователей и экспертов в области конституционного и избирательного права отмечают пассивное отношение народа при их непосредственном участии в жизни государства, что, в свою очередь, влечет одну из главных проблем, связанных с реализацией в нашей стране народного суверенитета.

Е. А. Петрова признает, что в наше время все чаще можно упоминать о том, что проведение референдумов стало крайне редким явлением в сфере механизмов реализации прямой демократии, и в большинстве случаев в качестве действующего механизма выступают выборы. Однако и тут наблюдается крайне низкая заинтересованность народа [14].

Следует отметить, что низкий процент явки избирателей на выборы позволяет сделать вывод о малой заинтересованности нашего народа в реализации такого государственного явления, как суверенитет.

Кроме того, существенная часть народа нашей страны, преимущественно люди молодого возраста, как правило, перекладывают осуществление властных полномочий институту государства, тем самым не реализуя свой суверенитет.

**Заключение.** В настоящее время, говоря об основах формирования и дальнейшем развитии гражданского общества в РФ, стоит отметить, что согласно Конституции Российской Федерации, непосредственным выражением власти народа признаны демократические выборы.

Академик О. Е. Кутафин в своих научных трудах отмечал, что: «главное для демократии то, что у нас должно быть гражданское общество, то есть общество, активно участвующее в государстве и политической жизни. Не просто как наблюдатели, демократическое общество – общество, которое по-настоящему активно, которое по-настоящему равнодушно» [12].

### Список литературы

1. Абражеева Д. В., Корниенко А. В., Симонова М. А., Степанова Т. В. Народный суверенитет: проблема понятия, сущности и содержания // Успехи современной науки и образования. – 2017. – Т. 8, № 4. – С. 104–107.
2. Авакьян С. А. Конституционное право России. Учебный курс: учебное пособие: в 2 т. – Т. 1. – 5-е изд., перераб. и доп. – М.: Норма: ИНФРА-М, 2014. – 865 с.
3. Авдеев Д. А. Российский народ как субъект конституционного права // Конституционное и муниципальное право. – 2017. – № 11. – С. 14–17.
4. Астафичев П. А. Народный суверенитет: понятие, содержание, конституционные формы выражения // Конституционное и муниципальное право. – 2014. – № 4. – С. 2–10.
5. Безруков А. В. Конституционное право России: учебное пособие. – 3-е изд., перераб. и доп. – М.: Юстицинформ, 2015. – 302 с.
6. Гаврилов Е. О. Цифровой суверенитет в условиях глобализации: философский и правовой аспекты // Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки. – 2020. – № 2(14). – С. 146–152.
7. Зиновьев А. В. Суверенитет, демократия, государство // Известия высших учебных заведений. Правоведение. – 2016. – № 6(269). – С. 20–28.

8. Кастельс М. Власть коммуникации: учебное пособие / под науч. ред. А. И. Черных; пер. с англ. Н. М. Тылевич. – М.: Издательский дом Высшей школы экономики, 2016. – 564 с.
9. Комарова В. В. Демократия через призму конституционных ценностей // Народовластие как конституционная ценность: правовое регулирование и гарантии реализации: монография / отв. ред. В. А. Виноградов, А. А. Ларичев. – М.: НИУ «Высшая школа экономики», 2021. – С. 12–19.
10. Комарова В. В. Конституционная система власти России и принцип разделения властей // Актуальные проблемы российского права. – 2017. – № 9(82). – С. 36–46.
11. Костина Н. Б., Чижев А. А. К вопросу о разграничении понятий «цифровой раскол», «цифровое неравенство» и «цифровой разрыв» // Уфимский гуманитарный научный форум. – 2022. – № 1(9). – С. 56–63.
12. Кутафин О. Е. Наша задача – поддержать законность в стране: интервью с сопредседателем Ассоциации юристов России, ректором Московской государственной юридической академии О. Е. Кутафиным // Юридический мир. – 2006. – № 12. – С. 14–25.
13. Нечаев П. Ю. Принцип народного суверенитета: проблемы теории и практики // Ленинградский юридический журнал. – 2014. – № 2. – С. 40–46.
14. Петрова Е. А. Проблемы реализации народного суверенитета в современных условиях // Вестник Ивановского государственного университета. Серия: Естественные, общественные науки. – 2021. – № 1. – С. 13–18.
15. Пяткин В. Н., Исаев А. А. Народный суверенитет как конституционно-правовая фикция // Научное обозрение. Международный научно-практический журнал. – 2021. – № 4. – URL: <https://srjournal.ru/2021/id325/>
16. Шарифов М. Ш. Теоретические проблемы определения содержания и соотношения народного, государственного и национального суверенитета // Труды института государства и права Российской академии наук. – 2009. – № 2. – С. 3–16.
17. Эбзеев Б. С. Человек, народ, государство в конституционном строе Российской Федерации: монография. – 2-е изд., перераб. и доп. – М.: Проспект, 2015. – 656 с.

**С. М. Курбатова,**

доктор юридических наук, профессор,  
Красноярский государственный аграрный университет

## **ЦИФРОВИЗАЦИЯ СИСТЕМЫ ПРАВОСУДИЯ КАК ЧАСТЬ МЕХАНИЗМА РЕАЛИЗАЦИИ ПРАВА НА ЗАКОННЫЙ СУД ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ**

**Аннотация.** Целью является обращение внимания на неравное положение лиц с ограниченными возможностями при реализации ими права на обращение в суд относительно других категорий населения. Представлена взаимосвязь между правом на обращение в суд и доступностью правосудия в контексте такой категории населения, как лица с ограниченными возможностями. Рассмотрена циф-

ровизация системы правосудия как способ решения проблемы и как дополнительная трудность для лиц с ограниченными возможностями при реализации ими своего права на обращение в суд.

**Ключевые слова:** правосудие, лица с ограниченными возможностями, право на суд, законность, доступность, цифровизация, гарантии

## DIGITALIZATION OF THE JUSTICE SYSTEM AS PART OF THE MECHANISM FOR THE REALIZATION OF THE RIGHT TO A LAWFUL COURT FOR PERSONS WITH DISABILITIES

**Abstract.** The aim is to draw attention to the unequal position of persons with disabilities in the exercise of their right to appeal to the court relative to other categories of the population. The article presents the relationship between the right to go to court and accessibility of justice in the context of such a category of the population as persons with disabilities. The article considers the digitalization of the justice system as a way to solve the problem and as an additional difficulty for people with disabilities in exercising their rights to appeal to the court.

**Keywords:** justice, persons with disabilities, the right to a court, legality, accessibility, digitalization, guarantees

**Введение.** Лица с ограниченными возможностями, к которым согласно Конвенции ООН 2006 г. «О правах лиц с ограниченными возможностями» отнесены те, «кто имеет долгосрочные физические, психические, интеллектуальные или сенсорные нарушения, которые при взаимодействии с различными барьерами могут препятствовать их полному и эффективному участию в жизни общества наравне с другими», сталкиваются с различными трудностями и препятствиями на протяжении своей жизни из-за имеющихся у них проблем со здоровьем физического и (или) когнитивного характера. Дополнительные проблемы им создает социум, где они подвергаются дискриминации «по признаку инвалидности», означающей любое различие, исключение или ограничение из-за имеющихся у лица нарушений здоровья, целью или следствием которых является умаление или сведение к нулю признания, пользования или реализации наравне с другими всех прав человека и основных свобод в политической, экономической, социальной, культурной, гражданской или любой другой области. Согласно позиции ООН в дискриминацию «по признаку инвалидности» включаются все формы дискриминации, в том числе такая специальная форма, как отказ в разумном приспособлении, под которым понимаются осуществление изменений и корректировки факторов внешней и социальной среды с учетом специфики конкретной ситуации таким образом, чтобы люди с ограниченными возможностями могли пользоваться правами человека и основными свободами на равной основе с другими людьми. Одним из таких прав является право на доступ к правосудию [3], с реализацией которого у лиц с ограниченными возможностями возникает много проблем [1], а одним из средств их разрешения может стать цифровизация системы правосудия, уже применяемая в ряде стран мира [2].

**Основная часть.** Вопросам, связанным с проблемой обеспечения доступа к правосудию лицам с ограниченными возможностями, уделяется достаточно большое внимание на уровне международного сообщества, отражаясь как в универсальных актах международного права, так и в региональных, являясь ориентиром для развития и совершенствования соответствующего национального законодательства конкретных государств. В первой группе актов особое внимание заслуживает Конвенция ООН 2006 г. «О правах лиц с ограниченными возможностями», которая закрепила новый подход к пониманию, что не все люди равны между собой по разным причинам, и что это обуславливает необходимость выделять такую группу населения, как лица с ограниченными возможностями. В ст. 9 данной Конвенции, посвященной необходимости государствам-участникам создания таким лицам условий для «возможности вести независимый образ жизни и всесторонне участвовать во всех аспектах жизни», включая «выявление и устранение препятствий и барьеров, мешающих доступности а) на здания, дороги, транспорт и другие внутренние и внешние объекты (*в том числе объекты системы правосудия – Авт.*); б) на информационные, коммуникационные и другие службы, включая электронные службы и экстренные службы», одним из средств достижения этого называет «новые информационно-коммуникационным технологиям и системам, включая Интернет» (п. g ст. 9 Конвенции).

В 2020 г. Организация Объединенных Наций выпустила свои первые в истории руководящие принципы по доступу к социальной справедливости для людей с ограниченными возможностями, чтобы облегчить им возможность обращения к системам правосудия по всему миру. В них подчеркивается, что никому не может быть отказано в доступе к правосудию на основании относимости к данной категории населения и отмечается необходимость государств обеспечить реализацию права на доступ к правосудию, в том числе с помощью информационных и прочих технологий.

Более детально эти идеи раскрываются в международных актах регионального уровня. Так, на уровне Евросоюза проблемам лиц с ограниченными возможностями уделяется внимание с конца XX в. Развитие технологий в XXI в. и анализ эффективности их применения способствовали формированию вывода о том, что отсутствие доступности и разумных приспособлений влияет на предоставление цифровых услуг и форматов, удобных для инвалидов, доступ к информации и встроенной среде в системе правосудия, а также на связь с ней и внутри нее; это варьируется от недоступных веб-сайтов до недоступных залов судебных заседаний. В связи с этим Европарламентом ЕС в дальнейшем была определена позиция, что при разработке систем по цифровизации правосудия (с точки зрения инструментов и процессов) следует уделять внимание потребностям людей с ограниченными возможностями в разработке инклюзивного трансграничного электронного правосудия. Это закреплено, например, в п. 18 Директивы ЕС 2016/2102 Европейского парламента и Совета от 26 октября 2016 года о доступности веб-сайтов и мобильных приложений органов государственного сектора, где речь идет о необходимости согласованных действий для обеспечения полного доступа к новому электронному контенту для лиц с ограниченными

возможностями. К сожалению, на уровне СНГ подобных правовых актов нет. Поэтому обратимся к ЕС, где, в частности, рассматриваются такие рекомендации по совершенствованию механизма реализации права на доступ к правосудию для лиц с ограниченными возможностями, как:

- признать доступность в качестве основного принципа цифровизации системы правосудия и обеспечить ее соблюдение во всех законодательных инициативах по цифровизации, в том числе в «наборе инструментов» мер по ускорению цифровизации в системах правосудия;
- обеспечить доступные альтернативы цифровым услугам и форматам и разумные приспособления, основанные на индивидуальных потребностях людей с ограниченными возможностями – будь то участники или работники системы правосудия;
- развивать повышение цифровых навыков людей с ограниченными возможностями с помощью конкретных действий, связанных с расширением их знаний о возможностях цифровой доступности и о том, как их использовать;
- поощрять обмен передовым опытом в области доступного цифрового правосудия между разными государствами;
- обучать сотрудников национальных органов, работающих в области отправления правосудия, с учетом потребностей лиц с ограниченными возможностями в доступе к правосудию на том же уровне, что и других людей;
- собирать данные о доступности и влиянии цифровизации правосудия на людей с ограниченными возможностями;
- обеспечить людям с ограниченными возможностями и представляющим их организациям на международном, национальном и местном уровнях участие в конструктивных консультациях при решении проблем, связанных с доступом к правосудию [4].

Представляется, что использование положительного опыта других государств в виде законодательных разработок, теоретических исследований, результатов реализации на практике различных механизмов, направленных на обеспечение прав лиц с ограниченными возможностями вообще и в системе правосудия, включая использование современных информационных технологий и интеллектуальных систем, в частности, будет способствовать изначально более высокому качеству формирования аналогичных направлений государственной политики в других странах, которые находятся еще на стадии их разработки.

**Заключение.** Ответственность за создание условий лицам с ограниченными возможностями для ведения независимого образа жизни и всестороннего участия в разных сферах жизнедеятельности лежит на каждом государстве, провозгласившем себя правовым и социальным, как, например, Российская Федерация. Это должно достигаться поэтапно, с определением приоритетов, в числе которых, безусловно, обеспечение данным лицам доступа к правосудию.

Реализация государственной политики на каждом этапе развития общества и государства и в целом мирового сообщества должна учитывать его современные особенности. Особенность настоящего времени заключается в том, что мир вступил в эпоху цифровизации. Поэтому одним из основных инструментов механизма реализации права лиц с ограниченными возможностями на доступ к

правосудию и законному суду должна стать цифровизация национальных систем правосудия, осуществляемая с учетом потребностей людей с разными возможностями.

### Список литературы

1. Носырева А. Е. Концепция доступа к правосудию инвалидов // Норма. Закон. Законодательство. Право: сборник материалов XXIII Международной научно-практической конференции, Пермь, 16–17 апреля 2021 года. – Пермь: Пермский государственный национальный исследовательский университет, 2021. – С. 738–742.
2. Томаева В. К. К проблеме обеспечения доступа к правосудию в условиях цифровизации судопроизводства // Вестник Арбитражного суда Московского округа. – 2023. – № 3. – С. 74–79.
3. Razveykina N. A., Shikhanova E. G., Dmitriev A. V. Digitalization of legal proceedings as a way to ensure access to justice // Vestnik Permskogo Universiteta. Yuridicheskie Nauki. – 2022. – № 58. – P. 621–627.
4. Uidru M. The digitalization of justice mean for persons with disabilities, 2020. – URL: <https://www.edf-feph.org/newsroom-news-what-does-digitalisation-justice-mean-persons-disabilities/>

**Л. Н. Осауленко,**

кандидат юридических наук,  
Евразийская экономическая комиссия

### ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВА ПОТРЕБИТЕЛЕЙ В ЕВРАЗИЙСКОМ ЭКОНОМИЧЕСКОМ СОЮЗЕ

**Аннотация.** В статье проанализированы ключевые проблемы процесса формирования потребительского права и совершенствования механизмов защиты прав потребителей в контексте развития цифровых технологий и трансформации экономических процессов в рамках Евразийского экономического союза. Объектом настоящего исследования явились основные механизмы защиты прав потребителей, закрепленные в праве Евразийского экономического союза. Цель исследования – определение направлений дальнейшего развития международного интеграционного сотрудничества государств-членов ЕАЭС для защиты прав потребителей в условиях цифровой трансформации. Основное внимание уделяется анализу действующих механизмов обеспечения и защиты прав потребителей в Евразийском экономическом союзе, а также предложениям по дальнейшему развитию политики ЕАЭС в этой сфере. Показано, что для повышения эффективности защиты прав потребителей на едином экономическом пространстве ЕАЭС необходимо создание международного права Евразийского экономического союза в сфере защиты прав потребителей, предусматривающего единые механизмы и правила защиты потребительских интересов граждан. Представлены общие предложения, способствующие развитию политики ЕАЭС в рассматриваемой сфере.

**Ключевые слова:** право, цифровые технологии, права потребителей, международные отношения, электронная торговля, интеллектуальные сервисы, искусственный интеллект, евразийская интеграция, ЕАЭС

## DIGITAL TECHNOLOGIES AND CONSUMER RIGHTS IN THE EURASIAN ECONOMIC UNION

**Abstract.** The key problems of the process of forming consumer law of the Eurasian Economic Union and improving mechanisms for protecting consumer rights in the context of the digital transformation of economic processes are analyzed. The object of this study was the main mechanisms for protecting consumer rights enshrined in the legislation of the EAEU member states. The purpose of the study is to determine directions for further development of international integration cooperation of the EAEU member states to protect consumer rights in the context of digital transformation. The main attention is paid to the analysis of existing and developing mechanisms for ensuring and protecting consumer rights in the Eurasian Economic Union, as well as proposals for the further development of the EAEU policy in this area. It is shown that in order to increase the effectiveness of consumer rights protection in the single economic space of the EAEU, it is necessary to create international law of the Eurasian Economic Union in the field of consumer rights protection, providing for uniform mechanisms and rules for protecting the consumer interests of citizens. General proposals are presented that contribute to the development of EAEU policy in this area.

**Keywords:** law, digital technologies, consumer rights, international relations, e-commerce, intelligent services, artificial intelligence, Eurasian integration, EAEU

**Введение.** Современные экономические условия характеризуются развитием цифровизации, быстрым распространением товаров и услуг через интернет и изменением государственного контроля в сторону снижения административного давления на бизнес. Это повышает вероятность возникновения новых проблем в области защиты прав потребителей.

В странах Евразийского экономического союза проживает более 183 миллионов человек, каждый из которых является потенциальным потребителем товаров и услуг [6].

Вопросы, связанные обеспечением интересов граждан как потребителей, особенно актуальны в связи с трансграничностью общего рынка ЕАЭС. В связи с этим возникает необходимость совершенствовать законодательство о защите прав потребителей и предоставить гражданам дополнительные гарантии защиты их интересов на уровне международного евразийского права.

**Основная часть.** Специфика потребительских правоотношений заключается в особом субъектном составе, где потребитель – физическое лицо [1], которое покупает или имеет намерение совершить покупку для личного пользования. При этом потребитель, априори, является слабой стороной правоотношений, не наделенной специальными познаниями в экономической сфере.

Потребительские правоотношения подразумевают наличие специфического субъектного состава, в котором обязательной и, априори, слабой стороной, яв-

ляется потребитель – физическое лицо, который приобретает, или только имеет намерение приобрести товар или услугу для личного пользования.

По результатам исследования, опубликованного Евразийской экономической комиссией [4] (далее – Комиссия), 95 % жителей стран ЕАЭС совершают покупки в интернете, а 78 % пользуются онлайн-услугами. Самые активные участники электронной коммерции находятся в возрастных категориях от 26 до 40 лет (45 %) и от 41 до 55 лет (37 %).

Развитие цифровых технологий и электронных средств коммуникации существенно влияет на общение между покупателями и поставщиками товаров и услуг, что неизбежно сказывается на процессах создания единого рынка в Евразийском экономическом союзе.

Базовым документом – Договором о Евразийском экономическом союзе от 29 мая 2014 года (далее – Договор о ЕАЭС), закреплено, что ЕАЭС представляет собой международную организацию региональной экономической интеграции [1]. Взаимодействие между государствами, являющимися членами Евразийского экономического союза происходит в рамках направлений, обозначенных в Договоре о ЕАЭС. Несмотря на то, что основная деятельность региональной интеграции направлена на развитие экономики, защита прав потребителей также входит в сферу международного сотрудничества государств-членов, хотя и с некоторыми особенностями.

Распределение компетенций в области защиты прав потребителей между странами и Евразийским экономическим союзом характеризуется тем, что каждое государство-член ЕАЭС самостоятельно регулирует эту сферу. Однако Комиссия имеет право давать рекомендации государствам-членам по этому вопросу.

В настоящее время, в странах ЕАЭС сформирована действующая правовая и институциональная основа для защиты прав потребителей на национальном уровне. Она имеет определенные сходства, но в то же время и различия.

Сходство заключается в том, что системы защиты прав потребителей, созданные в странах ЕАЭС, обладают в целом, общей структурой. Эта структура состоит из специальных правовых норм и правоприменительных институтов, предназначенных для обеспечения, охраны и восстановления прав потребителей среди граждан.

Например, программные документы по защите прав потребителей существуют только в Российской Федерации. На уровне субъектов РФ действуют региональные программы в этой области, а на федеральном уровне – Стратегия государственной политики РФ в сфере защиты прав потребителей до 2030 года [9]. В других странах ЕАЭС вопросы защиты прав потребителей не являлись предметом стратегического планирования.

Различия выражаются в том, в каждой стране ЕАЭС формируется своя нормативно-правовая база с различной степенью детализации, созданы неравнозначные по полномочиям и сферам компетенции институты, предназначенные для защиты прав потребителей.

Отмечается существенная разница в развитии организаций гражданского общества, работающих над защитой прав потребителей. Согласно данным, опубликованным на сайте Евразийской экономической комиссии [5], в 2023 году в ЕАЭС

насчитывалось около 1 300 общественных объединений потребителей (95 % из них – зарегистрированы в России). Если учесть население стран Евразийского экономического союза, то на одно общественное объединение потребителей приходится примерно 140 тысяч потребителей. Указанные приблизительные подсчеты говорят о явной нехватке профессиональных общественных организаций, специализирующихся на представлении и защите интересов потребителей.

Кроме того, в рамках ЕАЭС отмечается тенденция к существенному пересмотру норм национально права в области защиты прав потребителей, что ведет к росту несоответствий по ряду аспектов, особенно в контексте регулирования потребительских правоотношений в сфере электронной коммерции и применения интеллектуальных сервисов.

Электронная коммерция и использование интеллектуальных сервисов имеют большое значение для современной экономики, поскольку они способствуют развитию бизнеса, упрощению взаимодействия между продавцами и покупателями и повышению качества услуг. Однако эти процессы также порождают новые вызовы для обеспечения прав потребителей. В числе таких вызовов: сложность контроля и регулирования онлайн-рынка; недостаток прозрачности и открытости информации; высокие риски мошенничества и обмана.

При этом общей проблемой для стран ЕАЭС является отсутствие гарантий и защиты прав граждан. Так, в эпоху развития цифровых технологий и трансформации розничной торговли в данном контексте, ключевой проблемой для регуляторов становится потенциальное ограничение возможностей применения национального законодательства к трансграничным рыночным потребительским взаимоотношениям.

Указанное затрудняет реализацию гражданских прав в сфере электронной торговли и взаимодействие между предпринимателями и потребителями.

В настоящее время экспертами стран ЕАЭС ведется обсуждение вопросов формирования механизмов урегулирования трансграничных потребительских споров.

Аналогичная цифровая разработка должна быть создана и апробирована в рамках пяти стран Евразийского экономического союза. Ключевыми участниками такой системы могут стать предприниматели, занимающиеся онлайн-торговлей на территории стран ЕАЭС, национальные государственные органы, а также Евразийская экономическая комиссия, как точка объединения всех участников процесса, мониторинга и контроля за достижением результата рассмотрения обращения потребителя.

В настоящее время группой исследователей на площадке Евразийской экономической комиссии прорабатываются ключевые подходы для обеспечения безопасного применения интеллектуальных сервисов в правоотношениях с участием потребителей.

Так, участниками Евразийского цифрового форума, проходившего в Минске, отмечено, что «развитие искусственного интеллекта (далее – ИИ) и его интеграция в различные сферы экономики являются важными факторами для повышения конкурентоспособности и улучшения качества жизни населения» [7]. При

этом участниками дискуссии отмечены основные риски для потребителей, связанные с применением систем искусственного интеллекта (далее – ИИ):

- «сложность и непрозрачность алгоритмов, используемых ИИ, что может затруднить понимание и контроль со стороны потребителей;
- неконтролируемый доступ к личной информации, что может привести к утечкам и нарушению приватности;
- отсутствие механизма оценки адекватности решений, предлагаемых интеллектуальными сервисами, что может привести к неправильному использованию данных и принятию ошибочных решений;
- проблематика правового регулирования и определения механизмов добросовестной деловой практики (цифровой культуры) использования ИИ, что может создать барьеры для реализации прав граждан, а также для развития и внедрения новых технологий» [3].

Эксперты также обратили внимание на то, что для снижения риска недобросовестного использования ИИ в отношениях с потребителями следует исходить из того, что:

- «ИИ должен быть понятным для потребителей, компании должны предоставлять информацию о том, как работает система ИИ и какие данные используются для ее обучения;
- компании, использующие технологии на основе ИИ, должны нести ответственность за возможные негативные последствия и предпринимать меры для предотвращения ошибок или злоупотреблений;
- потребители должны иметь возможность контролировать использование своих данных системой ИИ, включая право на удаление своих данных или ограничение доступа к ним;
- системы ИИ должны разрабатываться с учетом этических норм и культурных ценностей общества, чтобы избежать дискриминации и нарушения прав человека;
- необходимо продолжать исследования и разработки в области ИИ для создания новых продуктов и услуг, полезных и безопасных для использования в сфере потребительских правоотношений» [7].

Учет указанных основных направлений в работе стран ЕАЭС по защите прав потребителей позволит выстроить каркас безопасного экономического пространства в рамках данной региональной интеграции.

**Заключение.** Таким образом, вопросы обеспечения прав потребителей в контексте электронной коммерции и использования интеллектуальных сервисов становятся особенно актуальными. Они требуют разработки и внедрения эффективных механизмов защиты прав потребителей, а также гармонизации законодательства в этой области на международном уровне

Эти проблемы особенно заметны в контексте электронной коммерции и использования интеллектуальных сервисов.

Цифровые технологии и электронные коммуникации оказывают значительное влияние на развитие законодательства о защите прав потребителей. Это связано с появлением новых участников правоотношений и развитием дистанционных способов продажи товаров.

Указанное будет способствовать формированию равных условий для граждан государств-членов по защите их интересов как потребителей, на едином экономическом пространстве ЕАЭС [1], а также обеспечению эффективной защиты потребительских прав граждан в контексте положений Руководящих принципов Организации Объединенных Наций для защиты интересов потребителей [8].

### Список литературы

1. Договор о Евразийском экономическом союзе (Астана, 29 мая 2014 г.) Правовой портал Евразийского экономического союза. Официальный сайт. [Электронный ресурс]. – URL: [https://docs.eaeunion.org/docs/ru-ru/0003610/itia\\_05062014](https://docs.eaeunion.org/docs/ru-ru/0003610/itia_05062014)
2. Евразийский взгляд на проблемы потребительских споров. Сайт Евразийской экономической комиссии. – URL: <https://potrebitel.eaeunion.org/ru-ru/Pages/Evrazijskij-vzglyad-na-problemi-potrebiteljskih-sporov.aspx>
3. Искусственный интеллект, новые возможности для продавцов и покупателей обсуждены в Минске. Сайт Евразийской экономической комиссии. – URL: <https://potrebitel.eaeunion.org/ru-ru/Pages/Iskusstvennij-intellekt,-novie-vozmozhnosti-dlya-prodavcov-i-pokupatelej-obsuzhdeni-v-Minske.aspx>
4. Общественное мнение населения стран ЕАЭС о правах потребителей в электронной торговле. Сайт Евразийской экономической комиссии. – URL: <https://potrebitel.eaeunion.org/ru-ru/Pages/Obschestvennoe-mnenie-naseleniya-stran-EAES-o-pravah-potrebitelej-v-elektronnoj-torgovle.aspx>
5. Общественные организации на защите интересов потребителей стран ЕАЭС. Сайт Евразийской экономической комиссии. – URL: <https://potrebitel.eaeunion.org/ru-ru/Pages/Obschestvennie-organizacii-na-zaschite-interesov-potrebitelej-stran-EAES.aspx>
6. Потребитель – центр евразийской интеграции. Как работает Евразийская экономическая комиссия в сфере защиты прав потребителей. Евразийская экономическая комиссия. Официальный сайт. [Электронный ресурс]. – URL: <https://potrebitel.eaeunion.org/ru-ru/Pages/eec.aspx>
7. Резолюция тематической сессии «Потребитель, предприниматель, искусственный интеллект: перспективы развития нового цифрового партнерства», 6 июня 2024 г., Минск // Сайт Евразийской экономической комиссии [Электронный ресурс]. – URL: [https://eec.eaeunion.org/upload/files/depsanmer/summary\\_06062024.pdf](https://eec.eaeunion.org/upload/files/depsanmer/summary_06062024.pdf)
8. Руководящие принципы Организации Объединенных Наций для защиты интересов потребителей (Приняты 22.12.2015 Резолюцией 70/186 на 81-ом пленарном заседании 70-ой сессии Генеральной Ассамблеи ООН) // Документы ООН. Сайт ООН [Электронный ресурс]. – URL: <https://documents.un.org/doc/undoc/gen/n15/449/13/pdf/n1544913.pdf>
9. Стратегия государственной политики Российской Федерации в области защиты прав потребителей на период до 2030 года: Распоряжение Правительства Российской Федерации от 28 августа 2017 г. № 1837-р // СПС «Консультант-Плюс» [Электронный ресурс] в локальной сети РНБ

А. Д. Твердышева,  
аспирант,  
Российская государственная академия  
интеллектуальной собственности

## ПРАВОВЫЕ АСПЕКТЫ ОХРАНЫ ГОЛОСА

**Аннотация.** В связи с появлением новых информационно-цифровых технологий правовая природа голоса человека и механизм его защиты в современном мире становится все более актуальным. Так, появляется необходимость определить голос в системе гражданского права и выявить правовые пробелы по данному вопросу, а также для повышения эффективности правовой охраны голоса предлагается признать голос нематериальным благом.

**Ключевые слова:** дипфейк; изображение гражданина; отечественное законодательство; человек; нематериальное благо; право на публичность; голос

## LEGAL ASPECTS OF VOICE PROTECTION

**Abstract.** Due to the emergence of new information and digital technologies, the legal nature of the human voice and the mechanism of its protection in the modern world is becoming increasingly relevant. Thus, it becomes necessary to identify the voice in the civil law system and identify legal gaps on this issue, as well as to increase the effectiveness of legal protection of the voice, it is proposed to recognize the voice as an intangible good.

**Keywords:** deepfake; image of a citizen; otechetvennoe legislation; person; intangible benefit; right of publicity; voice

**Введение.** В настоящее время усиливается тенденция коммерциализация индивидуальных особенностей личности. Однако в отечественном законодательстве санкционировано только право на изображение гражданина (ст. 152.1 ГК РФ), а вот голос человека на данный момент не получил законодательного регулирования.

**Основная часть.** В последние годы появилась необходимость правового регулирования голоса, так как с развитием искусственного интеллекта в случае нарушение прав обладателя голоса возникают вопросы, как защитить права на него. Тут можно рассмотреть спор Алены Андроновой актрисы дубляжа, которая подала иск против банка «Тинькофф» в 2023 году. Актриса заключила договор с «Тинькофф Банк», по которому она дает свое согласие на переработку ее голоса и его исполнения Банку. Представители Банка отметили, что голос актрисы будут использовать только для внутренних организаций банка. В итоге голос был размещен в общем доступе, из-за чего Алена Андропова лишилась новых проектов и возможности контролировать использование другими лицами ее голоса, что достаточно критично для актрисы. На сегодняшний день судом дело не было рассмотрено.

Проблема правовой охраны голоса гражданина возникла после активного развития технологии deepfake, такая программа может синтезировать голос любого человека и потом его использовать. В связи с этим дикторы и актеры боятся

значительного снижения своих доходов, так как «в перспективе получить синтезированную речь станет дешевле, чем записать диктора» [2. С. 9].

Проблема использования синтезированного голоса гражданина без его согласия затронула не только гражданско-правовой среды, но и область публичного права. Это связано с таким явлением, как дипфейк, по-другому – это определенные действия с медиа-материалами (видео, аудиозаписи, фотографиями). Продукт искусственного интеллекта генерируемый голос или изображение могут применить в разного рода сценариях [1. С. 126–130].

Сперва стоит определить, что такое голос, и может ли он быть уникальным для человека.

Под голосом понимаются разнообразные звуки, образующиеся при помощи голосового аппарата и служащие для общения между живыми существами. [3. С. 56–64]. Например, в Большой Медицинской Энциклопедии указано определение, что голос – это совокупность самых разнообразных по высоте, силе и тембру звуков, издаваемых человеком при помощи голосового аппарата [6].

Однако на индивидуальность голоса человека влияют три составляющие голосового аппарата: органы дыхания; голосовые связки; артикуляционный аппарат.

В случае если голос является уникальным проявлением личности, как и изображение, то стоит защитить право на него.

В 2024 в кинопрокат вышел мультфильм «Кунг-фу Панда 4» где главного героя мультфильма ранее озвучивал шоумен Михаил Галустян, но в «Кунг-фу Панда 4» персонаж Панда По разговаривал другим голосом, что разочаровало зрителей. Из чего следует, что голос является неотъемлемой частью человека, и его изменение означает посягательство на человека, способно менять представление о личности или главном герое мультфильма [4].

Если голос является индивидуальной особенностью человека, как и его внешность, то стоит установить механизм защиты от незаконного использования другими лицами.

Большинство научных деятелей склонны относить голос к нематериальным благам, так как перечень является открытым.

В отечественном законодательстве, а именно в п. 1 ст. 150 ГК РФ, закреплен открытый перечень нематериальных благ. Можно предположить, что голос личности, который прямо не указан в данном перечне, относится именно сюда. Стоит отметить, что голос – это абсолютное право. В связи с этим перечень таких прав должен быть закрытым, поскольку необходимо понимать, какие права другие лица не вправе использовать без согласия. Из-за того, что в законе нет четко перечня нематериальных благ, это и создает проблему правовой неопределенности [5. С. 118–131]. Она возникает в связи с отсутствием четкого правового регулирования таких вопросов.

Следовательно, можно сделать вывод, что голос является нематериальным благом, на которое каждый человек имеет личное неимущественное право. Поэтому голос может быть отнесен в один ряд с изображением, но при этом будет являться самостоятельным элементом, право на защиту которого должно быть

защищено законодательством. Такая позиция поддерживается некоторыми зарубежными странами.

Например, в США охрана голоса и иным индивидуальным особенностям гражданина предоставляется в рамках права на публичность (right of publicity) [7]. Такой институт в США был выработан около 100 лет назад, не признается на федеральном уровне, но охраняется во многих штатах и решается на уровне судебных прецедентов. Человек вправе контролировать коммерческое использование своей индивидуальности, в том числе на голос (ст. 3344 Гражданского Кодекса Калифорнии). Такая позиция поддерживается в других зарубежных странах: в ч. 18 ст. 66 Конституции Эквадора перечислено в одном ряду необходимость защиты чести, образа и голоса человека; в ч. 7 ст. 2 Конституции Перу закреплено право человека на голос и образ.

Одним из первых дел, связанных с защитой такого права, является дело Midler v. Ford Motor Co. [8]. Компания Ford, не получив согласия на использование уникального голоса Бетт Мидлер в рекламе, обратилась к другой исполнительнице с просьбой симитировать ее голос. Суд пришел к выводу, что Мидлер вправе защитить свои права в рамках right of publicity, а голос не защищается инструментами права интеллектуальной собственности.

Например, игровая компания CD Projekt RED, производитель видеоигры Cyberpunk 2077, прекратила свое сотрудничество с РФ, а через время после выхода новых изменений к видеоигре в интернете стали появляться версии на русском языке, созданные с помощью искусственного интеллекта на основе оригинальных голосов актеров озвучки.

Совсем недавно появилась новость, что разработан законопроект об охране голоса «обнародование и дальнейшее использование голоса гражданина (в том числе записи, в которой он содержится, или записи, в которой содержится воссоздаваемый с помощью специальных технологий голос гражданина) допускается только с согласия этого гражданина. То есть голос приравнивается к нематериальному объекту. Данный законопроект охватывает только синтезированные голоса, но не охватывает использование дипфейков. Пока законопроект не был внесен Госдуму.

**Заключение.** Таким образом, исследовав российский и зарубежный опыт, можно прийти к выводу, что правовое регулирование в области охраны голоса на данный момент недостаточно проработано. В соответствии с этим стоит рекомендовать расширить предмет ст. 151.2 ГК РФ охраной голоса гражданина наравне с изображением, помимо этого, включить данный объект в перечень нематериальных благ.

### Список литературы

1. Ващенко Д. Г. Особенности гражданско-правовой охраны голоса актеров дубляжа // Сборник научных статей 7-й Международной научной конференции. – Т. 2. – 2024. – С. 126–130.
2. Лебедева В., Литвиненко Ю. У дикторов крадут голоса: Представители отрасли просят о регулировании технологий синтеза речи // Коммерсант. – 2023. – 27 янв. – С. 9.

3. Киселев А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник Московского государственного областного университета. Серия: Юриспруденция. – 2021. – № 3. – С. 56–64.
4. Кунг-фу панда По больше не заговорит голосом Михаила Галустяна // Дзен [Электронный ресурс]. – URL: [https://dzen.ru/a/ZXvzeV\\_d5C72NI-n](https://dzen.ru/a/ZXvzeV_d5C72NI-n)
5. Матвеев А. Г., Мартыанова Е. Ю. Гражданско-правовая охрана голоса человека при его синтезе и последующем использовании // Ex Jure. – 2023. – № 3. – С. 118–131.
6. Петровский Б. В. Большая Медицинская Энциклопедия (БМЭ) [Электронный ресурс]. – М.: Советская энциклопедия, 1974. – URL: <https://xn--90aw5c.xn--c1avg/index.php/%D0%93%D0%9E%D0%9B%D0%9E%D0%A1>
7. California Civil Code of 1872 § 3344.
8. Midler v. Ford Motor Co., 849 F.2d 460 (9th Cir. 1988) [Electronic resource]. – URL: <https://law.justia.com/cases/federal/appellate-courts/F2/849/460/37485/>

**Т. Ю. Фролова,**

аспирант,

Московский финансово-юридический университет

## **ЗАЩИТА ПАССИВНОГО ИЗБИРАТЕЛЬНОГО ПРАВА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: РОЛЬ СУДОВ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Аннотация.** Работой определены пределы влияния позиций судов РФ на законодательную деятельность в области избирательного процесса с учетом внедрения цифровых технологий. Приведены кейсы, порядок разрешения которых не имеет на сегодняшний день регламентации избирательным законодательством, что предопределяет возрастающую нагрузку на правоприменительные органы (в частности, суды) при решении вопросов, связанных с защитой пассивного избирательного права.

**Ключевые слова:** пассивное избирательное право, судебная защита пассивного избирательного права, цифровизация, дистанционное электронное голосование, цифровые технологии в избирательном процессе, Конституционный Суд РФ, Верховный Суд РФ

## **PROTECTION OF PASSIVE SUFFRAGE IN THE CONTEXT OF DIGITALIZATION: THE ROLE OF THE COURTS OF THE RUSSIAN FEDERATION**

**Abstract.** The work defines the limits of the influence of the positions of the courts of the Russian Federation on legislative activity in the field of the electoral process, taking into account the introduction of digital technologies. The cases are presented, the procedure for resolving which is currently not regulated by electoral legis-

lation, which determines the increasing burden on law enforcement agencies (in particular, the courts) in solving issues related to the protection of passive suffrage.

**Keywords:** passive suffrage, judicial protection of passive suffrage, digitalization, remote electronic voting, digital technologies in the electoral process, the Constitutional Court of the Russian Federation, the Supreme Court of the Russian Federation

**Введение.** Пассивное избирательное право представляет собой право на осуществление государственной власти, местного самоуправления посредством избрания на выборные должности, а его нарушение – прямое несоблюдение основных принципов демократического государства.

**Основная часть.** За защитой своего нарушенного права быть избранным кандидат вправе обратиться с административным иском заявлением в суд общей юрисдикции. Порядок производства по таким делам регламентируется главой 24 Кодекса административного судопроизводства Российской Федерации [3] (далее – КАС РФ). Анализ судебной практики по вопросам защиты избирательных прав граждан показывает, что споры в абсолютном большинстве случаев связаны с реализацией именно пассивного избирательного права [12. С. 38].

Также в порядке конституционного судопроизводства возможно оспорить конституционность тех или иных положений законодательства, влекущих за собой нарушение избирательных прав граждан.

В то время как Президиумом Верховного Суда Российской Федерации периодически утверждаются Обзоры судебной практики по вопросам, возникающим при рассмотрении дел о защите избирательных прав и права на участие в референдуме граждан Российской Федерации, кроме того даются разъяснения законодательства Российской Федерации о выборах и референдумах (например, Постановление Пленума Верховного Суда РФ № 24 от 27 июня 2023 года [9], Постановление Пленума Верховного Суда РФ №17 от 25 июня 2024 [10]), «обобщению решений Конституционного Суда РФ уделено недостаточное внимание по вопросу защиты права быть избранным в органы государственной власти и местного самоуправления» [13. С.64].

В условиях стремительно развивающейся цифровизации и отсутствия своевременной полноценной законодательной регламентации ее внедрения в избирательный процесс, роль судов в процессе защиты пассивного избирательного права трудно переоценить. Право на судебную защиту «выполняет восстановительную функцию в отношении всех других конституционных прав и свобод, что предопределено особой ролью судебной власти» [5]. Вместе с тем федеральным законом «О внесении изменений в уголовно-процессуальный кодекс Российской Федерации» решения ЕСПЧ (вступившие в силу после 15 марта 2022 года) утверждены подлежащими исполнению на территории РФ [11. С. 56].

Применительно к вопросу внедрения цифровых технологий в предвыборную агитацию Пленум Верховного Суда РФ дал определение понятию дипфейк, обозначив его как «вводящие в заблуждение и выдаваемые за достоверные недостоверные изображения, аудио- и аудиовизуальная информация, в том числе созданные с помощью компьютерных технологий» [9], а также установил наступление административной ответственности, предусмотренной статьей 5.12 Кодек-

са Российской Федерации об административных правонарушениях [1], за создание агитационных материалов, содержащих дипфейки.

Как составная часть цифровизации избирательного процесса дистанционное электронное голосование (*далее* – ДЭГ) с его внедрением поставило ряд вопросов, которые были проанализированы Конституционным Судом РФ в его определениях: по жалобе гражданина Юнемана Р. А. [6], по жалобе гражданина Лобанова М. С. [7]. Так, Конституционным Судом РФ ДЭГ было оценено как субсидиарный способ голосования, а его введение – содействие укреплению роста активности избирателей, но при условии его проведения с соблюдением прозрачности, эффективности и надежности, из чего следует, что законоположения, регулирующие порядок его проведения, не могут относиться к числу противоречащих Конституции РФ.

С проведением эксперимента по установлению специального налогового режима «Налог на профессиональный доход» [4] и появлением статуса «самозанятый» возник еще один спорный момент в части реализации указанной категорией граждан их пассивного избирательного права, что также стало поводом для обращения в Конституционный Суд РФ. Так, жалоба поступила от выдвинутой в порядке самовыдвижения и представившей необходимое количество подписей избирателей гражданки С., которой было отказано в регистрации в качестве кандидата по мотивам несоответствия сведений о роде занятий в заявлении о согласии баллотироваться, подписных листах и справке по форме КПД 1122035 (*далее* – справка) (в первом случае – род занятий «самозанятая», а во втором – постановка на учет в качестве физического лица -налогоплательщика налога на профессиональный доход). Согласно правовым позициям судов в справке «отсутствуют слова «самозанятый», «самозанятая», «самозанятость»» [15]. Не согласившись с такими выводами, С. обратилась с жалобой в Конституционный Суд РФ о проверке конституционности пункта 57 статьи 2, подпунктов «в» и «в1» пункта 24 статьи 38 федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан РФ», которые не дают разъяснений относительно документов, необходимых для предоставления в подтверждение статуса самозанятого, что создает препятствия в реализации пассивного избирательного права. В своем Постановлении от 30.05.2024 № 27-П Конституционный Суд РФ пришел к выводу о том, что отсутствие возможности у кандидата указания в представленных для регистрации документов в качестве рода занятий самозанятость «существенно ограничивает его электоральные возможности» [8], а также не позволяют продемонстрировать электорату себя (личные и деловые качества), тем самым привлечь отдать голос за себя, таким образом возникает неравенство избирательных прав граждан, что подлежит исключению путем внесения соответствующих изменений в правовое регулирование порядка регистрации в качестве кандидата.

Следуя предписаниям Конституционного Суда РФ, Министерство юстиции РФ предложило [14] соответствующие поправки в Федеральный закон № 67-ФЗ от 12 июня 2002 «Об основных гарантиях избирательных прав и права на участие в референдуме граждан РФ», а именно в статью 2 «основные термины и понятия». Так, согласно поправкам, самозанятость может быть указана кандида-

тами, поставленными на учет в качестве плательщиков налога на профессиональный доход, в качестве рода занятий. Исключение составляет лишь случай, при котором указанный кандидат зарегистрирован в качестве индивидуального предпринимателя.

**Заключение.** Подводя итог, стоит подчеркнуть отсутствие в действующем законодательстве полноценного регулирования всех возникающих трудностей, связанных с внедрением цифровых технологий в избирательный процесс, что предопределяет растущую на правоприменительные органы (суды в частности) нагрузку в части разрешения складывающихся проблемных аспектов. Суды Российской Федерации на сегодняшний день уже рассматривали вопросы, связанные с дистанционным электронным голосованием, дипфейками, сформулировали соответствующие правовые позиции, что наглядно демонстрирует необходимость оперативной реакции со стороны законодательных органов на стремительное внедрение цифровых технологий.

### Список литературы

1. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Российская газета. – № 256. – 31.12.2001.
2. Федеральный закон от 12.06.2002 № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» // Российская газета. – № 106. – 15.06.2002.
3. Кодекс административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ // Собрание законодательства РФ. – 09.03.2015. – № 10. – Ст. 1391/
4. Федеральный закон от 27.11.2018 № 422-ФЗ «О проведении эксперимента по установлению специального налогового режима «Налог на профессиональный доход» // Российская газета. – № 270. – 30.11.2018.
5. Постановление Конституционного Суда РФ от 15 июля 2021 г. № 37-П «По делу о проверке конституционности подпункта 1 пункта 3 статьи 158 и пункта 10 статьи 242.3 Бюджетного кодекса Российской Федерации, а также части 1 статьи 358 Кодекса административного судопроизводства Российской Федерации в связи с жалобой гражданина Ю. А. Рейнхиммеля» // Российская газета. – № 170. – 29.07.2021.
6. Определение Конституционного Суда РФ от 28 декабря 2021 г. № 2952-О «Об отказе в принятии к рассмотрению жалобы гражданина Юнемана Романа Александровича на нарушение его конституционных прав пунктами 1 и 5 части 2 статьи 4 Федерального закона «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва» и рядом положений Закона города Москвы «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва»» // СПС «КонсультантПлюс».
7. Определение Конституционного Суда РФ от 29 сентября 2022 г. № 2568-О «Об отказе в принятии к рассмотрению жалобы гражданина Лобанова Михаила Сергеевича на нарушение его конституционных прав положениями фе-

деральных законов «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации», «О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации» и «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования в городе федерального значения Москве», а также положениями Закона города Москвы «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования» и Порядка дистанционного электронного голосования на выборах, назначенных на 19 сентября 2021 года» // СПС «КонсультантПлюс».

8. Постановление Конституционного Суда Российской Федерации от 30.05.2024 № 27-П по делу о проверке конституционности подпункта 57 статьи 2 и подпунктов «в», «в-1» пункта 24 статьи 38 Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» в связи с жалобой гражданки Е.Г.Силаевой // Российская газета. – № 134. – 21.06.2024.

9. Постановление Пленума Верховного Суда РФ от 27.06.2023 № 24 «О некоторых вопросах, возникающих при рассмотрении судами административных дел о защите избирательных прав и права на участие в референдуме граждан Российской Федерации» // Российская газета. – № 149. – 10.07.2023.

10. Постановление Пленума Верховного Суда РФ от 25.06.2024 № 17 «Об отдельных вопросах, возникающих у судов при рассмотрении дел об административных правонарушениях, посягающих на установленный порядок информационного обеспечения выборов и референдумов» // Российская газета. – № 149. – 10.07.2024.

11. Дудченко О. С., Фролова Т. Ю. Цифровизация в избирательном праве: зарубежный опыт // Экономика и право в новых реалиях: вызовы современности: монография. – Ростов-на-Дону: Манускрипт, 2024. – С. 52–65.

12. Ильиных А. В. Отдельные аспекты реализации и защиты права быть избранным в органы государственной власти и органы местного самоуправления // Государственная власть и местное самоуправление. 2023. № 10. С. 38–42.

13. Филатова А. О. Содержание и судебная защита конституционного права быть избранным в органы государственной власти и местного самоуправления в Российской Федерации: дисс. ... канд. юр. наук: 12.00.02. – РГУП, Москва, 2018 – 143 с.

14. Минюст хочет разрешить кандидатам указывать род деятельности как «самозанятой» // Официальный сайт «Ведомости» [Электронный ресурс]. – URL: <https://www.vedomosti.ru/politics/articles/2024/07/29/1052482-minyust-hochet-razreshit-kandidatam-ukazivat-rod-deyatelnosti-kak-samozanyatii>

15. Почему самозанятой отказали в регистрации муниципальным кандидатом, разберется КС // Сайт Российского агентства правовой и судебной информации РАПСИ [Электронный ресурс]. – URL: [https://www.rapsinews.ru/judicial\\_news/20240401/309772587.html](https://www.rapsinews.ru/judicial_news/20240401/309772587.html)

**Н. И. Шумакова,**

доцент кафедры конституционного и административного права,  
Южно-Уральский государственный университет  
(национальный исследовательский университет)

## **НОВЫЕ ТРЕНДЫ В ПРАВОВОМ РЕГУЛИРОВАНИИ ЦИФРОВОЙ СРЕДЫ И ЗАЩИТЫ ПРАВ ЧЕЛОВЕКА: ЗАРУБЕЖНЫЙ ОПЫТ**

**Аннотация.** В статье обосновывается невозможность на национальном уровне своевременно отвечать вызовам цифровизации – принимаемые меры влекут за собой ограничение фундаментальных прав человека, таких как право на свободу слова и выражения мнений, одновременно демонстрируя свою низкую эффективность вследствие отсутствия в цифровой среде государственных границ. Поставленная цель достигается посредством анализа новейшего законодательства и правоприменительной практики в релевантной сфере посредством применения совокупности общенаучных и частных научных методов. Результатом проведенного анализа является выявление общего и различного в подходах к регулированию цифровой среды в зарубежном праве (Китай, США, Европейский Союз, Великобритания, Бразилия, Норвегия), установление общих трендов в изменении законодательства стран с различными политическими режимами и формами правления.

**Ключевые слова:** свобода выражения мнений, свобода информации, свобода слова, префильтрация контента, права человека, цифровая среда, цифровые технологии, блокировка контента, правовое регулирование цифровой среды

## **NEW TRENDS IN LEGAL REGULATIONS OF DIGITAL SPACE AND PROTECTION OF HUMAN RIGHTS: FOREIGN EXPERIENCE**

**Abstract.** The author substantiates the impossibility of an adequate response to the challenges of digitalization at the national level in a timely manner – the taken measures led to restriction of fundamental human rights such as the right to freedom of speech and the right to freedom of expression, whilst demonstrating their low efficiency due to the absence of state borders in the digital space. To achieve the stated goal, the author conducts an analysis of the latest legislation and law enforcement practice in the relevant area by employing a set of general scientific and specific scientific methods. The obtained results identify the different and the common in approaches towards the legal regulation of the digital space in foreign law (China, USA, European Union, Great Britain, Brazil, Norway), and spot general trends in legislations changing in countries with different political regimes and forms of government.

**Keywords:** freedom of expression, freedom of information, freedom of speech, prefiltration of content, digital space, digital technologies, content-blocking, legal regulations of digital space

**Введение.** В 2024 году уже не вызывает сомнений то, что цифровая среда стала новым публичным пространством, требующим особого законодательного регулирования ввиду специфики реализации в ней прав человека и гражданина, в частности права на свободу слова, творчества и информации. Способствующие распространению языка ненависти, ультра-правой идеологии и идей насильственного экстремизма, возникающие в нем правоотношения также оказывают непосредственное влияние на изменения в национальных законодательствах европейских государств, таких как Германия, пытающаяся найти баланс между реализацией гарантированной конституцией свободой выражения мнений и защитой прав и законных интересов своих граждан в социальных сетях и стриминговых платформах [6] и ограничением распространения противоправного контента, или Бразилия, в попытках противостоять распространению дезинформации среди населения, избравшая радикальный путь штрафов и блокировок определенных платформ.

Опасение при этом вызывают не только возможность поляризации населения посредством социальных медиа [2], оказание давления на формирование политических взглядов несовершеннолетних [7] и иные социальные вызовы национальной безопасности, где в роли краеугольного камня зачастую выступает религия и взаимодействие различных религиозных групп между собой, но также безопасность данных пользователей, где угрозу могут представлять в том числе используемые третьими лицами технологии активного прослушивания, к использованию которых, как недавно было установлено независимым журналистским расследованием, могут прибегать такие гигантские корпорации как Google и Amazon.

Меры противодействия перечисленным рискам регулярно принимаются на национальных уровнях, но не всегда показывают свою эффективность вследствие отсутствия в цифровой среде каких-либо границ, она является глобальным, в то время как государствам свойственны попытки подчинить киберпространство собственным политическим амбициям посредством сбора данных, оказания давления на интернет-платформы и использования иных механизмов формирования так называемого суверенного интернета [1. С. 270]. О недостаточности их эффективности можно сделать вывод после изучения документов международных организаций.

Так, во «Всемирном докладе по мониторингу образования, 2023 год: технологии в сфере образования: кто диктует условия для этого инструмента?», эксперты ЮНЕСКО, изучая применение новых технологий в процессе образования, отмечают, что вследствие отсутствия за цифровыми платформами должного государственного контроля даже коллективные образовательные ресурсы помимо положительного эффекта, создают новые риски, связанные, в том числе с хранением данных несовершеннолетних, что требует изменения национальных законодательств и принятия новых стандартов, направленных на обеспечение благополучия и безопасности обучающихся и обучающихся.

ЮНЕСКО также предупреждает о росте проблемы кибер-буллинга, мошенничества, кражи данных, и в целом негативного влияния социальных сетей на физическое и психическое благополучие детей и молодежи. Контртеррори-

стическое отделение ООН, в свою очередь, признало, что цифровая среда создает благоприятные условия для распространения экстремистской идеологии, радикализации населения, распространения дезинформации и различных вредных нарративов, включив в свою «Глобальную программу по предупреждению насильственного экстремизма» рекомендации для стран-участниц по развитию стратегической коммуникации с организациями гражданского общества в целях противодействия угрозам миру и безопасности.

Программа развития ООН дополнительно акцентирует внимание, что меры противодействия распространению экстремистских идей и идеологий в цифровой среде в большинстве случаев заключаются в перекладывании ответственности на владельцев платформ социальных сетей, от которых требуют своевременного удаления противоправного контента, а несоблюдение данного требования влечет за собой наступление санкций в виде денежных штрафов, что также не является эффективным способом противодействия, поскольку:

1) ведет к увеличению давления на небольшие платформы и влечет к удалению контента, не являющегося противоправным;

2) экстремистские группировки переходят в так называемый «Темный интернет» или «Даркнет» и правоохранительные органы утрачивают возможность мониторинга их активности;

3) экстремистские группировки разрабатывают методы обхода обнаружения противоправного контента либо создают «вредный, но законный» контент, удаление которого может основываться только на субъективной интерпретации вреда, а потому может оказывать негативное влияние на свободу выражения мнений;

4) для поиска противоправного контента применяются технологии ИИ, способные вести к дискриминации индивидов и маргинализированных групп.

Целью данной статьи является обоснование невозможности на национальном уровне своевременно отвечать вызовам цифровизации – принимаемые меры влекут за собой ограничение фундаментальных прав человека таких как право на свободу слова и выражения мнений, одновременно демонстрируя свою низкую эффективность вследствие отсутствия в цифровой среде государственных границ.

Для достижения поставленной цели проведен анализ новейшего законодательства и правоприменительной практики в релевантной сфере посредством применения совокупности общенаучных (анализ, синтез, контент-анализ, индукция, дедукция) и частных научных методов (конкретно-социологический метод изучения государственно-правовых явлений, методы сравнительного правоведения).

Результатом проведенного анализа является выявление общего и различного в подходах к регулированию цифровой среды в зарубежном праве, установление общих трендов в изменении законодательства стран с различными политическими режимами и формами правления.

Научная новизна проведенного исследования определена его гипотезой – правовое регулирование цифровой среды не может эффективно осуществляться без ограничения прав и свобод человека, а потом требует создания новых норм международного права, разработки глобальных стандартов, универсальных методов и инструментов регулирования и контроля.

Полученные результаты имеют практическую значимость и могут быть использованы в качестве основы для дальнейших исследований и разработки правовых норм, направленных на обеспечение безопасности и благополучия в цифровой среде.

Основным ограничением исследования являются рестрикции доступа для пользователей Интернета с российскими IP-адресами к зарубежным нормативным правовым актам и актам правоприменения.

**Основная часть.** Неотвратимый процесс цифровизации продолжает трансформировать все сферы жизни общества и государства, оказывая влияние на индивидов, их способы и виды взаимодействия, психическое здоровье и когнитивные способности [3. С. 272–274]; на взаимодействие правоохранительных органов с гражданами [5. С. 553, 556–566] и даже на эффективность отправления государственными органами своих функций и полномочий в условиях формирования новой реальности, диктующей их присутствие в цифровой среде [8]. При этом влияние это может быть как положительным, так и отрицательным. Отрицательное влияние здесь, прежде всего, связывают с беспрепятственным распространением информации, анонимностью и отсутствием государственного контроля за цифровой средой, что рассматривается как часть реализации права человека на свободу информации и выражения мнений [4. С. 30–31].

Такой подход, в частности, практикует Норвегия, в 2021 году королевство запустило кампанию «Стратегия поощрения свободы выражения мнений в норвежской внешней политике и политике развития», которая преследует своей целью дальнейшее развитие данной свободы на международном уровне. В п. 1.3. одноименного документа кампании, норвежский МИД признает важность для поддержки и сохранения демократических институтов возможности представителей разных национальностей и культур взаимодействовать между собой, но в этом же пункте указывает на широкое распространение в цифровой среде языка ненависти, манипуляцию мнением населения, рост дезинформации, онлайн-насилия и так далее как угрозу правам человека. Ссылаясь в п. 1.4. на положения «Руководящих принципов предпринимательской деятельности в аспекте прав человека ООН», к предпринимателям в котором, очевидно, в данном контексте относятся и владельцы интернет-платформ, напоминают об ответственности коммерческих предприятий в случае непринятия ими своевременных мер по предотвращению и/или смягчению фактических и потенциальных неблагоприятных последствий их деятельности для прав человека. В п. 4.1. вновь обращается внимание на угрозы, вызванные работой систем рекомендаций контента вкупе с неадекватным модерированием контента, и признается возможность возникновения необходимости введения государственного надзора за цифровым пространством на условиях ненарушения права на частную жизнь и сохранения технологий, используемых для сохранения анонимности.

Основные же стратегические меры создания безопасной цифровой среды для свободы слова и выражения мнений указаны в п. 4.5, особого внимания среди которых в рамках проводимого исследования заслуживают два пункта:

- 1) построение межкультурного диалога и ликбез;

2) создание новой международной нормативной базы, которая будет способна обеспечить своевременную идентификацию опасного контента и его удаление в социальных сетях.

В попытке защитить демократические институты, Норвежское управление по защите данных обязало дочернюю компанию одной из крупнейших корпораций на рынке социальных сетей (Irish Meta<sup>3</sup>, принадлежащую признанной в Российской Федерации экстремистской и запрещенной Meta<sup>4</sup>, и оказывающую услуги запрещенной в России социальной сети ) изменить политику в отношении сбора данных подданных королевства, наложив на нее обязательный штраф в размере одного миллиона норвежских крон в сутки, поскольку коммерческая слежка в маркетинговых целях незаконна и собирает большое количество данных о частной жизни, что позволяет манипулировать мнением индивида, способствует укреплению стереотипов и оказывает иное вредное воздействие на свободу информации и выражения мнений, компания попыталась оспорить данное решение как несоразмерное в Окружном суде Осло, ссылаясь на несоразмерность примененных к ним санкций, но суд принял сторону управления, в своем решении указав, что считать приказ о прекращении незаконной деятельности несоразмерным нельзя (дела за номерами 23-114365TVI-TOSL/08 и 23-114359TVI-TOSL/08).

Более радикальный путь избрала Бразилия, где Федеральный верховный суд заблокировал социальную платформу X за несоблюдение законов республики и неуплаты штрафов, манипуляцию мнением избирателей и другие действия, влекущие создание «атмосферы полной безнаказанности», а за обход физическими и юридическими блокировки установил наказание в виде штрафа в размере 50.000 реалов в сутки (дело за номером PET 12404 – петиция Александра де Мораеса).

Со штрафами и блокировками сталкивается и еще один социал-медиа гигант – принадлежащий китайской компании ByteDance TikTok. Так, президент США Джо Байден одобрил внесенный Палатой Представителей законопроект, направленный на «защиту национальной безопасности Соединенных Штатов от угрозы, исходящей от контролируемых иностранным противником приложений, таких как TikTok» и иных приложений и сервисов, разработанных ByteDance, либо находящихся под их контролем, где незаконным признается в том числе распространение и обновление таких приложений. Ранее Итальянское конкурентное ведомство наложило штраф в размере 10 000 000 евро на три дочерние компании the Bytedance Ltd group за непринятие адекватных мер по своевременному удалению потенциального опасного для несовершеннолетних контента (решение за номером PS12543). Стоит отметить, что Итальянский орган регулирования связи также резолюцией № 298/23/CONS от 22 ноября 2023 принял регламент, определяющий процедуры ограничения распространения контента в целях защиты прав и законных интересов несовершеннолетних, а также разработал правила, распространяющиеся на создателей контента – от инфлюенсеров до

---

<sup>3</sup> Мета – организация признанная экстремистской, ее деятельность запрещена на территории Российской Федерации.

<sup>4</sup> То же.

любителей мемов, где одним из руководящих принципов является уважение человеческого достоинства.

В свою очередь, Франция приняла закон за номером № 2023-451, направленный на правовое регулирование деятельности так называемых «инфлюенсеров», которых ст. 1 определяет как «физических или юридических лица, которые за определенную плату мобилизуют свою известность среди своей аудитории для доведения до всеобщего сведения с помощью электронных средств контента, направленного на прямое или косвенное продвижение товаров, услуг или любых других целей, осуществляют коммерческую деятельность по влиянию с помощью электронных средств».

Ст. 10 данного нормативного акта допускает возможность модерации контента поставщиками услуг, ст. 15 обязывает операторов онлайн-платформ к сотрудничеству с государством, а ст. 4 состоит из перечня запретов для создателей контента – от рекламы никотиновой продукции до привлечения к съемкам экзотических животных. Для проводимого исследования интерес представляет и правоприменительная практика – в стране учрежден специальный отдел прокуратуры при Прокуратуре Парижа «J3: Боевой отдел по борьбе с киберпреступностью», именно по итогам его предварительного расследования был произведен арест создателя и директора сервиса TELEGRAM Дурова П. как соучастника ряда преступлений, включая распространение противоправного контента и отказ в сотрудничестве с правоохранительными органами.

Годом ранее, в 2023-м, во время общественных протестов Правительство Франции рассматривало полную блокировку всех социальных сетей на территории страны на период восстановления общественного порядка, а весной 2024, вновь обвинив интернет-платформы в подстрекательстве населения к участию в антиправительственных погромах, а Китай – во вмешательство во внутреннюю политику демократического государства, заблокировала на территории Новой Каледонии работу приложения TikTok в качестве меры противодействия организации общественных беспорядков. Положения французских нормативных правовых актов перекликаются с Регламентом (ЕС) 2022/2065 Европейского парламента и Совета от 19 октября 2022 г. «О едином рынке цифровых услуг» и Регламентом (ЕС) 2022/1925 Европейского парламента и Совета от 14 сентября 2022 г. «О состязательных и справедливых рынках в цифровом секторе и о внесении изменений», действие которых распространяется в том числе и «на онлайн-сервисы посредничества, онлайн-поисковые системы, операционные системы, онлайн-социальные сети, сервисы платформ обмена видео, независимые от номера межличностные коммуникационные сервисы, облачные сервисы, виртуальных помощников, веб-браузеры и онлайн-рекламные сервисы, включая сервисы посредничества в рекламе» (п.14 Регламента 2022/1925), поскольку они также оказывают влияние на большое количество физических и юридических лиц. Накладываемые же обязательства и ограничения объясняются как необходимые для решения проблем в государственной политике, «принимая во внимание необходимость охраны общественного порядка, защиты частной жизни и борьбы с мошеннической и обманной коммерческой практикой», также уточняется, что

иных, менее ограничительных и более эффективных мер на сегодняшний день не существует (п. 35 Регламента 2022/1925).

Не осталась в маргинальном меньшинстве и Великобритания, принявшая «Закон об интернет безопасности 2023», возложивший на провайдеров связи и поставщиков новые обязанности, связанные с обеспечением безопасности и благополучия населения в интернете (ч. 3–5) – так, например, согласно положениям секции 7, провайдеры сервисов коммуникации пользователя с пользователем несут обязанности по оценке рисков, связанных с распространением незаконного контента, а также обязаны сообщать уполномоченным органам об обнаружении такого контента. Оба этих правовых нормативных акта формируют так называемый «Цифровой закон» или «Пакет цифровых актов», где конечной целью является противодействие распространению противоправного контента, товаров и инструментов, а также увеличению прозрачности работы цифровых платформ и площадок, как следует из официального разъяснения Еврокомиссии.

Отдельно стоит остановиться на ст. 17 Директивы (ЕС) № 2019/790 «Об авторском праве и смежных правах на едином цифровом рынке», направленная на противодействие систематическому нарушению авторских прав на онлайн-платформах и сервисах обмена контентом, в основу которого должно лечь сотрудничество правообладателей с поставщиками услуг.

Правозащитники отмечают, что изначально данная статья содержала указание на применение инструментов распознавания контента для возможности удаления материалов, имеющих признаки нарушения авторского права, еще до их публикации, то есть, введение обязательной префилтрации контента, и, хотя в конечной редакции от данного положения было решено отказаться, обработка больших объемов информации каким-либо иным способом невозможна, что создает риск свободе выражения мнений.

Заслуживают внимания и выпущенные Государственной канцелярией интернет-информации КНР требования к технологическим компаниям по модерации и аутентификации всего контента, размещаемого на Интернет-платформах, озаглавленные как «Руководящие принципы для ‘Самомедиа’».

От платформ веб-сайтов требуют:

1) усиления проверки достоверности информации при регистрации, оперативной проверки достоверности вносимых изменений и отказа в услугах в случае выявления недостоверных данных;

2) проверки необходимых сертификатов и иных подтверждений квалификации, в случае, если деятельность «самомедиа» связана с производством информационного контента в сфере финансов, образования, медицины и здравоохранения, юстиции и других областях – такие «самомедиа» подлежат специальной маркировке;

3) стандартизации маркировки информации – если «самомедиа» публикует информацию, касающуюся текущих событий внутри страны и за рубежом, государственной политики, социальных событий и т. д. Интернет-платформы должны требовать от них точного обозначения источника информации и ее отображения на видном месте при публикации, собственные фото и видео на страни-

цах «самомедиа» также подлежат маркировке, как и созданные с применением технологий генеративного искусственного интеллекта;

4) запрашивания от «самомедиа» подтверждения достоверности информации;

5) контроля за соблюдением «самомедиа» требований по маркировке художественного вымысла;

6) маркировки спорной информации и ограничения ее распространения;

7) маркировки и опровержения слухов, распространения опровержения с использованием алгоритмов рекомендации;

8) стандартизации процесса регистрации «самомедиа», предотвращения перерегистрации заблокированных учетных записей;

9) усиления контроля за выдачей и приставкой монетизации контента;

10) усиления контроля за ограничением прибыли от незаконной деятельности, если те «нарушают общественный порядок и добрые нравы или занимаются злонамеренным маркетингом, связывая несколько учетных записей для спекуляций на горячих социальных событиях»;

11) передачи данных о «самомедиа», занимающихся противоправной деятельностью, в уполномоченные государственные органы;

12) установления контроля за возможностью подписки на «самомедиа», уличенные в противоправной деятельности;

13) оперативного выявления и блокировки «самомедиа», нарушающих закон с внесением их в специальную базу данных и передачей информации о их деятельности уполномоченным государственным органам;

14) ведения специальных образовательных рубрик на своих платформах в превентивных целях.

Таким образом, Китай, с одной стороны, тоже переложил ответственность непосредственно на сами социальные медиа и иные площадки, с другой – усилил контроль за деятельностью блогеров и иных создателей контента, которые в новом нормативном акте обозначены как «самомедиа». До этого деятельность блогеров в КНР также попала под регулирование «Закона о рекламе», в частности, ст. 44 устанавливает, что действие закона распространяется на рекламу в Интернете, тем самым определяя какую продукцию и каким образом могут рекламировать «инфлюенсеры», а ст. 45 устанавливает обязанность для операторов телекоммуникационного бизнеса и поставщиков информационных услуг удалять незаконную и противоправную рекламу.

В Китае также установлен государственный контроль за всей религиозной активностью и взаимодействиями на религиозную тематику в цифровой среде, как следует из ст. 1 «Мер по администрированию служб религиозной информации в Интернет», принят данный нормативный акт в целях защиты прав граждан на свободу религиозных убеждений. В основе же этих законов лежит «Закон о кибербезопасности», например, в ст. 47 возложивший на сетевые операторов обязанности по «усилению управления информацией, предоставляемой их пользователями», то есть в случае выявления информации, раскрытие или передача которой запрещены законами или административными правилами, передача ее должна быть немедленно прекращена, создана регистрационная запись факта

передачи противоправных материалов для направления в компетентные органы и предприняты меры по уничтожению такой информации с целью предотвращения ее дальнейшего распространения, в то время ст. 68 устанавливает ответственность за не выполнение этих обязанностей, а ст. 58 и вовсе позволяет вводить ограничение связи в целях защиты общественной безопасности.

**Заключение.** Проведенный анализ показал, что общими трендом в правовом регулировании цифровой среды стали попытка распространения государственного контроля на общественные отношения, возникающие в ее пределах. Полученные результаты также позволяют выделить и общие инструменты реализации государственной политики в данной сфере, к которым относятся штрафы, ограничения и блокировки (контента, пользователей, платформ и сервисов).

Применение данных инструментов создает неразрешимый парадокс – защита прав человека осуществляется посредством их же существенных ограничений, в том числе гарантированных в ст. 8 (право на уважение семейной и частной жизни), ст. 10 (свобода выражения мнений), ст. 14 (запрещение дискриминации) Европейской конвенции о защите прав человека и основных свобод, ограничение которых предусмотрено положениями самой конвенции лишь в исключительных случаях, возведение же ограничения фундаментальных прав человека в норму ведет к искажению их сущности, и, в конечном итоге, к приданию им номинального статуса.

О том, что данный процесс уже запущен, свидетельствует пренебрежение правом на свободу выражения мнений Европейским Союзом во имя защиты авторского права, на что справедливо указывает Генеральный адвокат Хенрик Саугмандсгаард Йое в Деле С – 401/19 «Республика Польша против Европейского Парламента и Совета Европейского Союза», отмечая, что у ограничения прав и свобод человека существует абсолютный предел, который не может быть пересечен ни при каких обстоятельствах, а именно – их сущность.

Учитывая, что поставщикам услуг предоставлен выбор как именно проверять загружаемые файлы, можно предположить, что это спровоцирует возникновение дополнительных рисков, связанных с доступом к собранным данным, в том числе персональным.

Более того, текущая правоприменительная практика указывает на неэффективность таких мер, где ярким примером является попытка привлечения к уголовной ответственности владельцев сервисов и платформ как новая мера противодействия неадекватной модерации, способствующей росту преступлений в цифровой среде. Нельзя не согласиться и с официальной позицией МИДа Норвегии – без построения межкультурного диалога, повышения образования и правосознания граждан никакие из принимаемых меры не будут иметь должной эффективности. Эту позицию также разделяет специальный докладчик ООН Специальный докладчик по вопросам поощрения и защиты прав человека в условиях борьбы с терроризмом Фионнуала Ни Аолаин, в докладе A/HRC/52/39 «Последствия разработки, использования и передачи новых технологий в контексте борьбы с терроризмом и пресечения и предотвращения насильственного экстремизма» от 1 марта 2023 года подчеркивающая, что цифровые технологии имеют огромный потенциал для обеспечения позитивных изменений, связанных с

устойчивым повышением уровня жизни, гарантии и защиты прав человека, углублению и развитию коммуникаций при равномерном и надлежащем их использовании, и что использование их в противоправных целях, безусловно, представляет угрозу безопасности, однако установившаяся практика борьбы с распространением посредством установление ограничений способна усугубить ситуацию с распространением экстремизма и насильственного терроризма, кроме того, связанные с высоким риском технологии теперь применяются под эгидой защиты прав человека и обеспечению безопасности, но в действительности лишь способствуют дальнейшему ослаблению широкой коллективной безопасности и «подрывают» поощрение и защиту прав человека.

Можно также утверждать, что большинство стран сегодня тяготеет к адаптации китайского подхода к регулированию цифровой среды, где, во-первых, четко определены нормы взаимодействия в Интернете, то есть – пределы прав и свобод физических и юридических, во-вторых, установлены обязанности как для пользователей, так и для сетевых операторов и владельцев цифровых платформ и площадок, а в-третьих, определены пределы ответственности для всех участников взаимодействия в цифровой среде, включая поставщиков цифровых услуг, религиозных организаций и блогеров.

Тот самый подход, за который КНР подвергалась критике со стороны ООН как несоразмерный и нарушающий фундаментальные права человека, как, например в п. 26 «Оценки УВКПЧ проблем с правами человека в Синьцзян-Уйгурском автономном районе, Китайская Народная Республика», где нарушение прав человека Управление ООН по правам человека увидело в использовании Интернета, социальных сетей и сервисов обмена сообщениями и литературой, признанной в Китае экстремистской либо для обмена опытом и обучением на материалах, признанных экстремистскими, а также запрете использования Интернета для незаконного прослушивания, просмотра и распространения зарубежных религиозных радиопередач и телевизионных программ.

Исходя из изложенного, можно заключить, что демаркация цифровой среды с целью обеспечения национальных интересов и защиты прав и свобод граждан снижает эффективность мер противодействия вызовам цифровизации и глобализации, поскольку цифровое пространство безгранично и на каждую меру государственного регулирования находится контрмера как со стороны преступных групп, так и самих граждан, что создает эффект «снежного кома» и влечет ко все большему ограничению фундаментальных прав и свобод человека во имя их же защиты, искажая саму их сущность.

Более того, блокировка или наложение санкций, например, в рамках исполнения «Цифрового закона» Европейского Союза поражает не только права граждан стран, входящих в его состав, либо же пользователей, находящихся на его территории, но всех пользователей интернет-платформ и площадок без исключения, вне зависимости от их гражданства и территориального нахождения. По сути, глобальное пространство цифровой среды таким образом начинает функционировать по законам европейского политического объединения государств, хотя другие страны полномочиями такого глобального, все сетевого полицейского Евросоюз не наделяли.

Очевидно, что данный подход будет порождать противоречия в праве как внутреннем, так и международном, поскольку пределы ограничений прав человека и пределы установления ответственности для владельцев интернет-платформ и площадок в данном случае зависят исключительно от толкования их правоприменителем. Возникновение же судебных разбирательств, таких как Дело С-401/19 «Республика Польша против Европейского Парламента и Совета Европейского Союза», где одной из причин для подачи иска послужило толкование фундаментального права человека на свободу выражения мнений как менее значимого в сравнении с авторским правом, с чем Польша выразила свое несогласие, демонстрирует, что в будущем это можем создать почву для новых межгосударственных конфликтов, тем самым спровоцировав новую угрозу мировому порядку – риск, предотвращением которого в нынешней геополитической ситуации вряд ли можно пренебречь.

На культурном и социальном уровне негативные последствия курса ограничений и блокировок с передачей права управления цифровой средой коллективному Западу тоже не заставят себя ждать – такой курс способствует разобщенности, нарушению культурных связей и диалогов, разрушению профессиональных и межличностных связей, дальнейшей маргинализации и даже демонизации отдельных наций, групп и сообществ, а также усилению кризиса правды посредством введения цензуры и распространения пропаганды.

Отдельно необходимо поставить вопрос о том, почему во имя защиты прав детей и несовершеннолетних блокировке и цензуре подлежат Интернет-площадки, на которых этой категории находиться не должно. Здесь как раз наиболее адекватным является подход китайского законодателя, узаконившего проверку личных данных пользователя и борьбу с предоставлением ложной информации.

Подводя итог вышесказанному, можно сделать вывод о том, что из сложившегося нового глобального кризиса может быть два выхода: 1) создание новых норм международного права, разработка глобальных стандартов, универсальных методов и инструментов регулирования и контроля, что продиктовано неспособностью государств самостоятельно справляться с возникшими угрозами без существенного ограничения прав граждан; 2) признание на международном уровне факта неравноценности прав и свобод человека в реальной жизни правам и свободам человека в цифровой среде, для чего также необходима разработка новых норм международного права.

### Список литературы

1. Abdelkarim Y.A. Demarcation of Cyberspace: Political and Legal Effects of Applying the Concept of Sovereign States' Interests *Journal of Digital Technologies and Law*. – 2024. – DOI: 10.21202/jdtl.2024.14
2. Arora S. D., Singh G. P., Chakraborty A., Maity M. Polarization and social media: A systematic review and research agenda *Technological Forecasting and Social Change*. – 2022. – October. – DOI: 10.1016/j.techfore.2022.121942
3. Dai Z. Social Media and Mental Health: Examining the Relationship of the Use of Social Media to Anxiety *Lecture Notes in Education Psychology and Public Media*. – 2024. – August. – DOI: 10.54254/2753-7048/58/20241771
4. Ganesh B. THE UNGOVERNABILITY OF DIGITAL HATE CULTURE *Journal of International Affairs*. – 2018. – Spring/Summer.
5. Hu X., Rodgers K. et al “We are more than crime fighters”: Social media images of police departments *Police Quarterly*. – 2018. – December. – DOI: 10.1177/1098611118783991
6. Maaß S., Wortelker J., et al Evaluating the regulation of social media: An empirical study of the German NetzDG and Telecommunications Policy. –2024. – June. – DOI: <https://doi.org/10.1016/j.telpol.2024.102719>
7. Oden A., Porter L. The Kids Are Online: Teen Social Media Use, Civic Engagement, and Affective Polarization *Social Media + Society*. – 2023. – July. – DOI: 10.1177/20563051231186364
8. Yang C., Gu M. et al. Government in the digital age: Exploring the impact of digital transformation on governmental efficiency *Technological Forecasting and Social Change*. – 2024. – November. – DOI: <https://doi.org/10.1016/j.techfore.2024.123722>

## ЦИФРОВАЯ БЕЗОПАСНОСТЬ И ПРАВО

**А. В. Белякова,**

кандидат юридических наук, ведущий научный сотрудник,  
Институт законодательства и сравнительного правоведения  
при Правительстве Российской Федерации

### ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Аннотация.** Стремительное развитие информационных технологий во всех областях и сферах жизнедеятельности приводит к тому, что правовое регулирование не успевает адаптироваться к новейшим технологиям. В настоящее время правовое регулирование в рассматриваемой сфере крайне разрознено и фрагментарно, что приводит к необходимости переосмысления действующего законодательства. Предлагается проанализировать имеющиеся пробелы в данной области и сформулировать ряд предложений по дальнейшему развитию направления с учетом междисциплинарного подхода.

**Ключевые слова:** кибернетика, информационные технологии, искусственный интеллект, информационная безопасность, роботизация, право, правовое регулирование

### FEATURES OF LEGAL REGULATION IN THE FIELD OF INFORMATION SECURITY

**Abstract.** The rapid development of information technology in all sectors and spheres of life has led to a situation where legal regulation has not kept up with the latest technologies. At present, legal regulations in this area are highly fragmented and scattered, necessitating a rethinking of current legislation. This paper proposes to analyze the gaps in this field and formulate some proposals for the future development of this area drawing on an interdisciplinary approach.

**Keywords:** cybernetics, information technology, artificial intelligence, information security, robotics, law, legal regulation

Внедрение цифровых продуктов и алгоритмов в государственное управление и социально-экономические отношения набирает обороты, являясь объективной необходимостью в эпоху совершенствования технологических и информационных процессов.

Юриспруденция, правовая система, право, государственное и муниципальное управление вынуждены адаптироваться к изменениям в обществе, экономике, науке, технике, политике и государственном устройстве. С одной стороны, цифровые и электронные продукты упрощают и оптимизируют процессы и выполнение задач, в том числе в условиях многозадачности, а с другой стороны, существуют риски чрезмерного использования искусственного интеллекта и минимизации человеческого фактора.

Существует ряд сфер профессиональной деятельности, где замена экспертов и специалистов роботами и информационными системами может привести к фатальным ошибкам. Общеизвестным фактом является то, что в настоящее время технический прогресс способствует росту мошеннических и иных преступных схем с использованием информационных технологий, что позволяет злоупотреблять правом, нарушать личные границы и конституционно-правовые гарантии.

Сформировавшийся массив нормативных правовых актов и локальных актов, содержащих нормы об исследуемой области, имеет фрагментарную регламентацию данного рода общественных отношений в большинстве кодифицированных источников права России. При этом в правовой доктрине уже многие годы идут обсуждения по вопросу о необходимости кодификации и систематизации правовых норм данной сферы. Обсуждаются вопросы о «цифровом кодексе» [1; 2; 4], «информационном кодексе» [3] и т. п. При этом единого мнения по данному аспекту среди правоведов до настоящего времени не сформировалось. Автор полагает, что это связано в первую очередь с тем, что отсутствует междисциплинарный подход к развитию данной отрасли.

Ревизия нормативных актов в данной области необходима по ряду причин. Одна из основных – повсеместная цифровизация социально-экономических отношений, которая приводит к увеличению числа информационных систем в различных отраслях, сферах и областях. Их реализация приводит к тому, что традиционные способы осуществления тех или иных задач видоизменяются, трансформируются, в том числе возникают и негативные тенденции, приводящие к нарушению прав, свобод и законных интересов как частных лиц, так и неограниченного круга. В связи с этим полагаю, что осуществление правового мониторинга позволит оптимизировать процессы технологизации современного общества. Для этого необходимо развивать междисциплинарный, комплексный подход и стремиться к межведомственному взаимодействию.

Таким образом, предлагаем разработать единую национальную концепцию развития кибернетики и информационной безопасности, обращаясь к мнению как юристов, так и технических специалистов.

### Список литературы

1. Вайпан В. А. Источники цифрового права // Вестник арбитражной практики. – 2024. – № 1. – С. 3–29.
2. Жарич А. В. Национальные и международные предпосылки создания Цифрового кодекса РФ // Цивилист. – 2023. – № 4. – С. 5–9.
3. Нестеров А. В. Цифровое право против информационного кодекса // Юрист. – 2021. – № 11. – С. 8–12.
4. Рожкова М. А. Является ли цифровое право отраслью права и ожидать ли появления цифрового кодекса? // Хозяйство и право. – 2020. – № 4(519). – С. 7.

**А. Р. Богданова,**  
аспирант,  
Казанский инновационный университет  
имени В. Г. Тимирязова

## **РОЛЬ ГОСУДАРСТВА В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ**

**Аннотация.** В статье анализируется роль государства в обеспечении безопасности критической информационной структуры. Обосновывается важность и актуальность обеспечения подобной защиты и участия государства в управлении. Кратко описаны основные функции государства и стратегии обеспечения защиты. Подчеркивается общая концепция национальной безопасности в качестве основной темы по обеспечению информационной безопасности. Автор делает вывод, что государство играет важнейшую роль в обеспечении безопасности критической информационной инфраструктуры, поскольку государство разрабатывает основные концепции обеспечения защиты и контролирует их.

**Ключевые слова:** кибербезопасность, государство, критическая информационная инфраструктура, национальная безопасность

The article analyzes the role of the state in ensuring the security of the critical information structure. The importance and relevance of ensuring such protection and state participation in management are substantiated. The main functions of the state and strategies for ensuring protection are briefly described. The article presents the main goals and ideals of ensuring the protection of the Russian Federation and China. The article emphasizes the general concept of national security as the main concept for ensuring information security. The author concludes that the state plays a vital role in ensuring the security of the critical information infrastructure, since the state develops the main concepts of the direction of ensuring protection and controls them.

**Keywords:** cybersecurity, state, critical information infrastructure, national security

Вопросы обеспечения национальной безопасности в целом, и обеспечение непосредственно информационной безопасности, в частности, являются ведущими направлениями деятельности на современном этапе развития государства [1].

Национальная безопасность является предпосылкой национального развития. Так, например, Китайская Народная Республика (далее – КНР), крайне обеспокоена обеспечением кибербезопасности, так как 14-й пятилетний план и план развития до 2035 года рассматривают «координацию развития и безопасности и построение более безопасного Китая на более высоком уровне» как важную руководящую идеологию, расширяя горизонты и теории исследования управления рисками безопасности [2]. Безопасность критической информационной инфраструктуры (далее – КИИ) связана с национальной экономикой и жизнедеятель-

ностью людей. Она играет важную роль для национальной экономики и жизнедеятельностью людей в разных сферах [3].

КИИ является важным краеугольным камнем, поддерживающим функционирование страны и общества, охватывая многие отрасли и сферы. Поэтому обеспечение безопасности КИИ является важной гарантией поддержания национальной безопасности и социальной стабильности. Генеральный председатель КНР Си Цзиньпин подчеркивает, что КИИ в сфере финансов, энергетики, электроснабжения, связи и транспорта требует обеспечения крайне высокого уровня безопасности [4].

Государства в целях обеспечения безопасности КИИ разрабатывают различные нормативные правовые акты, которые обеспечивают прочную правовую основу для развития этого института. Эти акты определяют сферу действия КИИ, принципы защиты, систему надзора и управления, обязанности операторов, формулируют меры безопасности, а также устанавливают юридическую ответственность, закладывая прочную правовую основу для всех сторон. Законодательство государств о защите КИИ закрепляют наиважнейшие принципы управления такими объектами, защиту информации, обеспечение устойчивости КИИ в целом и ее отдельных элементов, а также управление кризисами и чрезвычайными ситуациями [5].

Страны обеспечивают создание систем и механизмов управления для защиты КИИ, подробно определяющих роли национальных ведомств и органов по обеспечению кибербезопасности. Государства регулируют создание механизмов обмена информацией, координирует обмен информацией о состоянии обеспечения кибербезопасности между ведомствами, координирует соответствующие департаменты и органы для создания механизма реагирования между соответствующими департаментами, департаментами защиты, операторами и службами по кибербезопасности.

Государства поощряют и поддерживают инновации в области технологий кибербезопасности для повышения эффективности сетевой защиты. Важно отметить также роль государства в усилении надзора и контроле правоприменения. Так, соответствующие национальные ведомства обеспечивают надзор и контроль правоприменения в отношении КИИ и обеспечивают профилактику нарушений законодательства.

Таким образом, можно сказать, что государство посредством политического воздействия, финансовой поддержки и других мер, играет незаменимую роль в обеспечении безопасности КИИ. Именно государство предоставляет надежные гарантии обеспечения безопасности КИИ путем разработки нормативных правовых актов, создания систем и механизмов управления, предоставления технической поддержки, усиления надзора и управления, проведения проверок систем безопасности, а также содействия инновациям в области технологий защиты безопасности и промышленного развития. И, если государство продолжит расширять возможности независимых инноваций, укреплять механизмы мониторинга рисков безопасности и раннего оповещения, а также укреплять международное сотрудничество и обмены для всестороннего повышения уровня защиты КИИ, это поможет обеспечить безопасную и стабильную работу КИИ, окажет

мощную поддержку экономическому и социальному развитию, а также будет способствовать повышению статуса и влияния самой страны в сфере международной кибербезопасности.

### Список литературы

1. Горохова С.С. О некоторых аспектах обеспечения безопасности критической информационной инфраструктуры в Российской Федерации // Право и политика. 2018. № 6.
2. 王驰, 曹劲松.数字新型基础设施建设下的安全风险及其治理[J].江苏社会科学, 2021, 318(05):88-99+242-243. Ван Чи, Цао Цзиньсун. Риски безопасности и управление при создании новой цифровой инфраструктуры [J]. Jiangsu Social Sciences, 2021, 318(05):88-99+242-243.
3. 张艺腾.总体国家安全观视域下的关键信息基础设施 安全防护[J].网络安全技术与应用, 2023, 267(03):158-160. Чжан Итэн. Защита безопасности критической информационной инфраструктуры с точки зрения общей национальной безопасности [J]. Технологии и приложения сетевой безопасности, 2023, 267(03):158-160.
4. 中共中央党史和文献研究院.论党的宣传思想工作[M].北京:中央文献出版社, 2020. Научно-исследовательский институт истории партии и литературы при ЦК КПК. О пропагандистской и идеологической работе партии[M]. Пекин: Центральное литературное издательство, 2020.
5. Jangirala, Srinivas & Das, Ashok Kumar & Kumar, Neeraj. (2018). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems. 92. 10.1016/j.future.2018.09.063.

**Е. В. Булгакова,**

кандидат юридических наук, доцент,  
Московский университет Министерства внутренних дел  
Российской Федерации имени В. Я. Кикотя

**А. Н. Кубанков,**

доктор военных наук, профессор,  
Московский технический университет связи и информатики

**К. А. Гудкова,**

магистрант,  
Финансовый университет  
при Правительстве Российской Федерации

**В. В. Булгаков,**

курсант,  
Московский университет Министерства внутренних дел  
Российской Федерации имени В. Я. Кикотя

## **ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКИХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ: КОНЦЕПЦИЯ КИБЕРИММУНИТЕТА**

**Аннотация.** В статье представлен анализ текущей ситуации на рынке средств обеспечения информационной безопасности. В рамках исследования выделены основные виды санкций в отношении российских финансовых институтов и их влияние на стратегии защиты. В работе проанализированы возможности применения кибериммунных систем для обеспечения информационной безопасности кредитно-финансовой сферы.

**Ключевые слова:** кибериммунитет, информационная безопасность, финансовые организации, импортозамещение, критическая информационная инфраструктура, защита информации, искусственный интеллект, машинное обучение

## **ENSURING INFORMATION SECURITY OF RUSSIAN FINANCIAL INSTITUTIONS: THE CONCEPT OF CYBER IMMUNITY**

**Abstract.** The article provides an analysis of the current situation in the information security market. The study highlighted the main types of sanctions against Russian financial institutions and their impact on defense strategies. The paper analyzed the possibilities of using cyber-immune systems to ensure the information security of the credit and financial sector.

**Keywords:** cyber immunity, information security, financial institutions, import substitution, critical information infrastructure, information protection, artificial intelligence, machine learning

**Введение.** В условиях современной геополитической обстановки и санкционного давления на Россию, вопрос обеспечения информационной безопасно-

сти финансовых организаций приобретает особую актуальность. Основными факторами, оказывающими влияние на текущую ситуацию, выступают ограничения на поставки зарубежного оборудования и программного обеспечения, отключение от международных платежных систем, а также возросшая активность хакеров.

В данной работе проводится анализ возможностей применения кибериммунных систем для обеспечения кибербезопасности российских банков. Цель исследования – выявление потенциала внедрения данной технологии для противодействия современным киберугрозам. В рамках работы будут рассмотрены основные виды санкций, влияющие на информационную безопасность, проанализировано текущее состояние рынка средств защиты информации (далее – СЗИ), а также изучены принципы и преимущества концепции кибериммунитета.

**Основная часть.** Современное геополитическое противостояние все чаще переходит в киберпространство, где одним из ключевых инструментов борьбы становятся киберсанкции. Эти меры, аналогичные традиционным санкциям (запрет на поездки, заморозка активов), применяются для сдерживания и наказания за кибератаки. Однако использование кибервозможностей в конфликтах может привести к эскалации напряженности и нанести ущерб гражданской инфраструктуре, имея серьезные последствия для общества [1].

Западные страны активно используют ограничения доступа России к передовым информационным и коммуникационным технологиям (далее – ИКТ) как инструмент геополитического и экономического давления. Эти меры, включающие экспортный контроль, и ужесточаются меры по соблюдению санкций, направлены на ослабление военного и экономического потенциала России. Несмотря на то, что полностью прекратить использование западных ИКТ в России не удалось, эти ограничения, по мнению западных аналитиков, уже нанесли значительный ущерб российской экономике и технологическому развитию, что будет иметь долгосрочные последствия [2].

Российский рынок кибербезопасности переживает период перехода и адаптации. До недавнего времени иностранные компании играли ключевую роль, занимая 24,2 % рынка ключевых вендоров СЗИ в 2022 году [3]. Однако начало специальной военной операции привело к пересмотру стратегий и изменению ситуации на рынке.

Согласно Yale CELI List of Companies – списку иностранных организаций, оперирующих в России, ряд компаний, связанных со сферой информационных технологий прекратили или значительно сократили свое присутствие в стране, однако многие продолжают свою деятельность в обычном режиме. Как видно из Таблицы 1, некоторые поставщики, такие как Cisco и IBM, полностью прекратили любые виды сотрудничества, другие, такие как Check Point, Fortinet и ESET, либо сохранили, либо временно сократили свое присутствие. Доминирование сетевых решений безопасности и высокий рейтинг иностранных поставщиков в этом сегменте подчеркивают их важную роль на российском рынке решений кибербезопасности. В сложившейся ситуации открываются возможности для отечественных разработчиков, способных заполнить образовавшиеся ниши и ускорить процесс импортозамещения. Дальнейшее развитие ситуации будет зависеть от долго-

срочных стратегий как иностранных вендоров, так и российских компаний, а также от эффективности государственных программ поддержки импортозамещения.

**Перечень значимых иностранных поставщиков и их позиция  
на российском рынке**

| <b>Компания</b>                   | <b>Категория СЗИ</b>                                     | <b>Статус</b>                                                      | <b>Группа по Yale CELI list</b> | <b>Место в рейтинге ЦСР (в своей категории)</b> |
|-----------------------------------|----------------------------------------------------------|--------------------------------------------------------------------|---------------------------------|-------------------------------------------------|
| Check Point Software Technologies | Средства защиты сетей (network security)                 | Продажа продуктов кибербезопасности в России                       | F                               | 1                                               |
| Fortinet                          | Средства защиты сетей (network security)                 | Временно сократил операции, сохраняя при этом возможности возврата | B                               | 2                                               |
| Cisco                             | Средства защиты сетей (network security)                 | Свернул деятельность                                               | A                               | 3                                               |
| IBM                               | Средства защиты инфраструктуры (infrastructure security) | Свернул деятельность                                               | A                               | 2                                               |
| Micro Focus                       | Средства защиты приложений (application security)        | Временно сократил операции, сохраняя при этом возможности возврата | B                               | 3                                               |
| F5                                | Средства защиты приложений (application security)        | Свернул деятельность                                               | –                               | 5                                               |
| ESET                              | Средства защиты «конечных точек» (endpoint security)     | Временно сократил операции, сохраняя при этом возможности возврата | B                               | 3                                               |
| CyberArk Software                 | Средства защиты пользователей (user security)            | Временно сократил операции, сохраняя при этом возможности возврата | –                               | 2                                               |

*Источник:* составлено автором на основе Yale CELI List of Companies [4] и Исследования Центра стратегических разработок [3].

Стремление России к технологической независимости оказывает значительное влияние на информационную безопасность банковского сектора. Уход иностранных поставщиков ПО и оборудования, таких как Thales и Oracle, вынуждает банки искать отечественные альтернативы, что сопряжено с рядом сложностей и рисков.

Процесс импортозамещения в банковской сфере сталкивается с рядом серьезных вызовов. Замена зарубежных HSM-модулей [5] и СУБД требует значительных финансовых вложений и перестройки ИТ-инфраструктуры, что может быть непосильно для малых банков. Отечественные аналоги зарубежного ПО зачастую уступают по функциональности и надежности, вызывая опасения у финансовых организаций [7]. Кроме того, существует дефицит квалифицированных кадров, необходимых для внедрения и поддержки новых систем [6]. Переходный период, связанный с заменой ПО и оборудования, повышает уязвимость банков к кибератакам, что требует особого внимания к вопросам информационной безопасности.

Согласно указу Президента РФ № 166, к 1 января 2025 года госорганы России обязаны отказаться от иностранного ПО на объектах критической информационной инфраструктуры, а с 31 марта 2022 года госзакупки для этих объектов возможны только с согласования уполномоченного органа [8]. Российские банки столкнулись с проблемой зависимости от американской СУБД Oracle. Переход на отечественные автоматизированные банковские системы, такие как ЦФТ, «Диасофт» и R-Style Softlab, сопряжен с высокими затратами, достигающими сотен миллионов рублей [7]. Разработка и внедрение отечественных решений, таких как KasperskyOS и платформы 1С, позволяет снизить зависимость от зарубежных технологий и обеспечить надежную защиту от внешних и внутренних угроз.

Стоит отметить, что процесс импортозамещения затронул вопросы безопасности клиентов финансовых организаций. Удаление официальных банковских приложений из магазинов приложений создает благоприятную среду для мошенников, распространяющих фальшивые приложения и осуществляющих фишинговые атаки. В то же время в условиях геополитической напряженности возрастает вероятность целенаправленных атак на финансовую систему России со стороны хактивистов. В связи с этим банкам необходимо инвестировать в развитие собственных систем безопасности и активно сотрудничать с ФинЦЕРТ для эффективного противодействия киберугрозам [9]. Такой подход позволит стимулировать разработку отечественных решений в области кибербезопасности, одним из которых стала система KasperskyOS.

KasperskyOS, операционная система, разработанная «Лабораторией Касперского», решает проблемы уязвимости и ограничений традиционных операционных систем, используя микроядерную архитектуру и инновационные технологии безопасности, такие как MILS и FLASK. Эти функции значительно сокращают поверхность атаки и обеспечивают надежную защиту от киберугроз, что делает KasperskyOS идеальным выбором для критической инфраструктуры и государственных учреждений [10].

Интеграция KasperskyOS в различные секторы российской экономики ускоряется. Партнерство с такими компаниями, как Centerm [11] и Tsplus [12], привело к разработке безопасных тонких клиентов и решений для виртуальных рабочих столов, а сотрудничество с ИнфоТеКС [13] и Систэм Электрик [14] способствует созданию кибериммунных устройств для промышленных и энергетических предприятий. Эти партнерства демонстрируют универсальность и адаптивность KasperskyOS, делая ее краеугольным камнем усилий России по импортозамещению в области кибербезопасности.

Более того, акцент на кибериммунитете соответствует растущей глобальной тенденции моделей безопасности Zero Trust. Строгий контроль доступа и механизмы изоляции, реализованные в KasperskyOS, перекликаются с принципами Zero Trust Network Access (ZTNA), признанной ключевой технологией безопасности будущего [15]. Это соответствие позиционирует KasperskyOS как ведущее решение не только в России, но и на мировой арене, демонстрируя стремление страны к разработке передовых технологий кибербезопасности.

Стоит отметить, что подобные инициативы не ограничиваются российским рынком. Зарубежные компании также активно развивают концепцию кибериммунитета. Например, иммунная система IBM Security предлагает интегрированный и целостный подход, основанный на когнитивном ядре управления безопасностью и аналитики, способном изучать множество переменных риска в рамках всей экосистемы связанных возможностей [16].

Зарубежная технология IBM Cyber immune system опирается на искусственный интеллект и машинное обучение. Система использует SOAR (Security Orchestration, Automation and Response) для автоматизации реагирования на инциденты, обеспечивая быстрое и эффективное управление угрозами [17]. Она собирает информацию об угрозах, анализирует данные для выявления аномалий и использует структурированный подход к реагированию на инциденты. В основе архитектуры лежит принцип нулевого доверия, который подразумевает постоянную проверку всех пользователей и устройств [18].

Несмотря на схожесть двух решений, отечественная разработка обладает рядом преимуществ, среди которых:

1. Упор Kaspersky на принципы безопасной разработки и архитектуру с отказом по умолчанию предлагает более проактивный подход к кибербезопасности, потенциально снижая вероятность успешных атак по сравнению с фокусом IBM на обнаружении и реагировании.
2. Безопасная ОС и контроль приложений Kaspersky значительно ограничивают потенциальные точки входа для злоумышленников, предлагая преимущество перед более широким подходом IBM.
3. Kaspersky позволяет более гибко адаптировать систему к конкретным потребностям по сравнению с потенциально более жесткой структурой IBM.

В условиях санкционного давления и растущей активности киберугроз, обеспечение информационной безопасности финансовых организаций в России становится задачей стратегической важности. Импортозамещение, несмотря на вызовы переходного периода, открывает возможности для развития отечественных технологий и укрепления цифрового суверенитета. Концепция киберимму-

нитета, реализованная в KasperskyOS, представляет собой перспективный подход к созданию надежных и устойчивых к кибератакам систем.

Внедрение кибериммунных решений в финансовом секторе позволит:

- Снизить зависимость от зарубежных технологий и поставщиков, повышая уровень технологической независимости.
- Обеспечить высокий уровень защиты от киберугроз, минимизируя риски утечки данных, финансовых потерь и нарушения бизнес-процессов.
- Повысить доверие клиентов к финансовым организациям;
- Создать основу для дальнейшего развития инновационных финансовых технологий в условиях безопасной и надежной цифровой инфраструктуры.

**Заключение.** Таким образом, концепция кибериммунитета и ее практическая реализация в KasperskyOS представляют собой важный шаг на пути к обеспечению устойчивости и безопасности российского финансового сектора в условиях современных вызовов.

### Список литературы

1. Балахонова С. И. Киберсанкции как инструмент конкуренции в глобальном киберпространстве // Международная аналитика. – 2023. – Т. 14(1). – С. 52–71.
2. Epifanova A. Tech Sanctions Against Russia: Turning the West's Assumptions Into Lessons. (DGAP Analysis, 3). Berlin: Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V. [Электронный ресурс]. – URL: <https://nbn-resolving.org/urn:nbn:de:0168-ssor-87675-5>
3. Прогноз развития рынка кибербезопасности Российской Федерации на 2023-2027 годы. Центр стратегических исследований [Электронный ресурс]. – URL: <https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-kiberbezopasnosti-v-rossiyskoy-federatsii-na-2023-2027-gody>
4. Over 1,000 Companies Have Curtailed Operations in Russia–But Some Remain [Электронный ресурс]. – URL: <https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain>
5. Thales нашли замену. Первые российские HSM-модули получили сертификат соответствия ФСБ России [Электронный ресурс]. – URL: <https://ib-bank.ru/bisjournal/news/19062>
6. Греф оценил дефицит IT-специалистов в 1 млн человек [Электронный ресурс]. – URL: <https://www.vedomosti.ru/economics/news/2023/09/21/996468-gref-otsenil-defitsit>
7. Софт в банках: в чем проблема с замещением системного ПО в финансовом секторе [Электронный ресурс]. – URL: <https://www.forbes.ru/tekhnologii/492646-soft-v-bankah-v-chem-problema-s-zameseniem-sistemnogo-po-v-finansovom-sektore>
8. Путин запретил использовать иностранное ПО на объектах критической инфраструктуры с 2025 года [Электронный ресурс]. – URL: <https://www.vedomosti.ru/technology/news/2022/03/30/915906-putin-zapretil-ispolzovat-inostrannoe-po>

9. Киберугрозы финансовой отрасли: промежуточные итоги 2023 года [Электронный ресурс]. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/>
10. Мифы и реальность технологий кибериммунитета [Электронный ресурс]. – URL: <https://blog.kaspersky.kz/cyberimmunity-technology-myths/27161/>
11. Centerm будет предустанавливать Kaspersky Thin Client на свою аппаратную платформу [Электронный ресурс]. – URL: <https://os.kaspersky.ru/latest/kaspersky-and-centerm-to-provide-cyber-immune-thin-clients-worldwide/>
12. «Лаборатория Касперского» и TSplus подписали соглашение о партнерстве [Электронный ресурс]. – URL: <https://os.kaspersky.ru/latest/kaspersky-and-tsplus-sign-a-partnership-agreement/>
13. «Лаборатория Касперского» и «ИнфоТеКС» продолжают развивать технологическое партнерство [Электронный ресурс]. – URL: [https://www.kaspersky.ru/about/press-releases/2023\\_laboratoriya-kasperskogo-i-infoteks-prodolzhat-razvivat-tehnologicheskoe-partnyorstvo](https://www.kaspersky.ru/about/press-releases/2023_laboratoriya-kasperskogo-i-infoteks-prodolzhat-razvivat-tehnologicheskoe-partnyorstvo)
14. «Лаборатория Касперского» и «Систэм Электрик» планируют создавать кибериммунные устройства на основе KasperskyOS для промышленных и энергетических предприятий [Электронный ресурс]. – URL: <https://finance.rambler.ru/business/51006506-laboratoriya-kasperskogo-i-sistem-elektrik-planiruyut-sozdavat-kiberimmunnye-ustroystva-na-osnove-kasperskyos-dlya-promyshlennyh-i-energeticheskikh-predpriyatiy/>
15. Кибериммунитет обретает реальные очертания [Электронный ресурс]. – URL: [https://www.anti-malware.ru/analytics/Technology\\_Analysis/Cyber-Immunity](https://www.anti-malware.ru/analytics/Technology_Analysis/Cyber-Immunity)
16. The IBM Security Immune System. [Электронный ресурс]. – URL: <https://onwireco.com/the-ibm-security-immune-system/>
17. The Power of the Security Immune System [Электронный ресурс]. – URL: <https://securityintelligence.com/the-power-of-the-security-immune-system/>
18. Integrated, End-To-End Cybersecurity Strategy [Электронный ресурс]. – URL: <https://www.siainnovations.com/blog/integrated-end-to-end-cybersecurity-strategy/>

Ю. М. Графова,  
аспирант,

Казанский инновационный университет  
имени В. Г. Тимирязова

## НЕКОТОРЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ СОЦИОИНЖЕНЕРНЫМ АТАКАМ

**Аннотация.** В работе рассматриваются образовательно-просветительские меры противодействия социоинженерным атакам. Отмечается, что обучение сотрудников компании методам противодействия социоинженерным атакам является наиболее эффективным средством защиты от такого типа угроз. Таким об-

разом, чем более четко обучаемые способны соотносить события на их рабочем месте с обучением, которое они получают, тем более вероятно, что они будут приводить в действие процедуры обеспечения безопасности.

**Ключевые слова:** социальная инженерия, мошенничество, образование, профилактика, просвещение

## SOME MEASURES TO COUNTER SOCIOENGINEERING ATTACKS

**Abstract.** The paper considers educational and educational measures to counter socioengineering attacks. It is noted that training company employees in methods of countering socioengineering attacks is the most effective means of protection against this type of threat. Thus, the more clearly trainees are able to relate events in their workplace to the training they receive, the more likely they are to put safety procedures in place.

**Keywords:** social engineering, fraud, education, prevention, education

В основе развития социальной инженерии лежит несколько базовых идей. Эпистемологическая асимметрия возникает, когда человек или группа обладает значительным преимуществом в знаниях над другими людьми. Технократическое доминирование возникает, когда человек обладает высокой степенью технических знаний и использует эти знания для осуществления изменений в поведении других людей, когда такое поведение ставит жертву в подчинение злоумышленнику.

Телеологическая замена происходит, когда человек или группа замещает в другом индивидууме или группе первоначальную цель или цель их поведения своими собственными, часто через изменение самого поведения цели. Эти свойства составляют основу социальной инженерии, выражается ли это в политике или киберпространстве. Все вышесказанное позволяет глубже понять характер потенциальных угроз.

Использование знаний в качестве контрмеры социоинженерным атакам требует, чтобы пользователь опирался на свои навыки в том, что такое угроза и как она действует, чтобы адекватно реагировать на нее, если она возникнет [1]. Именно по этой причине можно отметить, что лучший способ избежать участи жертвы атак социальной инженерии – быть осведомленным в вопросах противодействия таким атакам, т. е. в вопросах информационной безопасности.

Таким образом, чем более четко обучаемые способны соотносить события на их рабочем месте с обучением, которое они получают, тем более вероятно, что они будут приводить в действие процедуры обеспечения безопасности.

Корреляции такого рода включают в себя видение некоторых конкретных социоинженерных атак, с которыми сталкивается сотрудник, и использование их моделей в обучении. Так как особенности любой реальной атаки будут отличаться во многих важных отношениях из учебных примеров, необходимо отрабатывать правильную реакцию, опирающуюся на способность обучаемого абстрагироваться от специфических особенностей атаки.

Необходимость проводить соответствующее обучение сотрудников для повышения у них навыка противостояния социоинженерным атакам отмечена и в работе Dina Aladawy, Kristian Beckers, Sebastian Pape [2]. Указанные авторы считают, что наиболее эффективными в данной области могут стать деловые игры, в процессе которых сотрудники учатся противостоять мошенникам. Соответственно, сегодня назрела острая необходимость обеспечить обучение сотрудников компаний умению распознавать риски, связанные с социоинженерными атаками, и противостоять им. Практика показывает, что осведомленность сотрудников о возможных угрозах является лучшей защитой от утечки данных [3].

Таким образом, можно констатировать, что обучение сотрудников компании методам противодействия социоинженерным атакам является наиболее эффективным средством защиты от такого типа угроз.

### Список литературы

1. Sanders, C. A. (2018). *Social Engineering Knowledge Measured as a Security Countermeasure*. (Master's thesis). – URL: <https://scholarcommons.sc.edu/etd/4567>
2. Aladawy, D., Beckers, K., & Pape, S. (2018). PERSUADED: Fighting Social Engineering Attacks with a Serious Game. In *Lecture notes in computer science* (Pp. 103–118). – DOI: [https://doi.org/10.1007/978-3-319-98385-1\\_8](https://doi.org/10.1007/978-3-319-98385-1_8)
3. Hussain Ali Aldawood, Geoffrey Skinner A Critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications.

**Г. А. Грищенко,**

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

### ПРАВОВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ

**Аннотация.** В современном цифровом мире дети являются наиболее уязвимой аудиторией пользователей в сети Интернет. Чрезмерное доверие несовершеннолетних к популярным блогерам (инфлюенсерам) приводят к тому, что зачастую размываются границы реальной и виртуальной жизни, и, как следствие, может привести к причинению вреда жизни и (или) здоровью себе и окружающим. Целью статьи является проведение анализа законодательства, правоприменительной практики, общественного мнения и научной литературы в области регулирования информационной безопасности детей, и выработка рекомендаций по совершенствованию правовой регламентации соответствующих отношений с учетом новых вызовов и угроз в условиях цифровизации. Проведенный анализ показал недостаточность и неэффективность регулирования некоторых аспектов обеспечения информационной безопасности детей в цифровой среде. В качестве

выводов предложены рекомендации по реализации правовых решений, которые помогут достичь должного уровня регламентации отдельных направлений по обеспечению информационной безопасности детей в цифровой среде.

**Ключевые слова:** информационная безопасность детей, угрозы в цифровой среде, сеть Интернет, цифровые технологии, деструктивный «вредный» контент, правовые проблемы, совершенствование законодательства

## LEGAL PROBLEMS OF ENSURING THE INFORMATION SECURITY OF CHILDREN IN THE DIGITAL ENVIRONMENT

**Abstract.** In today's digital world, children are the most vulnerable audience of Internet users. Excessive trust of minors in popular bloggers (influencers) leads to the fact that the boundaries of real and virtual life are often blurred, and, as a result, can lead to harm to life and (or) health to oneself and others. The purpose of the article is to analyze legislation, law enforcement practice, public opinion and scientific literature in the field of regulating information security of children, and to develop recommendations for improving the legal regulation of relevant relations, taking into account new challenges and threats in the context of digitalization. The conducted analysis showed the insufficiency and inefficiency of regulation of some aspects of ensuring information security of children in the digital environment. As conclusions, recommendations are proposed for the implementation of legal solutions that will help achieve the proper level of regulation of certain areas to ensure the information security of children in the digital environment.

**Keywords:** information security of children, threats in the digital environment, the Internet, digital technologies, destructive "harmful" content, legal problems, improvement of legislation

**Введение.** В современных цифровых реалиях одной из самых уязвимых категорий с позиции обеспечения информационной безопасности являются дети. Учитывая постоянное совершенствование цифровых технологий и расширение сферы их применения, дети наиболее подвержены не всегда положительному влиянию сети Интернет. При этом зачастую выявить информационные угрозы цифровой среды достаточно сложно и взрослым, и специалистам в сфере информационной безопасности (особенно это касается так называемой «фейковой» информации, когда, например, дипфейки способны подделать не только изображение человека, но и его голос).

По результатам различных социологических исследований (ВЦИОМ, Лига безопасного Интернета, Лаборатория Касперского и др.), более половины несовершеннолетних детей практически постоянно находятся в сети Интернет (более 60 % лиц возраста 13–16 лет), при этом количество проводимого времени в данном виртуальном пространстве с каждым годом увеличивается (до 8–10 часов в сутки). Доля детей дошкольного и младшего школьного возраста в общей статистике по количеству проводимому времени в Интернете тоже с каждым годом возрастает, что свидетельствует о повышении значимости данной формы коммуникации в современном обществе [2; 3; 5; 8].

Таким образом, проблема обеспечения информационной безопасности усложняется тем, что с каждым годом количество детей, проводящих время в цифровой среде, увеличивается, а возраст знакомства с виртуальным пространством снижается, о чем свидетельствуют различные опросы общественного мнения.

**Основная часть.** Погруженность детей с самого раннего возраста в информационную среду Интернета отражается на дальнейшей социализации ребенка дошкольного возраста и может создавать определенную трудность при вхождении ребенка, например, в образовательное пространство, именно поэтому с малых лет важно обеспечить безопасность детей относительно информации, полученной из сети Интернет, и научить извлекать полезное и познавательное самостоятельно [1. С. 38–40; 4].

Выработка эффективных механизмов по вопросам обеспечения информационной безопасности детей в контексте ее правовой регламентации на протяжении последних лет является одной из наиболее обсуждаемых тем не только в масштабах отдельной страны, но и всего мирового сообщества, что подтверждается соответствующими концептуальными и стратегическими нормативными правовыми актами (например, указы Президента Российской Федерации от 17 мая 2023 г. № 358 «О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года», от 9 ноября 2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей», от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации», от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», Распоряжение Правительства Российской Федерации от 22 декабря 2022 г. № 4088-р «Об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации»).

Анализ вышеуказанных документов показывает, что основное внимание государства нацелено на формирование у детей и взрослых знаний (навыков, умений) по всему спектру вопросов обеспечения информационной безопасности (распознавание дипфейков, различных форм цифрового мошенничества, создание и систематическое обновление надежных паролей, критическая оценка получаемой информации, владение мерами противодействия распространению «вредной» информации и т. д.).

При этом, несмотря на все принимаемые государством меры, существующая ситуация свидетельствует о наличии определенных проблем по созданию эффективных механизмов по предотвращению (минимизации) распространения «вредного» деструктивного контента среди детей в цифровой среде (прежде всего, это касается социальных сетей, мессенджеров и иных каналов активного взаимодействия пользователей сети Интернет). Статистика обращений в государственные и общественные структуры по вопросам обеспечения информационной безопасности, рассматриваемых споров, рост объема распространения незаконного контента в Интернете и цели втягивания в соответствующие сообщества де-

тей свидетельствуют о том, что правовое регулирование не успевает за слишком активным развитием общественных отношений в рассматриваемом контексте.

Конечно, в Российской Федерации приняты определенные нормативные правовые акты, целью которых является защита детей от информации, причиняющей вред их здоровью и развитию. Среди таких актов, прежде всего, следует отметить Конституцию Российской Федерации, федеральные законы от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее – ФЗ о защите детей от информации) и от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» (далее – ФЗ об основных гарантиях прав ребенка), устанавливающие базовые принципы обеспечения безопасности детей в интернет-среде.

Отдельные вопросы реализации общественных отношений, связанных с оборотом разного рода информации, регулируются федеральными законами от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ об информации) и от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Особое внимания заслуживает новая Концепция информационной безопасности детей в Российской Федерации, утвержденная Распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р, которая определяет принципы обеспечения информационной безопасности детей и приоритетные задачи, а также механизмы реализации государственной политики в данной сфере (предыдущая Концепция действовала с 2015 по 2020 гг.).

На региональном уровне также принимаются нормативные документы, направленные на регламентацию различных аспектов обеспечения информационной безопасности детей в цифровой среде. Например, во многих субъектах Российской Федерации действует проект «КиберПатруль», главной целью которого является формирование безопасного интернет-пространства для несовершеннолетних, поиск «вредной» деструктивной информации, проведение информационной работы по безопасности в сети с несовершеннолетними и их родителями (Красноярск, Тюмень, Курск, Иркутск и др.). Деятельность подобных проектов, несомненно, способствует повышению эффективности противодействия киберпреступности среди детей разных возрастных категорий и обеспечения информационной безопасности.

Регулирование вопросов обеспечения информационной безопасности детей осуществляется также на отраслевом уровне (например, Приказ Минцифры России от 1 декабря 2020 г. № 644 «О плане мероприятий, направленных на обеспечение информационной безопасности детей, на 2021 – 2027 годы», Письмо Минобрнауки России от 28 апреля 2014 г. № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет»).

Несмотря на сформировавшуюся в целом нормативно-правовую базу регулирования обеспечения информационной безопасности детей в цифровой среде, остается еще много нерешенных вопросов в данной области. Появляются новые условия и возможности для совершения новых правонарушений, не всегда охватываемых действующими составами уголовного и административного зако-

нодательства или недостаточно четко и однозначно их определяемые (например, кибербуллинг, треш-стрим); когнитивные возможности детей и особенности психологического развития данной возрастной группы не всегда готовы правильно оценить ситуацию и среагировать на возможные угрозы из сети Интернет.

В связи с этим представляется целесообразным изменить подход к понятийному аппарату данной сферы и расширить трактовку информационной безопасности детей, сделав акцент именно на информационно-психологической безопасности детей, включив соответствующие изменения в ФЗ о защите детей от информации.

Наличие пробелов (коллизий) в праве, стремительное развитие информационных (цифровых) технологий, недостаточный уровень цифровой грамотности, игнорирование правил безопасной работы в цифровой среде обуславливают необходимость совершенствования российского законодательства в сфере обеспечения информационной безопасности детей.

Очевидно, что со временем степень вызовов, угроз и рисков в цифровой среде будет только возрастать, будут появляться новые категории (сущности) общественных отношений, требующих тщательной проработки и правового регулирования. Трагические события в учебных заведениях, связанные с применением насилия в отношении учащихся и педагогов («колумбайны»), порождают в обществе дискуссии не только по поводу ужесточения мер по обороту оружия, но и по поводу интернет-контента, влияющего на сознание ребенка, повышающего уровень его агрессивности, снабжающего опасными знаниями. Последнее дело в Челябинской области, когда мальчик принес в школу самодельное взрывное устройство, которое смастерил по видеоурокам в Интернете (причем родители не препятствовали таким занятиям, поощряя научный потенциал сына), демонстрирует, что изменения в российском законодательстве просто необходимы [6].

В Интернете существует огромное количество разнообразных сообществ, которые представляют собой аккумуляцию молодежных субкультур и которые могут распространять «вредную» информацию, хотя изначально они позиционируют себя как тематические группы, созданные с целью объединения единомышленников, никак не противоречащей законодательству (фурри, слэш, аеу, аниме и др.).

Подобные интернет-сообщества могут знакомить сразу со всеми видами деструктивной информации (пропаганда наркотиков, суицидов, школьных расстрелов, нетрадиционных отношений и т. д.), которая всегда подается с юмором, лишая возможности ребенку критически оценить возможную опасность от потребляемого контента. Со временем ребенок подписывается на узкотематические группы и попадает под негативное влияние руководителей (кураторов) соответствующих сообществ.

Многие специалисты, занимающиеся анализом практики вовлечения детей в деструктивные сообщества, говорят о так называемых «воронках вовлечения» [7], которые отражают последовательность действий ребенка и рост его зависимости от выполнения разнообразных опасных заданий.

Так, изначально информация по различным темам (суицид, травля, наркотики) размещается в открытой группе, в которую ребенок может вступить, вы-

полнив определенное простое задание. Усложняя задания, куратор сообщества постепенно переключает внимание ребенка на его важность и значимость в данной группе, находясь в которой можно только соблюдая некоторые правила, характерные для данной субкультуры. Со временем ребенок переходит в закрытые группы, в которых общение происходит в основном посредством личных сообщений, и заканчивается такая «игра» выполнением заданий в реальном времени.

Отдельно стоит отметить необходимость донесения до детей информации о возможности попадания в такие зависимые группы и о правильности реагирования на получение соответствующих приглашений по вступлению в подобные интернет-сообщества.

В связи с этим считаем необходимым продолжить работу по просвещению детей, а также их родителей и учителей в сфере обеспечения информационной безопасности, проводя в образовательных учреждениях специальные уроки по знакомству с новыми формами мошенничества в цифровой среде, с новыми техническими решениями (программами, сервисами, платформами) по выявлению информации, не соответствующей действительности (сайты по распознаванию дипфейков) и т. д.

Хотелось бы обратить внимание еще на одну проблему обеспечения информационной безопасности, которая затрагивает в целом всех субъектов интернет-пространства – обеспечение защиты персональных данных, когда незаконная обработка личной информации может использоваться злоумышленниками в противоправных целях.

Статистика свидетельствует, что дети зачастую не осознают все потенциальную опасность размещения в Интернете личной информации о себе и членах своей семьи:

- 58 % указывают свой домашний адрес и мобильный телефон;
- 39 % указывают номер школы;
- 29 % выкладывают фото, на которых видна обстановка в квартире;
- 23 % размещают информацию о родителях и родственниках;
- 10 % указывают свой реальный возраст;
- 7 % публикуют геолокацию [7].

Очевидно, что дети должны знать, какие персональные данные существуют (к которым, помимо общеизвестных фамилии, имени, отчества, относятся также изображение, голос, отпечатки пальцев и др.), кому и как их можно предоставлять и в каких случаях следует обратиться за помощью к взрослым.

Учитывая вышеизложенное, представляется целесообразным дальнейшую работу по совершенствованию российского законодательства в сфере обеспечения информационной безопасности детей выстраивать по следующим направлениям:

1) следует унифицировать понятийный аппарат в рассматриваемой сфере, определить особенности распространения информации в сети Интернет, ориентированной на детскую аудиторию (особенно в социальных сетях), осмыслить и сформулировать новые составы правонарушений, к которым может привести распространение деструктивного контента, и внести соответствующие изменения в нормативные правовые акты;

В связи с этим целесообразно в ФЗ о защите детей от информации ввести дефиницию вредной (вредоносной) информации, определить ее критерии, и в целом расширить трактовку самой категории «информационная безопасность детей», определив ее как «информационно-психологическую безопасность детей».

2) учитывая, что контент в сети Интернет может быть как положительным, так и негативным (деструктивным), необходимо привить детям навыки по его анализу и конструктивной оценке. В связи с этим представляется необходимым включение в образовательный процесс уроков информационной безопасности, цифровой грамотности (цифровой гигиены) и проведение просветительских мероприятий для родителей и работников сферы образования;

Необходимо усилить работу по методической поддержке образовательных учреждений в сфере информационной безопасности детей, разработать понятные и доступные учебно-просветительские материалы.

3) очевидно, что влияние цифровых медиа (социальных сетей, форумов, блогов и проч.) на процессы формирования и проявления общественного мнения достаточно существенно, особенно среди детей. Это требует разработки принципиально новых механизмов реагирования на нарушения в цифровой среде, например, в рамках деятельности блогеров, тиктокеров и других лидеров молодежного мнения в цифровом пространстве России, в части досудебной блокировки неправомерного контента в сети Интернет. Необходимо усовершенствовать механизм подачи электронных жалоб на обнаруженный незаконный контент, особенно в различных мессенджерах;

4) также следует разделить угрозы информационной безопасности детей по степени их общественной опасности и возможных негативных последствий (аутодеструктивные, суицидальные, экстремистские и проч.), что должно найти отражение в уголовном и административном законодательстве в части выработки эффективного соотношения между наносимым вредом и уровнем ответственности, а также в части предупреждения совершения противоправных деяний в цифровой среде.

**Заключение.** Комплексная реализация представленных предложений позволит развить теоретические и практико-ориентированные положения по вопросам исключения (минимизации) угроз распространения деструктивного контента в сети Интернет, и выработать действенную эффективную систему принципов, приоритетных задач и механизмов, обеспечивающих реализацию государственной политики в области информационной безопасности детей.

### Список литературы

1. Алексеенко А. А., Иванова М. М. Обеспечение информационной безопасности детей дошкольного возраста // Цифровая экономика: проблемы и перспективы развития: Сб. научных статей 4-й Всероссийской научно-практической конференции. – Курск, 2022. – С. 38–40.

2. Анненкова И. В., Залоило М. В. Новая культура коммуникаций в условиях цифровой и социокультурной глобализации: право, медиа и национальная идентичность // Журнал зарубежного законодательства и сравнительного правоведения. – 2019. – № 3. – С. 140–155.

3. ВЦИОМ: результаты опроса о восприятии россиянами интернета и о возможности его ограничения [Электронный ресурс] // Сайт Всероссийского центра изучения общественного мнения. 22.03.2021 [Электронный ресурс]. – URL: [https://wciom.ru/analytical-reviews/analiticheskii-obzor/internet-i-deti-vozmozhnosti-i-ugrozy#:~:text=%D0%94%D0%B5%D1%82%D0%B8%20%D0%B2%20%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5,%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8%20%D0%B2%20%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5%20\(81%25\)](https://wciom.ru/analytical-reviews/analiticheskii-obzor/internet-i-deti-vozmozhnosti-i-ugrozy#:~:text=%D0%94%D0%B5%D1%82%D0%B8%20%D0%B2%20%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5,%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8%20%D0%B2%20%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5%20(81%25))
4. Магдилова Л. В. Правовые основы обеспечения информационной безопасности несовершеннолетних // Сайт научной электронной библиотеки КиберЛенинка. 2017. 10.21779/2224-0241-2017-23-3-104-108
5. Сколько времени в день ребенку можно проводить в Интернете? // Сайт Лиги безопасного Интернета. 13.02.2023. [Электронный ресурс]. – URL: <https://ligainternet.ru/skolko-vremeni-v-den-rebenku-mozhno-provodit-v-internete/>
6. Сустина Т. К вопросу об интернет-безопасности детей // «Адвокатская газета». – 2022. – № 5.
7. Угрозы для детей в цифровой среде [Электронный ресурс] // Сайт Центра правовой помощи гражданам в цифровой среде ФГУП «ГРЧЦ». 2023. – URL: <https://4people.grfc.ru/faq/detskaya-bezopasnost-v-internete-na-chto-sleduet-obraschat-vnimanie/>
8. 56 % детей постоянно находятся в Сети [Электронный ресурс] // По материалам сайта kaspersky.ru. [Электронный ресурс] – URL: <http://security.mosmetod.ru/internet-zavisimosti/99-56-detej-postoyanno-nakhodyatsya-v-seti>

**Г. Г. Егоров,**

кандидат юридических наук, доцент,  
Волгоградский государственный университет  
(Волжский филиал)

## **ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕЙ ДЛЯ МОНИТОРИНГА ПРОТИВОПРАВНЫХ ОТНОШЕНИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Аннотация.** В статье рассматриваются перспективны использование современных машинных комплексов анализа правовых отношений на предмет ответственности современному действующему законодательству. Выделяются основные направления противоправных действий, выявление которых становится возможным при использовании графологических нейронных сетей (GNN) основанных на логике асинхронного анализа правонарушений основанных на нарушения финансового оборота. В качестве практической составляющей использовался опыт апробации данных комплексов в Китайской народной республики, при этом проводится анализ как технических так и правовых особенностей внедрения тождественных систем в контрольную сферу Российской Федерации. Определя-

ются основные сложности по внедрению цифровых систем контроля и перспективы по их адаптации к Российским условиям.

**Ключевые слова:** нейронные графологические сети, контроль за правомерностью отношений, технические средства выявления правонарушений, федеральный контроль за цифровой безопасностью, правовой статус информации, цифровой контроль.

## USING NEURAL NETWORKS FOR MONITORING ILLEGAL RELATIONS IN THE RUSSIAN FEDERATION

**Abstract.** The article considers the prospects of using modern machine complexes for analyzing legal relations for compliance with current legislation. The main areas of illegal actions are identified, the identification of which becomes possible with the use of graphological neural networks (GNN) based on the logic of asynchronous analysis of offenses based on violations of financial turnover. The experience of testing these complexes in the People's Republic of China was used as a practical component, while an analysis of both technical and legal features of the implementation of identical systems in the control sphere of the Russian Federation is carried out. The main difficulties in the implementation of digital control systems and prospects for their adaptation to Russian conditions are determined.

**Keywords:** neural graphological networks, control over the legality of relations, technical means of identifying offenses, federal control over digital security, legal status of information, digital control.

**Введение.** В условиях стремительного развития цифровых технологий и финансовых инноваций, возникает необходимость переосмысления подходов к обработке данных в сфере ПОД/ФТ.

Постоянно увеличивающийся поток данных и необходимость оперативно-го анализа рисков отмыывания денег требуют внедрения и развития искусственно-го интеллекта в системы противодействия финансовым преступлениям [7].

Повышенный интерес к технологиям искусственного интеллекта (далее – ИИ) обусловлен эволюцией преступных схем, использованием ИИ злоумышленниками, необходимостью обработки огромных объемов данных в финансовой разведке и развитием экспертных систем в сфере противодействия отмыыванию денег.

Научная база для изучения ИИ в сфере ПОД/ФТ пока еще находится в стадии формирования. Существующие исследования в основном сосредоточены на рисках злоупотребления ИИ для отмыывания денег, проблемах регулирования и внедрения ИИ в системы ПОД/ФТ, а также на потенциале ИИ в финансовой сфере [6].

**Основная часть.** В 2022–2023 годах ИИ все чаще используется в преступных целях. Одной из самых серьезных угроз стали фейковые видео, аудио и изображения, созданные нейросетями. Люди склонны верить видео, поэтому дипфейки, поддельные видео с реальными людьми, представляют особую опасность. Примеры таких преступлений включают вымогательства с использовани-

ем поддельных видео с руководителями или родственниками, а также мошеннические схемы с использованием фальшивых рекламных роликов.

ИИ используется банками для биометрической идентификации пользователей по лицу при входе в мобильные приложения, в то время как преступники применяют нейросети для создания новых наркотиков, улучшения взрывчатых веществ и разработки более опасных видов оружия.

ИИ-сервисы все чаще используются для получения советов по незаконному обналичиванию денег и усовершенствованию схем отмыwania денег. Пользователей интересуют правила финансового контроля, а также деятельность регуляторов в этой области. Параллельно с этим, резко увеличилось количество поддельного контента, созданного с помощью искусственного интеллекта, который используется для пропаганды и вербовки преступников. Ежедневно создаются миллионы фальшивых изображений.

Преступники научились создавать с помощью искусственного интеллекта стандартные комментарии, которые распространяются через ботов в социальных сетях, разжигая рознь, экстремизм и провокации. В 2023 году количество мошенничеств с использованием ИИ резко возросло. Например, на Филиппинах таких случаев стало в 45 раз больше по сравнению с предыдущим годом, а во Вьетнаме, США и Японии – в 30–28 раз [8].

Искусственный интеллект необходим финансовой разведке для обработки огромных массивов неструктурированных данных, их очистки и улучшения качества. Социальные сети и мессенджеры являются ценным источником информации о фигурантах финансовых расследований. Помимо пропаганды и вербовки преступников, эти платформы используются для сбора и перевода незаконно полученных средств, а также для легализации преступных доходов [5].

Анализ данных из соцсетей в финансовой разведке проводится в рамках общей системы обработки информации с использованием искусственного интеллекта. Росфинмониторинг получает данные о финансовых операциях, от государственных органов, иностранных финансовых разведок, СМИ и пользователей. Вся информация хранится и очищается с помощью машинного обучения. Далее проводится углубленный анализ данных: создаются списки, модели поведения и профили риска [12].

В результате обработки данных получаем ответы на запросы, инициативно предоставляем информацию государственным органам, спецслужбам и банкам, уведомляем в соответствии с законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (ст. 8 Федерального закона от 07.08.2001 № 115-ФЗ) и информируем зарубежные финансовые разведки [1].

Сбор, обработка, анализ и распространение информации о террористических и экстремистских группах в интернете – это работа с большими данными. В Росфинмониторинге для поиска в социальных сетях используется российская поисковая система с учетом смысла слов. В системе реализована оценка риска сообщений и автоматическое создание отчетов по новостям и социальным сетям. Сейчас данные переносятся на российское программное обеспечение.

Одновременно с этим в базе данных Росфинмониторинга обрабатываются данные о банковских картах, включая обязательные для контроля и подозрительные операции, которые также относятся к большим данным. Информация из онлайн-платформ объединяет структурированные и неструктурированные данные из множества источников, таких как тексты, изображения, видео, аудио и геолокация, образуя огромные массивы информации [4].

В основе автоматического поиска и анализа данных о террористических и экстремистских группах лежит анализ ключевых слов и объединение полученной информации. Пользователи системы могут использовать как готовые списки слов, так и создавать свои собственные.

Обработка данных осуществляется как автоматически, так и вручную. Ручная обработка требует много времени и ресурсов. Автоматизированные системы, такие как «СЕУС», «Георгий Победоносец», «Крибрум», «Сапфир», «Дарвин» и другие, позволяют быстро обрабатывать большие объемы информации в режиме реального времени [6]. Систему можно легко настроить под конкретные запросы пользователя. Помимо анализа интернет-ресурса, количества подписчиков и публикаций, программы определяют содержание сообщений и оценивают уровень вовлеченности пользователей. Некоторые системы также отслеживают изменения в профилях.

Особую значимость имеет функция сравнения адресов аккаунтов и сообщений с реестром запрещенных сайтов и списком экстремистских материалов. Человек необходим для оценки настроения сообщений, изменений взглядов и поведения пользователей, а также для уточнения их данных. Системы позволяют экспортировать данные в разных форматах.

Анализ данных с помощью искусственного интеллекта позволяет находить закономерности и тенденции, распределять данные по группам, выявлять исключения, определять связи между пользователями и их роли, собирать информацию из профилей и искать конкретных пользователей. Анализ текстов помогает выявить темы обсуждений, их эмоциональную окраску и основные направления.

Росфинмониторинг внедрил систему, основанную на машинном обучении, которая умеет отличать реальные компании от тех, что созданы только для перевода денег [9]. Эта система ищет в больших объемах данных информацию, которая не соответствует обычным правилам. Например, она может найти компании с неправильным количеством цифр в ИНН или ОГРН, с буквами вместо цифр или с неверными датами рождения.

Модель запускается автоматически по расписанию. Сначала загружаются свежие данные из ЕГРЮЛ, затем проводится классификация компаний и физических лиц с помощью заранее подготовленных моделей. Результаты этой классификации сохраняются в системе Росфинмониторинга. Такой подход позволяет находить повторяющиеся данные и улучшать их качество.

Качество моделей зависит от внешних факторов и может меняться. На это влияют выбранные характеристики, настройки пороговых значений, недостаток примеров для обучения и экспертные правила. Эксперт должен следить за состоянием моделей. Моделирование используется для классификации текстов по ключевым словам и анализа социальных сетей.

Ключевыми игроками в онлайн-пространстве экстремизма и терроризма являются криминальные и колумбайнерские сообщества, движение «МКУ», ультраправые группировки. Их сетевой характер подтверждается единой символикой, названиями, тематикой, общими администраторами или участниками, различной географической принадлежностью, взаимной рекламой и финансовыми связями.

Правонарушения часто связаны с финансовыми взаимодействиями между людьми. Во многих странах уже созданы схемы для выявления таких незаконных действий. Китайские исследователи Юэ Тянь, Гуаньцзюнь Лю, Цзяцзюнь Ван и Мэнчу Чжоу предлагают использовать модифицированную графическую нейронную сеть для обнаружения подобных отношений [18].

Онлайн-платежи, которые скрывают свою истинную цель, привлекают как финансовых мошенников, так и других преступников, нанося огромный ущерб частным лицам и банкам. Глобальные потери от таких действий достигли 25 миллиардов долларов в 2018 году и продолжают расти. Согласно данным Nilson Report, в 2020 году убытки увеличились до 28,65 миллиарда долларов. В ответ на это финансовые учреждения приняли меры для предотвращения мошенничества [15].

Традиционно онлайн-транзакции проверяются на соответствие определенным правилам, составленным экспертами. Если транзакция вызывает подозрения, ее передают модели обнаружения мошенничества. Эта модель, используя огромный объем исторических данных о транзакциях, выявляет закономерности, характерные для мошеннических действий. Цель модели – найти транзакции, которые с высокой вероятностью преследуют незаконные цели.

Возможности систем обнаружения связей ограничены и плохо адаптируются к быстро меняющимся мошенническим схемам. Ученые стремятся выявлять все больше схем мошенничества, но сложные схемы и системы обнаружения создают своего рода «динамическую игру». Записи о транзакциях часто содержат дополнительную информацию, такую как местоположение, время и предмет, что может быть полезно для анализа.

Существующие методы машинного обучения для обнаружения мошеннических транзакций требуют ручного создания признаков и построения классификаторов, что не гарантирует стопроцентное автоматическое обнаружение новых схем мошенничества. Между транзакциями существует множество взаимосвязей, анализ которых позволяет глубже изучить характер транзакций.

С другой стороны, поведение пользователей при совершении транзакций постоянно меняется, что затрудняет создание эффективной системы представления данных для обнаружения мошеннических действий. Мошенники постоянно меняют свои методы, что снижает эффективность многих существующих систем обнаружения и делает их менее универсальными [14].

В последнее время графовые нейронные сети (GNN) стали применяться для автоматического создания представлений данных в различных задачах прогнозирования [16]. В отличие от традиционных методов машинного обучения, GNN обрабатывают данные, учитывая их взаимосвязи, что позволяет строить более глубокие представления данных и затем использовать нейронные сети для

классификации объектов и прогнозирования связей между ними. Такие методы позволяют захватывать сложные взаимозависимости между данными и избегать создания искусственных признаков, что часто является недостатком традиционных подходов [17].

Несмотря на потенциал графовых нейронных сетей, их прямое применение к обнаружению мошеннических транзакций сопряжено с трудностями. Такие методы не учитывают взаимосвязи между различными характеристиками транзакций и не способны адаптироваться к динамическим изменениям в поведении пользователей. Исследования, проведенные специалистами [18], показали, что популярные модели GNN, такие как GraphSAGE и GCN, не позволяют надежно различать мошеннические и законные транзакции, как видно из рис. 1.

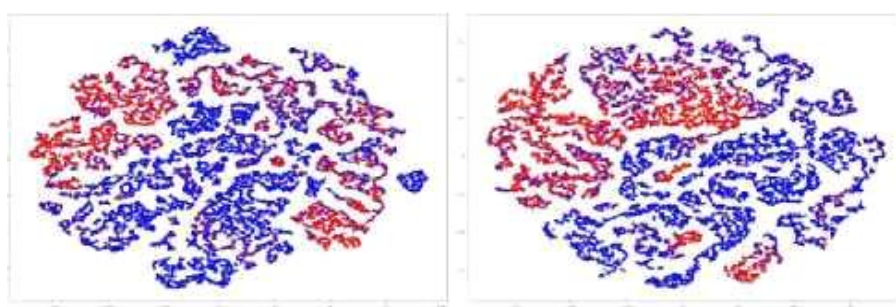


**Рис. 1. Результаты визуализации GCN модели GNN. Красные узлы представляют собой мошеннические транзакции, а остальные – законные.**

**(а) Перед обучением на наборе исходных финансовых данных.**

**(б) После обучения на наборе адаптивных финансовых данных [18]**

Кроме того, GNN сталкиваются с проблемой чрезмерного усреднения, когда представления узлов разных классов становятся слишком похожими. Эта проблема усиливается в контексте обнаружения мошенничества, где мошеннические узлы часто маскируются под законные, как показано на рис. 2. Такое смешивание классов данных еще больше затрудняет различение мошеннических и законных транзакций.

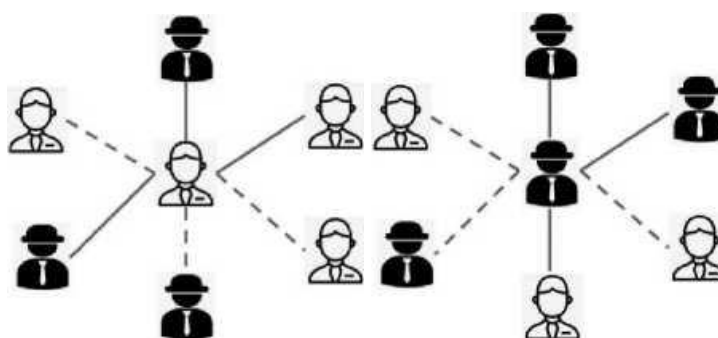


**Рис. 2. Маскировка мошенников. Мошенники ослабляют свои подозрения, маскируя поведение держателей карт так, что система обнаружения считает, что это законные транзакции [18]**

Для решения этой проблемы ряд авторов [18] предлагают использовать новый метод, названный ASA-GNN, основанный на адаптивной выборке и агрегации в графовых нейронных сетях для обнаружения мошеннических транзакций. Этот метод объединяет ранее предложенные авторами подходы. Сначала создается граф транзакций из необработанных данных, а затем, учитывая особенности мошеннических транзакций, анализируются взаимосвязи между различными характеристиками и динамические изменения в поведении пользователей.

Для отбора соседей, наиболее похожих на текущий узел, используется специальный алгоритм выборки, основанный на косинусной мере сходства и весе ребер. Этот алгоритм позволяет отфильтровать шумные соседи, сохраняя при этом структурную информацию графа. Для усиления эффекта отбора и уменьшения числа связей между мошенническими узлами предлагается увеличивать выборку подобных соседей.

Для борьбы с маскировкой мошенников вводится новая метрика разнообразия соседей, основанная на энтропии. Она позволяет оценить, насколько однородны или разнообразны соседи данного узла, отражая динамические изменения в поведении участников. Это помогает определить, приведет ли агрегирование информации от соседей к искажению представлений узла. Каждый узел получает свой коэффициент агрегации, позволяющий обеспечить компактность внутри классов и разделение между классами [3].

Исследователей предлагает новую модель для обнаружения мошеннических транзакций. Несмотря на существование множества методов, основанных на экспертных правилах и машинном обучении, которые успешно применяются в различных областях, включая обнаружение мошенничества, они имеют свои ограничения. Такие методы извлекают информацию из доступных данных для автоматического выявления признаков мошенничества, демонстрируя эффективность на известных типах мошенничества, однако они могут быть менее эффективны при обнаружении новых, неизвестных схем мошенничества [18].

Для решения этой проблемы эксперты обратились к методам глубокого обучения. Эти методы способны автоматически выявлять сложные взаимосвязи между различными характеристиками транзакций, обеспечивая более точное представление данных и позволяя эффективнее обнаруживать случаи мошенничества. Одним из наиболее распространенных методов глубокого обучения в этой области является сверточная нейронная сеть (CNN).

Помимо анализа взаимосвязей между характеристиками транзакций, существующие методы также извлекают ассоциации между самими транзакциями для улучшения результатов обнаружения мошенничества. Одним из распространенных подходов является агрегирование данных. Этот метод объединяет транзакции в группы по определенным временным интервалам и затем вычисляет агрегированные признаки, такие как суммарная сумма транзакций в группе и количество транзакций.

Для повышения информативности о поведении пользователя, в качестве дополнительных признаков агрегации учитывались местоположение и код продавца. Это позволило расширить временной контекст анализа. Параллельно с этим, для изучения динамики транзакций во времени стали применяться ре-

куррентные нейронные сети (RNN). В частности, сети с долгой краткосрочной памятью (LSTM) позволяют эффективно улавливать эволюцию распределения данных во времени [18]. Учитывая постоянные изменения в распределении данных, предлагаются динамические методы для достижения более высоких показателей точности.

Для комплексного изучения различных взаимосвязей между транзакциями исследователи построили граф на основе имеющихся данных. Графовые нейронные сети (GNN) позволяют эффективно выявлять эти взаимосвязи и улучшать обнаружение мошенничества. Однако поскольку GNN обычно используют только один тип связи для построения графа, они могут упускать из виду множество других полезных признаков, характерных для мошеннических действий [11].

Большинство существующих методов не охватывают одновременно все аспекты взаимосвязи между транзакциями, взаимосвязи между их характеристиками и динамические изменения в поведении пользователей. Мы предлагаем использовать взвешенный мультиграф и графовые нейронные сети (GNN) для комплексного анализа этих взаимосвязей и динамики. Однако наш метод также имеет определенные ограничения.

GNN – это мощная структура, способная изучать представления графов путем моделирования связей данных в неевклидовых графах. Некоторые специалисты ранее рассматривали эту систему как совокупность операций свертки, аналогичных тем, что используются при обработке изображений, но применительно к данным графов. После этого было предложено и успешно применено множество методов, основанных на графах [18].

Большинство ранних алгоритмов строят представления узлов в два этапа: сначала определяют последовательность соседних узлов случайным образом, а затем используют модели машинного обучения для анализа топологической структуры графа и получения векторного представления для каждого узла. Несмотря на то, что эти алгоритмы учитывают топологическую структуру, они игнорируют атрибуты самих узлов.

Некоторые методы, работающие с графами, используют атрибуты узлов, основанные на текстовой и статистической информации. Например, Graph Convolutional Network (GCN) применяет спектральные графовые свертки для извлечения информации о признаках. Graph Attention Network (GAT) определяет важность различных соседей с помощью механизма внимания. GraphSAGE позволяет гибко обновлять представления узлов путем выборки и агрегирования соседних узлов. Метод сети реляционных графов (RGCN) способен моделировать данные с различными типами связей [18].

Последние исследования успешно применяли крупномасштабные графы, преодолевая вычислительные сложности. Учитывая разнообразие типов узлов и ребер в гетерогенных графах, а также их динамическую природу, были предложены гетерогенные GNN и динамические GNN. Параллельно с этим велись исследования по интерпретируемости и оптимизации структуры GNN.

Однако применение существующих GNN к обнаружению мошеннических транзакций не позволяет полностью использовать все доступные данные для по-

строения графов. В результате полученные графы могут не содержать важной информации. Метод конкурентных графовых нейронных сетей (CGNN) [18] использует гетерогенные графы для моделирования нормального и мошеннического поведения в электронной коммерции. Метод MAFI применяет трехмерный механизм пространственно-временных транзакций для анализа графов транзакций, основанных на геолокации. Кроме того, MAFI использует механизм внимания на уровне агрегации и уровне отношений для изучения информации о соседях и различных типах связей [13].

LGM-GNN использует локальную и глобальную информацию для создания более различных представлений, улучшая точность прогнозирования. Однако эти методы не учитывают, что чрезмерная агрегация может привести к тому, что представления узлов разных классов станут слишком похожими и неразличимыми.

Это приводит к эффекту чрезмерного сглаживания в GNN. В контексте обнаружения мошеннических транзакций мошенники часто маскируют свою деятельность, имитируя поведение добросовестных пользователей. В результате, между узлами, связанными с мошенническими действиями, и легитимными узлами возникают сходства. Это усиливает негативное воздействие эффекта чрезмерного сглаживания.

Сталкиваясь с проблемой маскировки мошенников, метод CAouflage-RESistant GNN (CARE-GNN) вводит метрику сходства с учетом меток, используя расстояние N для выбора соседей. Однако он фокусируется исключительно на сходстве меток. Расстояние N становится менее эффективным в многомерном пространстве и неспособно описать сложное сходство поведения. Транзакционный граф (TG), построенный в схеме, способен уловить взаимосвязи между динамическим поведением транзакций, статическими атрибутами транзакций и самими транзакциями [18].

Однако он не учитывает, что мошенники избегают взаимодействовать с другими мошенниками. Более того, он не решает проблему чрезмерного сглаживания. Авторы предлагают использовать косинусное сходство и взвешивание ребер для устранения этих недостатков, а также фокусируются на оценке негативного влияния агрегации окрестностей на проблему чрезмерного сглаживания.

Структура ASA-GNN представлена на рис. 3. Ее ключевые компоненты – выборка соседей и агрегация соседей. На этапе выборки соседей, чтобы отсеять шумных соседей и сохранить структурную информацию, мы вводим новую стратегию выборки соседей, основанную на косинусном сходстве и весе ребер. В процессе агрегации соседей важность различных соседей определяется механизмом внимания. Затем применяется метрика разнообразия, чтобы контролировать степень агрегации. В заключение, функция softmax вычисляет вероятность мошеннической транзакции.

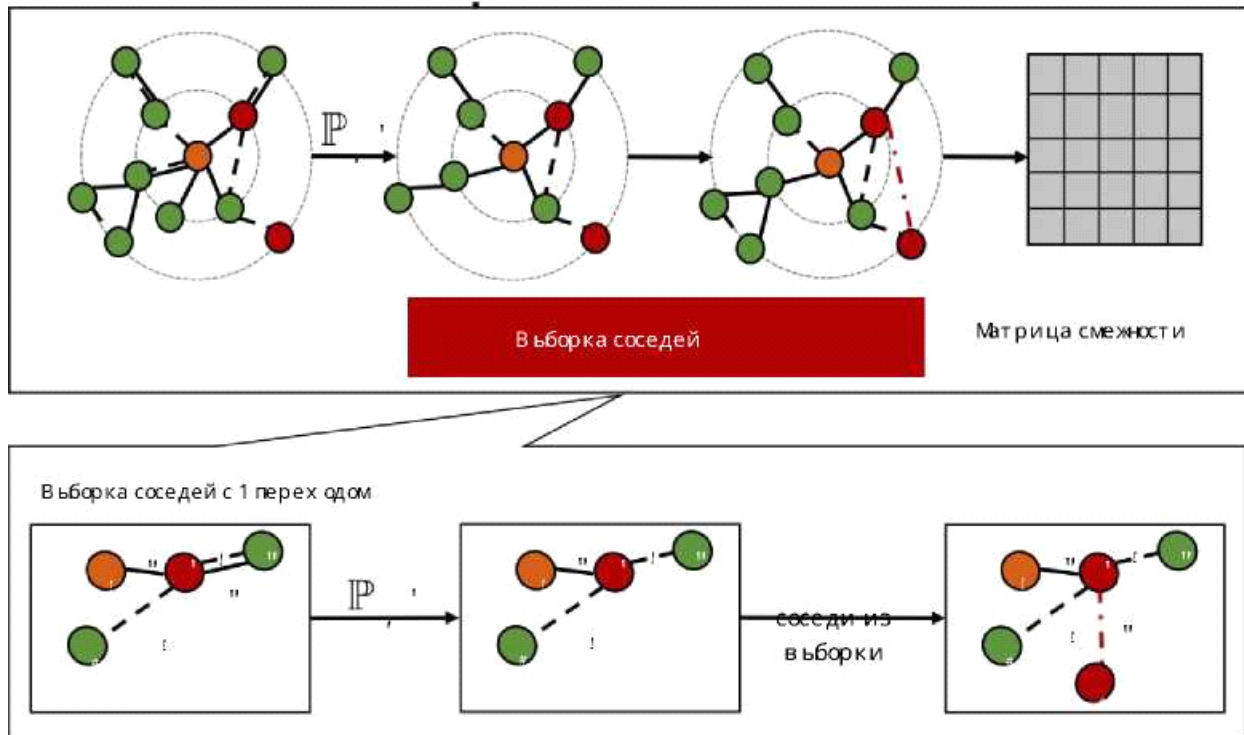


**Рис. 3. Обзор ASA-GNN: 1) Выборка соседей на уровне узла, при которой соседи Тор- $z$  выбирают информацию о шуме фильтра каждого узла, а затем производят избыточную выборку соседей для мошеннических узлов. 2) Расчет показателя внимания и степени агрегации для изучения представлений. 3) Сценка вероятности того, что транзакция будет предсказана как мошенническая на уровне обнаружения [18]**

GNN используют информацию о соседних узлах для построения более точных представлений. Существующие методы, такие как GraphSAGE, применяют случайный выбор соседей, исходя из предположения, что похожие узлы связаны между собой. Однако это не учитывает качество информации, предоставляемой соседями. Некоторые соседи могут быть бесполезными и вводить шум в процесс обучения, что затрудняет различение узлов разных классов. Другие соседи могут содержать много полезной информации, которую важно не упустить. Поэтому мы предлагаем новую стратегию выбора соседей, которая учитывает как степень сходства между узлами (косинусное сходство), так и силу связи между ними (вес ребра). Это позволяет отбирать наиболее информативных соседей и повысить качество полученных представлений [18].

Предлагается новая стратегия выбора соседей, учитывающая расстояние между узлами (вычисляемое с помощью косинусной меры сходства, часто применяемой в анализе пользовательского поведения) и вес ребра, соединяющего эти узлы. Такой подход позволяет более точно выбирать соседей и решает проблему, связанную с неэффективностью случайного выбора соседей в существующих методах.

Используемый в исследовании набор данных содержит 5 133,5 миллионов финансовых транзакций, осуществленных клиентами китайской компании во

втором квартале 2017 года. Все транзакции были предварительно классифицированы профессиональными следователями китайского банка на мошеннические и легальные [18]. Для устранения дисбаланса в данных, перед началом анализа была проведена пониженная выборка легитимных транзакций.

Для обработки данных использовалось горячее кодирование дискретных признаков и нормализация min-max для непрерывных. Учитывая высокую вычислительную сложность CARE-GNN, для экспериментов был выбран небольшой подвыбор данных (PR02), включающий последние 10 000 транзакций, что позволило ускорить процесс тестирования.

Набор данных TC1, предоставленный компанией Orange Finance, включает 160 764 транзакции, из которых 44 982 классифицированы как мошеннические, а 115 782 – как законные. Для создания обучающих и тестовых выборок данные были разделены по времени совершения транзакций. Транзакции одной недели формируют обучающую выборку, а следующей – тестовую. Таким образом, набор TC1 был разбит на три подвыборки: TC12, TC23 и TC34. К этим подвыборкам применялись те же методы предобработки, что и к наборам данных PR01 и PR02. Набор данных XF, выделенный из iFLYTEK2, содержит 20 000 записей и включает пять типов информации: основные данные, мультимедийные данные, временные данные, информацию об IP-адресах и информацию об устройствах. Набор XF сбалансирован по классам. Для обработки дискретных и непрерывных признаков применялись те же методы, что и для наборов данных PR01 и PR02. При построении графа транзакции рассматривались как узлы, а различные логические связи между ними – как ребра. Такой подход учитывает, что мошенники часто используют разнообразные схемы взаимодействия для создания сложных моделей мошенничества [18].

Наиболее ярким и масштабным примером организации криминальной субкультуры служит экстремистское движение «АУЕ» (его модель копируют аналогичные молодежные группировки).

Мониторинг российской соцсети VK в 2022 году выявил 91 559 сообществ, пропагандирующих криминальные субкультуры, активных в России, Беларуси, Казахстане, Азербайджане, Армении, Грузии и на Украине. Особую опасность представляют молодежные сетевые движения террористической направленности, проповедующие идеи «естественного отбора», «биомусора» и «человеконенавистничества». Характерными примерами таких движений являются «Колумбайн» («Скулшутинг») и «МКУ» (True Crime Community) [9].

Идеология «Колумбайн» (скулшутинг) пропагандирует массовые убийства в образовательных учреждениях, совершаемые учениками или посторонними лицами. Эта идеология основана на идеях собственного превосходства над другими, сравнивая себя с богом, на концепции естественного отбора, где часть людей считается «биомусором», и на оправдании насилия и убийств как способа восстановления справедливости.

После запрета движения в России в 2022 году последовала массовая блокировка связанных с ним пабликов, что привело к значительному сокращению их аудитории. Поскольку мониторинг деструктивных сообществ ведется по ключе-

вым словам, администраторы групп стали скрывать запрещенные названия, используя другие формулировки.

В ходе мониторинга социальных сетей и мессенджеров неоднократно фиксировалось использование российскими сторонниками террористического движения «Колумбайн» иностранных символов и иероглифов в качестве никнеймов и названий деструктивных сообществ. Цель такого подхода – маскировка запрещенного контента и затруднение мониторинга, выявления и блокировки опасных аккаунтов. Значительная часть пользователей перешла в закрытые группы и телеграм-каналы, где распространяется более радикальный и жесткий контент.

С субкультурой колумбайна тесно связано движение «МКУ», пропагандирующее убийства и насилие. Онлайн-сообщества «МКУ» в социальных сетях являются открытыми и содержат информацию о серийных убийцах, маньяках и террористах.

Учитывая запрет «МКУ» в России в 2023 году, открытые МКУ-сообщества стали активно ссылаться на закрытые ресурсы с экстремистскими материалами, включая видеоинструкции по изготовлению взрывных устройств, переделке оружия и проведению диверсий. Несмотря на пресечение деятельности более 150 сторонников «МКУ» в 50 регионах России в 2021–2022 годах, попытки организации диверсий на транспортной инфраструктуре и поджогов государственных зданий продолжают [9].

С началом СВО появилась новая угроза – деятельность диверсионных сообществ и одиночек, финансирующих терроризм и экстремизм. Росфинмониторинг активно противодействует этой угрозе, включив в 2023 году в Перечень террористов и экстремистов 87 диверсантов.

Поиск исполнителей для диверсий ведется через телеграм-каналы, где заинтересованным лицам предлагают поджечь объекты за вознаграждение. После выполнения задания и предоставления фото- или видеодоказательств, исполнителю перечисляют деньги. В социальных сетях преобладают аккаунты, связанные с неонацистской идеологией, что свидетельствует о радикализации ультраправых групп.

Ультраправые группы отличаются геопривязкой к Украине и большим количеством подписчиков. Они открыто пропагандируют неонацистские идеи и терроризм в описаниях своих каналов и пабликов. Многие такие группы ведут открытую деятельность. Важнейшим способом противодействия распространению деструктивных идей в сети является тщательный анализ интернет-активности пользователей.

В рамках интеллектуального анализа данных ключевыми направлениями являются: изучение аномалий, то есть выявление отклонений от нормального поведения, и отслеживание динамики аккаунтов, позволяющее выявить процесс радикализации и вовлечения пользователей в преступную деятельность.

Современные интернет-технологии в сфере борьбы с противоправным контентом должны сочетать автоматический поиск с ручной проверкой отдельных аккаунтов и пользователей. Сегодня эта работа ведется вручную, что требует значительных ресурсов. Единой государственной системы с искусственным ин-

теллектом для решения этой задачи пока нет, хотя отдельные ведомства и компании разрабатывают свои решения.

В рамках ПОД/ФТ необходимо детально изучать особенности финансирования, отслеживать финансовые потоки и связи между участниками. Сбор средств осуществляется через закрепленные в профилях или ссылках платежные реквизиты, с использованием различных платформ и криптовалют. Собранные средства переводятся на иностранные счета через зарубежные сервисы.

В преступной деятельности, особенно в сфере незаконного оборота наркотиков, широко применяются боты, выполняющие функции обменников криптовалют. Эти инструменты позволяют быстро обменять рубли на различные виды цифровых валют, используя при этом миксеры для сокрытия следов финансовых операций.

В Росфинмониторинге для отслеживания таких транзакций применяется программа «Прозрачный блокчейн», которая автоматически создает связи между владельцами криптокошельков, их финансовыми операциями и партнерами по сделкам [9]. В период с 2020 по 2023 годы эта программа успешно использовалась для борьбы с отмыванием денег, полученных от онлайн-продаж наркотиков.

Разработка экспертных систем и баз знаний является неотъемлемой частью искусственного интеллекта. В России создание экспертных систем в сфере ПОД/ФТ основывается на национальных и секторальных оценках рисков, разрабатываемых Росфинмониторингом. Эти документы содержат всесторонний анализ существующих угроз, схем преступной деятельности, тенденций и прогнозов развития системы ПОД/ФТ, созданный экспертами в данной области.

Все схемы отмывания денег классифицируются по этапам: создание незаконного дохода, ввод этих денег в легальный оборот, перемещение средств, обналичивание, вывод капитала за рубеж и использование легализованных средств. Существует около 70 основных способов отмывания денег.

В отличие от данных в базах данных, экспертные оценки способов отмывания денег описывают не отдельные случаи, а повторяющиеся наборы характеристик целых групп схожих действий, то есть определенные шаблоны поведения [10]. Эксперты ФАТФ считают, что искусственный интеллект может частично или полностью автоматизировать анализ рисков и предложить новые способы их выявления.

Использование технологий искусственного интеллекта в этой области позволит создать общие и специфические модели преступной деятельности, обнаружить новые виды преступлений, автоматизировать проверку подозрительных операций. При создании этих моделей ключевую роль играют данные, полученные от экспертов. Экспертные системы в сфере ПОД/ФТ могут применяться для анализа данных, мониторинга, обучения, предоставления рекомендаций аналитикам и службам комплаенса. Такие системы способны выдвигать стандартные версии событий, устанавливать связи между лицами и организациями, а также поддерживать принятие решений.

Будущее российской системы противодействия отмыванию денег заключается в создании самообучающихся интеллектуальных систем, постоянно совершенствующихся на новых данных и знаниях. Эти системы позволят значи-

тельно сократить ручную работу аналитиков, обеспечивая быструю обработку сообщений о подозрительных финансовых операциях и предоставляя рекомендации и прогнозы для подразделений финансовой разведки, банков и других участников системы ПОД/ФТ.

**Заключение.** Перспективными направлениями использования ИИ в сфере ПОД/ФТ являются: семантический анализ текстов, аудио-, фото- и видеоматериалов в соцсетях с применением нейросетей для обнаружения экстремистского контента, предложений о продаже запрещенных товаров и финансовых данных; классификация и анализ постов в соцсетях для выявления пропаганды, призывов к терроризму и легализации доходов; автоматизированный анализ стримов и онлайн-трансляций; выявление ботов, распространяющих фейки и дипфейки; автоматизация мультивалютных расследований с криптовалютами.

Необходимо регулировать использование ИИ в сфере ПОД/ФТ. По аналогии с операторами связи, нужно получать информацию от разработчиков нейросетей о пользователях, интересующихся незаконными финансовыми операциями. Следует закрепить использование инновационных технологий для проверок, применять инструменты обработки естественного языка и биометрию для идентификации клиентов, а также использовать поисковые модели для выявления манипуляций на финансовых рынках.

Необходимо включить отдельный раздел об искусственном интеллекте в Концепцию развития национальной системы противодействия легализации доходов, полученных преступным путем, и финансированию терроризма (утверждена Президентом РФ 30.05.2018) [2]. Концепцию можно дополнить обсуждением рисков, связанных с преступлениями, использующими технологии ИИ, а также мерами по внедрению ИИ в Единую информационную систему ПОД/ФТ.

Внедрение искусственного интеллекта в систему противодействия отмыванию денег – это не самостоятельный процесс, изолированный от всего остального. Многие руководители недостаточно осведомлены о возможностях ИИ и о том, как его можно использовать для решения различных задач. Также отсутствуют единые стандарты для тестирования и внедрения инструментов искусственного интеллекта.

Искусственный интеллект – дорогостоящий инструмент, требующий высококвалифицированных специалистов и развитой технической инфраструктуры. Недостаток кадров в области анализа данных и ИИ, а также сложность интерфейсов программ могут препятствовать их эффективному использованию. Применение сложных алгоритмов должно быть сбалансировано с необходимостью оперативного проведения финансовых расследований [5].

### Список литературы

1. Федеральный закон от 07.08.2001 № 115-ФЗ (ред. от 08.08.2024) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (с изм. и доп., вступ. в силу с 01.09.2024) // Российская газета. – № 151–152. – 09.08.2001.

2. Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (утв. Президентом РФ 30.05.2018) // СПС «КонсультантПлюс: Законодательство».

3. Егоров Г. Г. Перспективы развития современного гражданского права в условиях внедрения нейросетевых комплексов // В сборнике: Стратегия развития гражданского права в поисках ответов на вызовы XXI века (цифровые перспективы и действительность). Материалы II Международной научно-практической конференции. Волгоград, 2024. – С. 69–78.

4. Егоров Г. Г. Правовые формы обеспечения информационной безопасности в сети Интернет // Правовая парадигма. 2022. Т. 21. № 4. С. 70–76.

5. Егоров Г. Г. Нормативно-правовой оборот цифровых прав в России // В сборнике: Цифровые технологии и право. сборник научных трудов II Международной научно-практической конференции В 6 т. – Казань, 2023. – С. 154–168.

6. Красинский В. В., Леонов П. Ю., Морозов Н. В. Применение искусственного интеллекта в сфере противодействия отмыванию денег и финансированию терроризма // Современное право. – 2024. – № 5. – С. 75–82.

7. Казанцева С. Ю., Казанцев Д. А. Практика применения и перспективы развития технологий ИИ и робототехники в сфере финансового контроля // Вопросы инновационной экономики. – 2021. – № 2. – С. 553–564.

8. Красинский В. В. Цифровые технологии в антитерроре // Современное право. – 2020. – № 6. – С. 123–129. – DOI: 10.25799/NI.2020.93.13.009.

9. Красинский В. В. Противодействие финансированию терроризма с использованием криптовалют // Современное право. – 2022. – № 9. – С. 108–116. – DOI: 10.25799/NI.2022.58.84.018

10. Шатских С. И. Методология оценки рисков ОД/ФТ как возможная основа инженерии знаний и искусственного интеллекта в контрольно-надзорной деятельности // Финансовая безопасность. – 2023. – № 39. – С. 60 – 65.

11. Khazane A., Rider J., Serpe M., Gogoglou A., Hines K., Bruss C. B., Serpe R. Deeptrex: Embedding graphs of financial transactions // 18th IEEE International Conference On Machine Learning And Applications (ICMLA). – IEEE. – 2019. – Pp. 126–133.

12. Leonov P. Y., Sushkov V.M., Krasinsky V.V. [at al] Detecting Money Laundering Patterns through Cash Flow Analysis a Neural Network-Based Approach // IEEE International Scientific and Technical Conference Actual Problems of Electronic Instrument Engineering (APEIE). – Novosibirsk, 2023. – Pp. 1390 – 1393. – DOI: 10.1109/APEIE59731.2023.10347735

13. N. Jiang, F. Duan, H. Chen, W. Huang, and X. Liu, “Mafi: Gnn-based multiple aggregators and feature interactions network for fraud detection over heterogeneous graph // IEEE Transactions on Big Data. – 2021. – Vol. 8, № 4. – Pp. 905–919.

14. S. Yin, G. Liu, Z. Li, C. Yan, and C. Jiang, “An accuracy-and-diversitybased ensemble method for concept drift and its application in fraud detection,” in 2020 International Conference on Data Mining Workshops (ICDMW). IEEE, 2020. – Pp. 875–882.

15. The Nilson Report. [Online]. – URL: <https://nilsonreport.com/mention/1313/1link/>
16. X. Hou, K. Wang, C. Zhong, and Z. Wei, “ST-Trader: A Spatial-Temporal Deep Neural Network for Modeling Stock Market Movement,” IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 5, pp. 1015–1024, 2021.
17. Dou Y., Liu Z., Sun L., Deng Y., Peng H., Yu P. S. Enhancing graph neural network-based fraud detectors against camouflaged fraudsters // Proceedings of the 29th ACM International Conference on Information & Knowledge Management, 2020. – Pp. 315–324.
18. Yue Tian, Guanjun Liu, Jiacun Wang, Mengchu Zhou Transaction Fraud Detection via an Adaptive Graph Neural Network // JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. 8, AUGUST 2021. Pp. 1–10

**Т. Э. Кылчыкбаев,**

кандидат юридических наук, доцент,  
Кыргызский национальный университет  
имени Ж. Баласагына

## **ПОНЯТИЕ КИБЕРБЕЗОПАСНОСТИ В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ**

**Аннотация.** В современном цифровом мире понятие кибер-угрозы все больше проникает в нашу жизнь. Кибербезопасность становится важной проблемой для всех, от отдельных лиц до мировых компаний, корпораций и стран. В данной статье на основе анализа законодательных инициатив и практических мер органов исполнительной власти в сфере информационной безопасности Кыргызской Республики рассматриваются возможности государства по противодействию современным кибер-угрозам и формированию культуры личной информационной безопасности.

**Ключевые слова:** информационные технологии, кибербезопасность, цифровая информация, защита личных данных, законодательное регулирование

## **THE CONCEPT OF CYBERSECURITY IN THE KYRGYZ REPUBLIC**

**Abstract.** In today's digital world, the concept of a cyber threat is increasingly penetrating our lives. Cybersecurity is becoming an important issue for everyone, from individuals to global companies, corporations and countries. This article, based on an analysis of legislative initiatives and practical measures of executive authorities in the field of information security of the Kyrgyz Republic, examines the state's capabilities to counter modern cyber threats and create a culture of personal information security.

**Key words:** information technology, cybersecurity, digital information, personal data protection, legislative regulation

**Введение.** Цифровая революция, которая началась в конце XX века, продолжает стремительно развиваться, оказывая глубокое влияние на все сферы жизни современного общества. По данным Международного союза электросвязи

(ITU), к концу 2019 года более половины населения земного шара, а именно 53,6% или 4,1 миллиарда человек, имели доступ к интернету. Примечательно, что основная часть пользователей интернет-сети проживает в развивающихся странах, где число пользователей интернет-сети составляет 3,02 миллиарда человек. Однако, несмотря на очевидные преимущества, которые приносит цифровая революция, она порождает и целый комплекс угроз и вызовов, затрагивающих безопасность как отдельных граждан, так и целых государств [1].

**Основная часть.** Среди наиболее актуальных проблем можно выделить:

1. *Киберпреступность*: распространение вирусов, хакерских атак, кража личных данных, фишинговые схемы и другие виды киберпреступности становятся все более изощренными и опасными.

2. *Дезинформация и пропаганда*: распространение ложной информации в сети Интернет, а также использование социальных сетей для манипулирования общественным мнением представляет серьезную угрозу для демократических ценностей и стабильности общества.

3. *Проблемы конфиденциальности*: цифровые технологии позволяют собирать и хранить огромное количество личных данных, что ставит под вопрос конфиденциальность частной жизни и создает предпосылки для злоупотреблений.

4. *Неравенство доступа*: неравномерное распространение цифровых технологий и отсутствие доступа к качественному интернету в некоторых регионах страны усугубляет существующее социальное неравенство и препятствует развитию.

5. *Риски для национальной безопасности*: киберугрозы могут нанести серьезный ущерб инфраструктуре государства, экономике и обороноспособности, создавая предпосылки для дестабилизации и конфликтов. В связи с этим возрастает важность комплексной и скоординированной политики государства, направленной на минимизацию рисков и обеспечение безопасной цифровой среды для своих граждан. В этом контексте ключевую роль играет разработка и реализация национальных киберстратегий, которые должны включать в себя:

**Законодательное регулирование**: установление правовых норм, регулирующих деятельность в киберпространстве, борьбу с киберпреступностью, защиту личных данных и информационной безопасности.

**Развитие кибербезопасности**: создание сильных систем кибербезопасности, повышение уровня осведомленности населения о киберугрозах, развитие информационной инфраструктуры, создание специализированных подразделений по кибербезопасности в правоохранительных органах.

**Международное сотрудничество**: координация действий с другими странами в борьбе с киберпреступностью, обмен информацией и технологиями, создание международных механизмов реагирования на киберугрозы.

**Развитие цифровой культуры**: пропаганда цифровых компетенций, формирование у населения критического мышления и способности различать достоверную информацию от фейковых новостей.

Кыргызстан, как многие другие страны, сталкивается с вызовами цифровой революции, и в последние годы вопрос обеспечения кибербезопасности страны активно обсуждается в политических кругах и на академических пло-

щадках. Президент Кыргызстана Садыр Жапаров на церемонии открытия здания координационного центра по обеспечению кибербезопасности Государственного комитета национальной безопасности заявил: «Можно сказать, что это новое направление в общей системе обеспечения национальной безопасности страны в настоящее время находится на стадии становления. Учитывая, что в последнее время наблюдаются хакерские атаки на государственные и другие информационные системы, есть необходимость как можно скорее поднять и развить это направление до качественного уровня» [2]. Данное заявление свидетельствует о том, что сфера ИКТ в Кыргызстане стала приоритетным направлением развития страны, и показывает, насколько серьезно правительство относится к цифровизации и сопутствующим ей проблемам.

Однако Кыргызстан имеет относительно низкие показатели в Глобальном индексе кибербезопасности, который разработан Международным союзом электросвязи ООН [3]. Индекс ориентирован на выявление рисков в развитии цифровой среды, формулирование рекомендаций по укреплению киберзащиты государств и формирование глобальной цифровой культуры. Кыргызстан находится на низких позициях в индексе, что подчеркивает необходимость усиления мер по обеспечению кибербезопасности, поэтому было принято «правовые основы единой системы кибербезопасности, целью которой является защита личности, общества и государства путем обеспечения цифровой устойчивости информационной инфраструктуры КР» [4]. Несмотря на эти шаги, страна нуждается в дальнейшей разработке и реализации национальной киберстратегии, которая должна учитывать уникальные особенности Кыргызстана и опираться на лучшие практики других стран. В рамках этой стратегии необходимо осуществить ряд важных шагов:

- Укрепление законодательной базы: принятие новых законов и изменение существующих для обеспечения эффективной борьбы с киберпреступностью, защиты личных данных и информационной безопасности.
- Развитие системы кибербезопасности: создание централизованных систем мониторинга киберугроз, внедрение современных технологий киберзащиты, подготовка специалистов в области кибербезопасности.
- Повышение осведомленности населения: проведение программ по киберграмотности, просвещение граждан о киберугрозах, обучение безопасным практикам в интернете.
- Развитие международного сотрудничества: участие в международных программах по кибербезопасности, обмен опытом с другими странами, создание межведомственных структур для координации действий по кибербезопасности.
- Поддержка развития цифровой экономики: создание благоприятных условий для развития цифровых технологий и инноваций, стимулирование цифрового предпринимательства.

**Заключение.** Реализация этих шагов поможет Кыргызстану сделать шаг вперед в обеспечении цифровой безопасности и создании благоприятных условий для развития цифровой экономики. Важно понимать, что кибербезопасность – это не только техническая задача, но и вопрос общественной ответственности. Каждый пользователь интернета должен быть осведомлен о киберугрозах

и принимать меры для защиты своей личной информации. Цифровая революция создает огромные возможности для развития Киргизстана, но вместе с тем она несет в себе и определенные риски. Правильное понимание этих рисков разработка эффективных стратегий для их минимизации являются ключевыми факторами для успешной цифровизации страны.

### Список литературы

1. 2,9 млрд. человек все еще лишены подключения. [Электронный ресурс]. – URL: <https://www.itu.int/ru/mediacentre/Pages/PR-2021-11-29-FactsFigures.aspx>
2. Президент Киргизии дал поручение усилить кибербезопасность государства // ТАСС [Электронный ресурс]. – URL: <https://tass.ru/mezhdunarodnaya-panorama/17739891>
3. Основные показатели измерения уровня развития цифровой инфраструктуры Кыргызской Республики [Электронный ресурс]. – URL: <https://internetpolicy.kg/wp-content/uploads/2022/11/%D0%9F%D0%BE%D0%BA%D0%B0%D0%B7%D0%B0%D1%82%D0%B5%D0%BB%D0%B8-%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B8%CC%86-2.pdf>
4. Закон Кыргызской Республики «О кибербезопасности Кыргызской Республики» принятым Жогорку Кенешем КР от 12-июня 2024 г. // Сайт Министерства юстиции Кыргызской Республики [Электронный ресурс]. – URL: <https://cbd.minjust.gov.kg/4-5260/edition/1939/ru>

**Н. И. Легостаева,**

кандидат социологических наук,

Санкт-Петербургский государственный университет

**О. В. Медяник,**

кандидат психологических наук, доцент,

Санкт-Петербургский государственный университет

## ДУАЛЬНЫЙ СИМБИОЗ ЦИФРОВЫХ ФИНАНСОВЫХ ТЕХНОЛОГИЙ И КИБЕРМОШЕННИЧЕСТВА

**Аннотация.** Быстрая цифровая трансформация экономического сектора способствует развитию новых бизнес-моделей и улучшению прозрачности финансовых операций. При этом она открывает двери для кибермошенников, что подчеркивает необходимость комплексного подхода к изучению цифровых финансовых технологий и киберрисков. Взаимодействие традиционных финансовых услуг с инновационными финансовыми технологиями одновременно создает новые возможности и риски, поэтому компании должны соблюдать осторожность в использовании инновационных решений, чтобы избежать уязвимости перед киберугрозами. В статье акцентируются внимание на важности разработки единого правового подхода к определению понятия «кибермошенничество». Это

поможет устранить противоречия в законодательной и судебной практике, обеспечивая более эффективную защиту граждан.

**Ключевые слова:** цифровизация, финансовые технологии, кибермошенничество, киберпреступность, киберриски

## THE DUAL SYMBIOSIS OF DIGITAL FINANCIAL TECHNOLOGY AND CYBER FRAUD

**Abstract.** The rapid digital transformation of the economic sector is driving the development of new business models and improving the transparency of financial transactions. At the same time, it opens the door to cyber fraudsters, which emphasizes the need for an integrated approach to the study of digital financial technology and cyber risk. The interaction of traditional financial services with innovative financial technologies simultaneously creates new opportunities and risks, so companies must be cautious in utilizing innovative solutions to avoid vulnerability to cyber threats. The authors of the article emphasize the importance of developing a unified legal approach to the definition of cyber fraud. This will help to eliminate contradictions in legislative and judicial practice, ensuring more effective protection of citizens.

**Keywords:** digitalization, financial technology, cyber fraud, cyber crime, cyber risks

**Благодарность:** исследование выполнено за счет гранта Российского научного фонда № 23-28-00701, «Поведенческие стратегии потребителей финансовых услуг в условиях кибермошенничества: междисциплинарный анализ», <https://rscf.ru/project/23-28-00701/>

**Введение.** В настоящее время большую актуальность приобрели исследования, посвященные цифровизации экономического сектора и цифровой трансформации финансового поведения [2; 5]. Цифровизацию бизнеса связывают с развитием онлайн-магазинов, онлайн-сервисов, онлайн-рекламы [8; 16]. В одних исследованиях авторы изучают положительные стороны цифровой трансформации (повышение прозрачности экономических операций, исключение посредников, оптимизация издержек, создание новых продуктов и услуг и т. д.), другие исследования сосредоточены на рисках и угрозах цифровизации современного общества (цифровое мошенничество и киберпреступность, сокращение общего количества рабочих мест, риски рынка криптовалюты и др.) [3; 7].

Финансовые цифровые технологии относятся к сегменту рынка, где традиционные финансовые услуги сливаются с инновационными компаниями. С одной стороны, это открывает новые возможности для финансовых симбионтов («донор-реципиент»), но, с другой стороны, несет новые риски для предприятий в использовании инновационных технологий [1; 6; 9; 13].

В литературе по проблемам цифровизации в финансовой сфере отмечается рост случаев кибермошенничества и уровня финансовой тревожности российских граждан [4; 12; 17]. Исследователи отмечают, что снижение уровня доверия цифровым финансовым технологиям является низкой цифровой и финансовой

грамотность большинства потребителей, что требует усиления образовательных инициатив [10; 11; 14; 15].

**Основная часть.** В 2023 году в рамках реализации проекта «Поведенческие стратегии потребителей финансовых услуг в условиях кибермошенничества: междисциплинарный анализ» № 23-28-00701 авторы статьи провели пилотажное качественное исследование – интервью с экспертами. Интервью было ориентировано на судей, поскольку важно было выявить пробелы в законодательстве Российской Федерации в области защиты прав граждан, пострадавших от мошеннических действий. Целью интервью с экспертами стало выявить наиболее часто встречаемые виды мошенничества, с которыми сталкиваются истцы. Объектом исследования стали договоры потребительского кредита с нарушениями общих условий, установленных кредитором, и индивидуальных условий, согласуемых кредитором и заемщиком. Предметом исследования выступали случаи интервенции мошенников при заключении общих и индивидуальных условий договоров потребительского кредита. Гайд интервью включал такие вопросы, как:

1. «Назовите, пожалуйста, основные аргументы и доводы истца в данном гражданском деле?»

2. «По каким причинам судья Верховного Суда Российской Федерации (Судебной коллегии по гражданским делам Второго кассационного суда общей юрисдикции или Судебной коллегии по гражданским делам Верховного Суда Российской Федерации) удовлетворил/а требования истца?»

3. «Назовите, пожалуйста, форму кредитного обслуживания истца со стороны банка (онлайн или офлайн)?»

4. «Назовите причины, по которым судья первой инстанции отказал/а в удовлетворении требований истца?»

5. «Назовите, пожалуйста, статьи законов, в соответствии с которыми судья Верховного Суда Российской Федерации (Судебной коллегии по гражданским делам Второго кассационного суда общей юрисдикции или Судебной коллегии по гражданским делам Верховного Суда Российской Федерации) принял/а решение удовлетворить требования истца?» и др.

В результате проведенных интервью с пятью экспертами были выявлены:

1) причины, по которым истцам изначально было отказано в удовлетворении их требований;

2) причины, по которым требования истцов в дальнейшем были удовлетворены судьями;

3) наиболее часто встречаемые формы кредитного обслуживания со стороны банков, которыми пользуются мошенники и др.

По результатам пилотажного интервью с экспертами было выявлено, что судебные постановления по рассматриваемым ими гражданским делам по договорам потребительского кредита (5 кейсов), заключенных с нарушениями общих условий, установленных кредитором, и индивидуальных условий, согласованных кредитором и заемщиком, не отвечали требованиям законности и обоснованности и что судами первой инстанции при рассмотрении дел допущены нарушения норм права, которые являются существенными и не могут быть устранены без

отмены судебных постановлений и новых рассмотрений дел. Отмена судебных постановлений судов первой инстанции связана с неправильным применением норм материального права, нарушением норм процессуального права и несоответствием выводов судов обстоятельствам дел.

Заключение договоров в результате мошеннических действий является неправомерным действием, направленным против интересов гражданина, который не подписывал соответствующий договор, и являющегося применительно к статье 168 (пункт 2) Гражданского кодекса Российской Федерации третьим лицом, права которого нарушены. Наиболее часто применяемыми статьями судами второй инстанции при удовлетворении требований истцов являются следующие: статьи 379.5–379.7, 390, 390.1, 390.14 Гражданского процессуального кодекса Российской Федерации.

В результате исследования было выявлено, что телефонное мошенничество является наиболее часто встречающимся видом мошенничества, когда жертва после того, как с ней связался мошенник – якобы «сотрудник банка», предоставляет ему SMS-код и другую персональную информацию. Подписание договора электронной подписью с использованием SMS-кода предусматривали пункты кредитного договора, что явилось цифровым юридическим помощником для кибер-мошенников, поскольку, в соответствии с условиями договора, при предоставлении SMS-кода истцом (кредитором) банк выполняет свои обязанности перед кредитором путем перечисления суммы кредита на счет кредитора в банке.

**Заключение.** Таким образом, авторы делают вывод, что изучение амбивалентной природы отношений цифровых финансовых технологий и кибермошенничества заключается не только в исследовании положительных и отрицательных последствий цифровой трансформации экономического сектора, но и в поиске единого правового подхода в определении самого понятия «кибермошенничество» – сложного, быстроразвивающегося и высоко адаптивного явления современного общества, что исключит противоречия в законодательной и судебной практике. По результатам интервью с экспертами были выявлены значительные пробелы в российском законодательстве, касающиеся защиты прав граждан от мошеннических действий. Это подчеркивает необходимость разработки единого правового подхода к определению и регулированию кибермошенничества. По результатам исследования был сделан вывод, что телефонное мошенничество, связанное с передачей SMS-кодов и персональной информации, является наиболее распространенным видом. Это требует пересмотра условий кредитных договоров и усиления мер безопасности.

### Список литературы

1. Ваганова О. В., Коньшина Л. А. Развитие рынка финансовых технологий: зарубежный опыт и отечественная практика // Научный результат. Экономические исследования. – 2021. – Т. 7, № 1. – С. 80–88.
2. Иванова Т. Ю., Кочкова Я. А. Особенности маркетинга в социальных медиа в условиях цифровизации // Экономический журнал. – 2018. – № 3(51). – С. 67–76.

3. Масланов Е.В. Цифровизация и развитие информационно-коммуникационных технологий: новые вызовы или обострение старых проблем? // The Digital Scholar: Philosopher's Lab. – 2019. – Т. 2, № 1. – С. 6–21.
4. Медяник О. В. Влияние финансовой тревожности на страховое поведение россиян в условиях пандемии COVID-19 354 // Вестник Санкт-Петербургского университета. Социология. – 2020. – Т. 13, №4. – С. 354–373.
5. Мирошник А. Н., Хусточкин И. А. Медиатехнологии в функционировании современной банковской системы РФ: цифровизация банковских услуг // Экономика: теория и практика. – 2019. – № 2. – С. 61–65.
6. Семеко Г. В. Новые финансовые технологии: глобальные тренды и особенности России // Экономические и социальные проблемы России. – 2020. – № 1. – С. 50–74.
7. Халин В. Г., Чернова Г. В. Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски // Управленческое консультирование. – 2018. – № 10 (118). – С. 46–63.
8. Bouwman H., Nikou S., Molina-Castillo F. J., de Reuver M. The impact of digitalization on business models // Digital Policy, Regulation and Governance, Emerald Publishing Limited. – 2018. – Vol. 20(2). – Pp. 105–124.
9. Chen X., Yan D., Chen W. Can the digital economy promote FinTech development? // Growth and Change. – 2022. – Vol. 53, № 1. – Pp. 221–247.
10. Colleen T. A. Financial literacy and financial behavior: Assessing knowledge and confidence // Financial Services Review. – 2015. – Vol. 24. – Pp. 101–117.
11. Collins J. M. Financial advice: A substitute for financial literacy? // Financial services review. – 2012. – Vol. 21. – № 4. – Pp. 307–322.
12. Grable J., Heo W., Rabbani A. Financial anxiety, physiological arousal, and planning intention // Journal of Financial Therapy. – 2014. – Vol. 5. – № 2. – Pp. 1–18.
13. Haddad C., Hornuf L. The emergence of the global fintech market: Economic and technological determinants // Small business economics. – 2019. – Vol. 53, № 1. – Pp. 81–105.
14. Lin X., Bruhn A., William J. Extending financial literacy to insurance literacy: A survey approach // Accounting & Finance. – 2019. – Vol. 59. – Pp. 685–713.
15. Lusardi A., Mitchell O. S. Financial literacy around the world: an overview // Journal of pension economics & finance. – 2011. – Vol. 10, № 4. – Pp. 497–508.
16. Naskali J., Kaukola J., Matintupa J., Ahtosalo H., Jaakola M., Tuomisto A. Mapping business transformation in digital landscape: A prescriptive maturity model for small enterprises // Well-Being in the Information Society. Fighting Inequalities: 7th International Conference, WIS 2018, Turku, Finland, August 27–29, 2018, Proceedings 7. – Springer International Publishing, 2018. – Pp. 101–116.
17. Shapiro G. K., Burchell B. J. Measuring financial anxiety // Journal of Neuroscience, Psychology, and Economics. – 2012. – Vol. 5, № 2. – Pp. 92–103.

**Л. В. Магдилова,**

кандидат юридических наук, доцент,  
Дагестанский государственный университет

**М. М. Магдилов,**

кандидат юридических наук, доцент,  
Дагестанский государственный университет

## ПРАВОВОЕ И ТЕХНИЧЕСКОЕ РЕГУЛИРОВАНИЕ ТЕХНОЛОГИЙ 5G

**Аннотация.** В статье обоснована необходимость совершенствования правовой базы регулирования беспроводных сетей пятого поколения с учетом развития квантовых технологий, требованиями защиты персональных данных, развитием экономики данных. В результате предлагается определить правовой статус технологий 5G с учетом трансграничной составляющей. Ключевыми направлениями развития правового регулирования в данной области являются: обеспечение информационной безопасности, распределение радиочастотного спектра, совершенствование правовых норм к инновациям беспроводной связи в здравоохранении, транспорте, промышленности, государственном управлении.

**Ключевые слова:** квантовые технологии, беспроводная связь, аутентификация, обезличенные данные, интернет вещей, экономика данных, цифровая экономика

## LEGAL AND TECHNICAL REGULATION OF 5G TECHNOLOGIES

**Abstract.** The article substantiates the necessity of improving the legal base of regulation of wireless networks of the fifth generation taking into account the development of quantum technologies, the requirements of personal data protection, the development of data economy. As a result, it is proposed to determine the legal status of 5G technologies taking into account the transboundary component. The key directions of development of legal regulation in this area are: ensuring information security, distribution of radio frequency spectrum, improvement of legal norms to wireless communication innovations in health care, transportation, industry, public administration.

**Keywords:** quantum technologies, wireless communication, authentication, anonymized data, Internet of Things, data economy, digital economy

**Введение.** Развитие технологий 5G (пятое поколение беспроводной связи) открывает для общества безграничные возможности по скорости и объему передачи данных, появляются новые возможности в различных областях, включая промышленность, связь, медицину и т.п. В то же время возникают вопросы правового и технического регулирования данной сферы, проблемы воздействия на здоровье человека.

Пятое поколение беспроводной связи призвано обеспечить более высокую скорость передачи данных, минимальную задержку и увеличенную емкость сети в сравнении с предшествующими версиями. Среди основных преимуществ можно отметить превышение скорости 5G в 100 раз по сравнению с 4G; сверхнизкая

задержка в пределах 1 мс, которая позволяет применять технологию в критически важном программном обеспечении, как управление движением транспортных средств или роботами в медицине при проведении хирургических операций. Однако развитие технологий и использование новых архитектур и функций, таких как сегментирование сети, виртуализация и облако, представят новые угрозы, которые потребуют внедрения новых типов средств управления [2] и правовой регламентации.

Актуальность темы исследования обусловлена рядом факторов.

Во-первых, необходимостью разработки новых нормативных правовых актов, которые включают вопросы лицензирования частот, защиты персональных данных и обезличенных данных, обеспечения кибербезопасности, определение ответственности операторов связи и поставщиков оборудования. Также возникает необходимость в установлении стандартов безопасности технологий 5G, которая является главным приоритетом при развертывании беспроводной связи. Эти положения включают расширенные меры кибербезопасности в условиях развития квантовых технологий и управления существующими и потенциальными рисками. Внимание уделяется аутентификации устройств, защиты от вторжений и управления доступом, шифрования трафика.

Во-вторых, стандарты безопасности в сфере аутентификации устройств призваны обеспечить применение шифрования на основе квантовой криптографии и безопасные элементы в устройствах. Защита от вторжений включает интеллектуальные алгоритмы мониторинга сетевого трафика, которые дают возможность обнаруживать и блокировать кибератаки в режиме реального времени. Инновационные системы управления доступом регулируют и контролируют доступ критически важным сетевым ресурсам, ограничивая риски компрометации. Разработка стандартов безопасности относится к техническому регулированию, которое осуществляется в тесной связке с правовым.

В-третьих, важное значение приобретает защита персональных данных, которые обрабатываются при использовании беспроводных сетей. К ним относится определение местоположения, предпочтения и привычки, что требует усиления мер конфиденциальности в соответствии с новыми регуляторными нормами, такими как GDPR. Для обеспечения защиты персональных данных используется шифрование данных, управление согласием, проверка использования данных и прозрачность.

В-четвертых, развитие беспроводной связи открывает новые возможности для цифровой экономики, реализовать инновационные приложения и услуг. Развитие получают умные производства, удаленная хирургия и диагностика, беспилотные автомобили, удаленное образование и персонализированные онлайн-курсы.

В-пятых, использование беспроводных сетей сталкивается с техническими, экономическими и социальными проблемами. Так развертывание сетей 5G для обеспечения покрытия в труднодоступных регионах сопряжено со значительными финансовыми и капитальными затратами, а также сложностями построения инфраструктуры. Важной задачей становится сопряжение и совместимость сетей разных стандартов, их согласование. Возникает необходимость с помощью правового регулирования обеспечить стимулирование инноваций

и обеспечение безопасности цифровых технологий и сетей, что требует системных действий государства, общества и экономики отрасли связи.

В-шестых, внедрение технологий беспроводной связи воздействует на общество, приводящего к обсуждению социальных и этических вопросов. Так, в период пандемии в социальных сетях бурно обсуждался вопрос негативного воздействия стандарта 5G на здоровье человека. Это обосновывалось доводами и примерами из научной литературы и практики применения и требует детального изучения. Также многие обеспокоены угрозами неприкосновенности частной жизни и целостности данных. Возникает цифровое неравенство из-за высокой стоимости услуг нового вида связи, которые могут быть недоступны для некоторых групп населения.

В этой связи необходимо изучение существующих норм правового регулирования применения стандарта 5G и формирование предложений по его совершенствованию, а также решение таких задач, как исследование технологии 5G как объекта правового регулирования; определение особенностей технического регулирования технологий 5G; анализ социальных аспектов внедрения технологий 5G; исследование государственной политики в сфере развития технологий 5G; использование международного опыта и сотрудничества в области правового и технического регулирования технологий 5G; формулирование перспектив развития технологий 5G и их правового и технического регулирования.

**Основная часть.** В настоящее время принят ряд федеральных законов и подзаконных актов, направленных на регулирование технологий беспроводной связи, в том числе Распоряжение Правительства РФ от 24 ноября 2023 г. № 3339-р «Об утверждении Стратегии развития отрасли связи РФ на период до 2035 г.», приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 27 декабря 2019 г. № 923 «Об утверждении Концепции создания и развития сетей 5G/IMT-2020 в Российской Федерации». Законы «О связи» 1995 и 2003 годов четко определяют эволюционное видение государства на данную сферу: конкретизируя права и обязанности субъектов права, защищая свободы граждан и пользователей электросетей [3].

Исследование проблемы содержится в работах известных ученых в области информационного и цифрового права, таких как Бачило И. Л., Поляковой Т. А., Копылова В. А., Лопатина В. Н., Рассолова М. М., Батурина Ю. М., Залоило М. В., Минбалеева А. В., Камаловой Г. Г., Терещенко Л. К., Тедеева А. А., Чеботаревой А. А., Чубуковой С. Г., Наумова В. Б., Смирнова А. А., Добробабы М. Б. Сущность правового регулирования технологий беспроводной связи изложена в работах доктора юридических наук, профессора Ковалевой Н. Н. [1. С. 196–202], проблемы технического регулирования затронуты в исследованиях доктора юридических наук Камаловой Г. Г.

Проведенное исследование правового регулирования технологий беспроводной связи позволило определить основные проблемы и направления совершенствования в данной сфере общественной деятельности.

Одним из важных аспектов является определение правового статуса технологий 5G, которые рассматриваются с точки зрения телекоммуникационной инфраструктуры связи, подлежащие соответствующему лицензированию и регу-

лированию, или как технологические устройства, рассматриваемые как потребительские товары, на которые могут распространяться общие нормы безопасности и технического регулирования. Наиболее эффективным подходом должно стать комплексное регулирование беспроводных технологий, которое учитывает инфраструктурную и функциональную специфику, а также особенности устройств, с помощью которых осуществляется связь.

Технологии 5G с самого начала рассматривались как международный проект, поэтому важно учитывать их развитие по всему миру, требующее тесного сотрудничества многих стран и международных организаций. Сотрудничество в разработке стандартов заключается в согласовании общих технических стандартов и требований, что позволяет осуществлять совместимость и масштабируемость технологий. Координация в использовании и распределении радиочастотного спектра между странами позволяет эффективно разворачивать инфраструктуру. Обмен опытом и лучшими практиками приведет к ускорению процесса внедрения беспроводных сетей, снизит затраты на разработку однотипных элементов технологий и устройств. Обеспечение безопасности и конфиденциальности данных также требует сотрудничества стран, направленное на защиту персональных данных, минимизацию рисков критически важных объектов и повышения доверия к 5G.

Беспроводные технологии нового стандарта не нашли еще достаточно широкого применения, находятся на этапе развертывания, но уже сейчас демонстрируют значительный потенциал для трансформации различных сфер деятельности общества и экономики. В качестве перспективных направлений развития 5G можно отметить расширение областей применения от умного дома до умного города и производства, телемедицины, умного государства. Операторы связи будут развивать инфраструктуру 5G, инвестировать в увеличение площади покрытия и пропускной способности беспроводных сетей. Происходит интеграции с другими сквозными технологиями, как искусственный интеллект, виртуальная и дополненная реальность, робототехника. Основным фактором для повышения доверия потребителей будет обеспечение безопасности, защита информации конфиденциального характера от информационных угроз, создание стандартов безвредного использования беспроводной связи для людей.

В качестве перспектив развития правового регулирования необходимо отметить использование 5G для сбора и обработки больших объемов данных с применением систем искусственного интеллекта с учетом совершенствования законодательства о персональных данных и ответственности за их использование. Так законодателем было введено понятия «обезличенные данные» для их сбора без согласия субъекта персональных данных и невозможности его идентификации. Такие данные позволяют без привязки к конкретному лицу проводить исследования о предпочтениях, предложениях и т.п. Правовое и техническое регулирование необходимо при массовом внедрении технологий 5G в рамках концепции «Интернета вещей» для обеспечения кибербезопасности, совместимости устройств и защите прав потребителей. Важное значение приобретает регулирование беспилотных технологий (транспортных, летательных и других средств) для определения правовой ответственности создателя, программиста, пользователя.

Особенности технического регулирования технологий 5G заключаются в обеспечении безопасности, стандартизации оборудования и требований экологии, разрешении частотного спектра и развитие инфраструктуры, контроль за финансовыми расходами и использования данных. Стандартизация оборудования позволяет обеспечивать совместимость различных устройств, экологические стандарты устанавливают требования к энергоэффективности и воздействия на окружающую среду и человека. В этой связи разрабатываются технологические стандарты и протоколы на основе методов шифрования, аутентификации пользователей и устройств, фильтрации вредоносных программ. Управление спектром и его распределением позволяет избежать перекрестных помех среди операторов и оптимизировать использование ресурсов. Обеспечение высокой скорости достигается за счет создания новой инфраструктуры, включая установку новых вышек и оборудования. Операторы связи тратят значительные финансовые ресурсы для реализации технологии 5G, поэтому необходимо учитывать эффективность таких вложений. В то же время рост объемов данных предполагает совершенствование системы регулирования их использования и защиты данных конфиденциального характера.

**Заключение.** Мы считаем, что законодательство должно установить допустимый уровень SAR для дополнительной защиты жизни и здоровья граждан. Измерение поглощения излучения на квадратный сантиметр может быть адекватным решением, учитывая сложность характеристик тканей человека и других поверхностей. Законодательству следует адаптировать один из существующих стандартов или разработать собственный.

### Список литературы

1. Ковалева Н. Н. Правовое и техническое регулирование технологий 5G: перспективы развития в России // Новые горизонты развития системы информационного права в условиях цифровой трансформации / Отв. ред. Т.А. Полякова, А. В. Минбалеев, В. Б. Наумов. – М. : Институт государства и права РАН, 2022. – С. 196–202.
2. Радченко О. Л., Гаязова Е. Э. Проблемы безопасности 5G // Электронная наука. – 2021. – Т. 2, № 2. – EDN EGFSWI.
3. Целиковский В. Д., Ковтун Н. А. Правовое регулирование технического обеспечения и уровня электромагнитной энергии, включая SAR, для сетей 5G: жизнь и здоровье человека в РФ // Международный научно-исследовательский журнал. – 2024. – № 5 (143). – URL: <https://research-journal.org/archive/5-143s-2024-may/10.60797/IRJ.2024.143.123> – DOI: 10.60797/IRJ.2024.143.123

**Р. Р. Сабиров,**

аспирант,

Казанский инновационный университет

имени В. Г. Тимирязова

## **КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ЛИЦ, СОВЕРШАЮЩИХ ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

**Аннотация.** Актуальность исследования связана с высоким уровнем киберпреступности в России, что требует разработки эффективных мер противодействия. В статье рассматривается криминологическая характеристика лиц, совершающих преступления в сфере компьютерной информации, на основе анализа предыдущих исследований. Предлагается классификация таких преступников в зависимости от способа совершения преступления, уровня навыков в области информационных технологий и демографических признаков. Работа направлена на формирование более глубокого понимания типов киберпреступников, что позволит разрабатывать более целенаправленные и эффективные меры профилактики и борьбы с киберпреступлениями.

**Ключевые слова:** киберпреступность, киберпреступник, хакер, классификация киберпреступников, типология киберпреступников, личность киберпреступника, преступления в сфере компьютерной информации, способы совершения преступлений в сфере компьютерной информации

## **CRIMINOLOGICAL CHARACTERISTICS OF PERSONS COMMITTING CRIMES IN THE FIELD OF COMPUTER INFORMATION**

**Abstract.** The relevance of the study is related to the high level of cybercrime in Russia, which requires the development of effective counteraction measures. The article examines the criminological characteristics of persons who commit crimes in the field of computer information, based on the analysis of previous studies. The classification of such criminals is proposed depending on the method of committing the crime, the level of skills in the field of information technology and demographic characteristics. The work is aimed at developing a deeper understanding of the types of cybercriminals, which will allow us to develop more targeted and effective measures to prevent and combat cybercrime.

**Keywords:** cybercrime, cybercriminal, hacker, classification of cybercriminals, typology of cybercriminals, identity of a cybercriminal, crimes in the field of computer information, methods of committing crimes in the field of computer information

**Введение.** С каждым годом объем данных, циркулирующих в цифровом пространстве, стремительно растет, что создает благоприятные условия для злоумышленников, использующих уязвимости информационных систем в своих преступных целях. Нарушения в области компьютерной информации могут иметь разрушительные последствия не только для отдельных граждан и организаций, но и для национальной и глобальной безопасности.

Настоящее исследование актуально прежде всего необходимостью понимания мотивации, социальных и демографических особенностей лиц, совершающих преступления в сфере компьютерной информации, а также их профессиональных навыков и методов совершения преступлений. Это понимание играет ключевую роль в разработке эффективных стратегий предупреждения, раскрытия и расследования преступлений в данной области, а также в формировании адекватных законодательных и правоохранительных мер противодействия.

**Основная часть.** «Как отмечают исследователи, структура киберпреступности в России включает две группы преступлений: преступления в сфере компьютерной информации, а также преступления с применением информационно-телекоммуникационных технологий» [1. С. 114].

«Также одним из оснований типологии киберпреступников в научной литературе предлагается способ совершения преступлений. В зависимости от способа выделяют обычных киберпреступников, которые занимаются незаконными действиями в рамках отдельных видов преступной деятельности, например наркоторговля через Интернет. А также выделяют преступников, действующих в области компьютерной информации и технологий, чья противоправная деятельность возможна исключительно в киберпространстве, например, использование вредоносных компьютерных программ» [3. С. 105].

В настоящем исследовании предлагается рассмотреть криминологическую характеристику лиц, совершающих преступления в сфере компьютерной информации.

В бытовом обывательском представлении киберпреступник чаще всего ассоциируется с компьютерным хакером, одиноким асоциальным молодым человеком, способным «хакнуть», то есть взломать любую компьютерную систему. Подобное представление о киберпреступнике можно встретить и в научной литературе, исследователи характеризуют его как человека, не обладающего привлекательными внешними данными или имеющими трудности общения со сверстниками, противоположным полом, который ищет самореализации в виртуальном мире, самоутверждается, совершая неправомерный доступ к компьютерной информации или создавая компьютерный вирус [4. С. 86].

Подобное представление о киберпреступниках уже не соответствует реальной картине, киберпреступность стала коммерчески успешным явлением, что как следствие привлекло в эту сферу людей с предпринимательскими качествами и авантюрным духом [8. С. 258].

В современном мире характеристика киберпреступника может быть крайне разнообразна, преступления часто совершаются группой лиц с четким распределением ролей по специализации.

Современные киберпреступники могут отличаться различным уровнем образования, владения информационными технологиями, возрастом, мотивом, социальным положением, что подтверждается в отечественных [1; 3; 5; 8; 9] и зарубежных исследованиях [11. С. 102–103].

Характеризуя особенности лиц, совершающих преступления в сфере компьютерной информации в научной литературе, выделяют следующие типы в зависимости:

### 1. От способа совершения преступления.

Согласно имеющимся исследованиям [9] рассматриваемую категорию киберпреступников, можно классифицировать в зависимости от способа совершения преступления следующим образом:

– **Применение вредоносных компьютерных программ для неправомерного доступа к мобильным устройствам, компьютерам, ноутбукам и т. д.**

Преступники данной группы могут действовать как одни, так и в группе с четким распределением ролей и функций при реализации более сложного проекта, такие роли можно разделить на создателей, распространителей, и пользователей вредоносных программ. В зависимости от роли будут отличаться и средний возраст преступников, их уровень образования, а также наличие навыков в сфере информационных технологий (далее – ИТ). Однако обычно это мужчины 18–40 лет, с высшим или средним специальным образованием, действующие из корыстных мотивов [9. С. 26–27].

Наличие ролей у киберпреступников обусловлено не только техническими аспектами их деятельности, но и использованием методов социальной инженерии.

В большинстве случаев при киберпреступлениях средства защиты информации работают эффективно, однако слабым звеном часто оказывается сам пользователь из-за своей некомпетентности. Компьютерная система, подвергающаяся взлому, никогда не функционирует изолированно – всегда присутствует человеческий фактор [10. С. 134]. Проблема в том, что как специалисты по информационной безопасности, так и обычные пользователи компьютеров зачастую недостаточно осведомлены о рисках, связанных с применением технологий социальной инженерии [2. С. 31].

Социальная инженерия, направленная на манипуляцию человеческими эмоциями и поведением, позволяет киберпреступникам эффективно распределять задачи и роли внутри своих групп. Например, один участник может специализироваться на фишинге – искусстве обмана для получения конфиденциальной информации, тогда как другой – на технической поддержке атак, например, создании вредоносных компьютерных программ. Такое разделение ролей повышает эффективность операций, поскольку каждый участник группы концентрируется на своей задаче.

– **Неправомерный доступ к учетным записям в социальных сетях и электронным почтовым ящикам.**

Такие преступники чаще всего действуют самостоятельно из корыстных мотивов или с целью проверки своих умений, пол мужской, разброс по возрасту большой 16–40 лет, но четкого разграничения по уровню образования и социальному статусу не имеется, по характеру зажатые и стеснительные, реальному общению предпочитают виртуальное [9. С. 27–28].

– **DDoS-атака** (от англ. Denial of Service – отказ в обслуживании) – атака на систему, например сайт, в виде большого количества фиктивных запросов, что должно привести к отказу в доступе к системе обычным пользователям.

Преступники данной группы также действуют самостоятельно из корыстных мотивов, чаще всего это мужчины 20–40 лет, безработные, без высшего и

специального образования в сфере ИТ, в браке не состоят, не общительные и замкнутые, то есть виртуальный мир для них ближе реального [9. С. 28–29].

## **2. От уровня навыков киберпреступника в ИТ сфере.**

В научной литературе существуют исследования посвященные классификации киберпреступников в зависимости от их уровня владения компьютерной техникой и навыков программирования.

Так М. В. Жижина и Д. В. Завьялова предлагают выделить три группы субъектов преступлений в сфере компьютерной информации:

– **Лица с различным уровнем навыков в ИТ сфере, которые не ведут систематической преступной деятельности.**

Как указывают авторы это преступники, действующие в силу обстоятельств. Обычно такие лица ранее не были замечены в преступной деятельности и не связаны с криминальным миром [5. С. 154].

– **Лица с низким или средним уровнем навыков в ИТ сфере, которые ведут систематическую преступную деятельность.**

Такие лица обладают низкими или средними навыками в ИТ сфере, и как следствие плохо понимают работу программного кода. В связи с этим в своей преступной деятельности используют уже готовые технические решения, а не разрабатывают программное обеспечение специально под определенную жертву [5. С. 154].

– **Лица с высоким уровнем навыков в ИТ сфере, которые ведут систематическую преступную деятельность.**

Участники данной группы обладают профессиональными знаниями и навыками, чаще всего имеют узкую специализацию [5. С. 155–156].

Исследования в области киберпреступности показывают, что мотивация киберпреступников может быть весьма разнообразной и сложной [8. С. 258]. Одной из ключевых причин, способствующих вовлечению в киберпреступную деятельность, является финансовая выгода, экономические стимулы играют решающую роль в выборе пути киберпреступления. Преступники, желая получить быстрый доход, могут использовать различные методы, такие как фишинг, кража личных данных и проведение атак с целью вымогательства. Корыстные мотивы чаще характерны для представителей второй и третьей группы вышеперечисленной классификации, то есть для преступников ведущих систематическую преступную деятельность, для которых она является основным источником дохода. В то же время, некоторые киберпреступники могут быть мотивированы мстостью, хулиганскими, идеологическими или политическими целями, такими как протест против системной несправедливости или стремление подорвать политические режимы [5. С. 154–156].

## **3. От демографических признаков.**

Согласно данным отчета Судебного департамента при Верховном Суде РФ о демографических признаках осужденных за преступления в сфере компьютерной информации (статьи 272–274.2 УК РФ) за 2023 г. соотношение киберпреступников распределено следующим образом:

- по половому признаку:
- мужчины – 71,5 %;

- женщины – 28,5 %.
- по возрасту:
  - в возрасте от 18 до 24 лет – 42,3 %;
  - в возрасте 25–29 лет – 18,0 %;
  - в возрасте 30–49 лет – 35,7 %;
  - в возрасте 50 лет и старше – 3,9 %.
- по уровню образования:
  - обладатели высшего профессионального образования – 32,7 %;
  - среднего профессионального образования – 41,4 %;
  - среднего общего образования – 20,7 %;
  - с основным общим, начальным, либо без образования – 5,1 %.
- по месту жительства:
  - постоянные жители данной местности – 96,1 %;
  - другие жители иной местности – 3,9 %;
- по роду занятий (социальному положению):
  - рабочие – 25,8 %;
  - государственные и муниципальные служащие – 2,7 %;
  - служащие коммерческой или иной организации – 35,1 %;
  - лица, осуществляющие предпринимательскую деятельность или участвующие в предпринимательской деятельности – 3,3 %;
  - учащиеся и студенты – 1,5 %;
  - нетрудоспособные (неработающие) – 1,2 %;
  - трудоспособные лица без постоянного источника дохода – 16,8 %;
  - иные сотрудники правоохранительных органов, в том числе органов прокуратуры – 3,0 %;
  - лица прочих занятий – 10,5 %.

Проанализировав данные официальной статистики можно сделать вывод, что киберпреступником преступлений в сфере компьютерной информации чаще всего выступают местные жители мужчины в возрасте от 18 до 24 лет либо от 30 до 49 лет, обладающие средним профессиональным либо высшим профессиональным образованием, по роду занятий служащие коммерческой или иной организации либо рабочие [7].

Думаем верным согласиться с М. В. Жижиной и Д. В. Завьяловой в том, что по причине высокой латентности данных категорий преступлений официальная статистика не в полной мере отражает реальную картину [5. С. 153–154]. Это связано как с высоким уровнем профессионализма киберпреступников, их осторожностью и скрытностью при совершении преступлений, возможностью сохранения анонимности в сети, так и с тем, что часто потерпевшие от киберпреступлений не заявляют о преступлениях либо по причине стыда, что были обмануты, либо по причине неуверенности в положительном исходе расследования [6. С. 150].

**Заключение.** Одним из важных выводов является возможность выделения различных типов лиц, совершающих преступления в сфере компьютерной информации, в зависимости от ряда факторов. Во-первых, типология может быть основана на способах совершения преступления. Во-вторых, важным критерием является уровень ИТ-компетенций преступников, варьирующийся от низких

навыков у новичков до профессионалов, обладающих глубокими техническими знаниями и умениями. В-третьих, демографические признаки, такие как возраст, пол, образование и социальное положение, также оказывают влияние на криминальное поведение в цифровой среде.

Таким образом, более глубокое понимание характеристик преступников в сфере компьютерной информации открывает возможности для разработки целенаправленных профилактических и правоприменительных мер. Создание эффективных программ профилактики, повышение уровня киберграмотности населения и укрепление законодательной базы станут важными шагами в противодействии этой форме преступности.

### Список литературы

1. Бабурин В. В., Карабеков К. О. Криминологическая характеристика личности киберпреступника в Российской Федерации и Республике Казахстан // Психопедагогика в правоохранительных органах. – 2024. – Т. 29, № 1(96). – С. 113–119. DOI: 10.24412/1999-6241-2024-196-113-119
2. Бегишев И. Р., Берсей Д. Д. Генезис криминальной социальной инженерии // Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции (г. Казань, 22 сентября 2023 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 6. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – С. 23–34. EDN: IDLEUI. DOI: [http://dx.doi.org/10.21202/978-5-8399-978-5-8399-0819-2\\_476](http://dx.doi.org/10.21202/978-5-8399-978-5-8399-0819-2_476)
3. Григорян С. А. Особенности личности современного «киберпреступника» // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2022. № 8(147). С.103–106.
4. Евдокимов К. Н. Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области) // Сибирский юридический вестник. – 2011. – № 1(52). – С. 86–90.
5. Жижина М. В., Завьялова Д. В. Личность субъекта преступлений в сфере компьютерной информации как системообразующий элемент криминологической характеристики (по материалам российских и зарубежных источников) // Актуальные проблемы российского права. – 2022. – Т. 17, № 5(138). – С. 149–158. DOI: 10.17803/1994-1471.2022.138.5.149-158
6. Майоров А. В. Влияет ли цифровизация на виктимизацию в современном обществе? // Виктимология. – 2022. – Т. 9, № 2. – С. 148–156. DOI: 10.47475/2411-0590-2022-19202
7. Отчет о демографических признаках осужденных по всем составам преступлений Уголовного кодекса Российской Федерации // URL: [http://www.cdep.ru/userimages/sudebnaya\\_statistika/2023/k5\\_1-svod\\_vse\\_sudy-2023.xls](http://www.cdep.ru/userimages/sudebnaya_statistika/2023/k5_1-svod_vse_sudy-2023.xls)
8. Поляков В. В., Попов Л. А. Особенности личности компьютерных преступников // Известия АлтГУ. – 2018. – № 6(104). – С. 256–259. DOI: 10.14258/izvasu(2018)6-49

9. Родивилин И. П. Типологизация лиц, совершающих преступления в сфере компьютерной информации, по способу преступного деяния // Научный вестник Омской академии МВД России. – 2017. – № 4(67). – С. 25–29.

10. Янгаева М. О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. – 2021. – № 1(42). – С. 133–138.

11. Holt T. J., Bossler A. M., Seigfried-Spellar K. C. Cybercrime and Digital Forensics. Introduction. Second Edition. – Abingdon, Oxon : Routledge, 2018.

**А. С. Фартушнова,**  
сотрудник ООО «Отель»

### **ПРАВОВЫЕ АСПЕКТЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ: РЕАЛИИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ**

**Аннотация.** Сегодня и уже немало лет вопросы правового оснащения кибербезопасности не просто сохраняют свою актуальность, но и в отдельных аспектах своей сферы продолжают отставать от реальных темпов развития цифровых систем. Вместе с тем «цифра» сегодня максимально внедрена во все среды жизни человека. Оцифровываются изображения, текстовая информация о человеке, голосовые тонкости, детали движений и практически все, что связано с человеком и в полной мере идентифицирует его. Все эти возможности ограничиваются во всех случаях, прежде всего, техническими средствами и, как следствие, не ограничены в потенциальном риске, в лучшем случае, утраты, а в худшем – несанкционированной передачи и/или распространения и невозможности злоупотреблений с данными.

**Ключевые слова:** безопасность, право, цифра, цифровые решения, технологии, киберпространство, возможности, перспективы

### **LEGAL ASPECTS OF DIGITAL SECURITY: REALITIES AND DEVELOPMENT PROSPECTS**

**Abstract.** Today and for many years now, the issues of legal framework for cybersecurity not only remain relevant, but also in certain aspects of their sphere continue to lag behind the actual pace of development of digital systems. At the same time, "digital" today is maximally implemented in all environments of human life. Images, text information about a person, voice subtleties, details of movements and almost everything that is associated with a person and fully identifies him are digitized. All these possibilities are limited in all cases, first of all, by technical means and, as a result, are not limited in potential risk, at best, of loss, and at worst – unauthorized transfer and/or distribution and irreparable abuse of data.

**Keywords:** security, law, digital, digital solutions, technologies, cyberspace, opportunities, prospects

**Введение.** Кибербезопасность (иными словами, безопасность в сфере цифровых технологий) – это набор способов достижения свободы с устойчивой защищенностью от потенциальных и реальных угроз в цифровом поле.

ИТ-инфраструктура – по своей сути гибридна: с ресурсами локального и облачного характера, что, в свою очередь, позволяет любой системе гибко распределять все свои резервы. Вместе с тем локальное хранение любых данных – в прямой зависимости от их законного обладателя. С момента же размещения сведений в облачном хранилище такие сведения потенциально доступны не всегда даже до конца известному кругу лиц. Чем шире такой круг, тем выше риск утраты и/или повреждения информации, и стремятся к нулю возможности достоверного установления причинителей вреда.

Сегодня российский законодатель с целью обеспечения защиты своих граждан от злоумышленников в цифровой среде в первую очередь ориентирован на регламентацию деятельности юридических лиц – владельцев цифровых ресурсов, позволяющих обрабатывать персональные данные физических лиц, пользоваться людям соответствующими возможностями тех или иных электронных платформ. В отношении граждан, как субъектов права, законодательство в большей мере носит рекомендательный характер, что тоже позволяет в немалой степени повышать уровень безопасности посредством как образования (просвещения) граждан, так и постоянного напоминания не всегда очевидных вещей.

**Основная часть.** Общего характера меры по информационной защите отражены в ст. 16 Федерального закона № 149-ФЗ от 27.07.2006 года «Об информации...» [2]. И наряду с возможностью получения прав на доступ к информации, неизменной остается защита последней с обеспечением должной конфиденциальности.

Цифровые платформы, как и любое иное средство коммуникации людей, должны подчиняться международному праву и нормам права тех государств, на территории которых они зарегистрированы и/или функционируют. Однако при самом идеальном «правоустройстве» сегодня индивидуальная частная сеть (VPN), как технология, обеспечивающая сетевые соединения поверх какой-либо другой сети, позволяет пользователям обходить идеальную картину правового мира в сфере информационных технологий. И конечно, это не последнее технологическое достижение человечества. А значит, система права должна выстраиваться и функционировать таким образом, чтобы в поле международного права все государства представляли собой единое правовое пространство с минимальным набором коллизий. Проще говоря, чтобы страны взаимодействовали сообща.

Прогрессу в технологической среде сегодня способствует и уже достаточно неплохо развитый искусственный интеллект (далее – ИИ).

Немало граждан разных стран относительно молодого возраста сегодня с легкостью обращаются за помощью к ИИ в целях, в том числе: составления документов, сравнения текстов документов, получения вариантов решений спорных, конфликтных ситуаций и прочих. И ИИ вполне способен предлагать «здравые» решения для относительно простых и типовых задач. Вместе с тем доверие к ИИ повышается, профессионализм тем самым оттесняется как средство, требующее наибольших затрат, нежели ИИ. В качестве эксперимента можно попро-

бовать обратиться к ИИ за составлением проекта нормативного правового акта (НПА) на заданную тему.

Все это облегчает «трудозатратность» человека. Но одновременно с отсутствием должного самоконтроля, может привести к деградации путем максимально-го упрощения всего, что привычно делать человеку, в частности, интеллектуально.

При высоких скоростях развития технологий хаос в регламентации деятельности информационных систем, больших баз данных, выгоден до тех пор, пока «правила» не оказываются в «одних руках» «первых».

Условно говоря, если много лет назад человечество вело войны с целью завоевания земных территорий, то в настоящее время сражения иного плана ведутся между странами за киберпространство, как массовый инструмент влияния на человечество в целом и каждого отдельно взятого человека. Вместе с тем каждое государство, одновременно, должно быть заинтересовано и в том, чтобы максимально единолично влиять на граждан внутри своей страны. И все это тоже сводится к условию конфиденциальности, регламентированной в статье 16 ФЗ № 149-ФЗ от 27.07.2006 года «Об информации...» [2].

Таким образом, защищенность информации должна во всех случаях представлять собой вектор правового регулирования в сфере информационных технологий.

**Заключение.** Сегодня в России законодатель, конкретизировав, расширил гражданские права человека, включив в ст. 128 ГК РФ цифровые права – в имущественные [1].

В условиях развития «цифры» одним из приоритетных выступает международное право – в том его формате, где обеспечивается единство стран в задачах общемировой безопасности (которая неминуемо влечет за собой безопасность граждан отдельных стран) и многополярность в политике с несколькими полюсами сил, способствующая глобальной дисциплине, в том числе и в информационной среде, используемой человечеством.

Нельзя и не нужно «сражаться» за ограничение прав пользователей на получение информации из больших массивов данных. Равно как в обычной жизни человека, качественная и полная информация способствует, в частности, и экономическому развитию любого общества. В бизнесе информация дорого стоит, многое решает и зачастую обеспечивает первенство. Но в любом случае экономика в сфере цифры всегда, неизбежно сопряжена с данными людей: начиная от открытых данных глобальных руководителей и/или публичных личностей, заканчивая сведениями о рядовых сотрудниках, а также о контрагентах – без обеспечения должной защиты утекающими из сфер бизнеса. Так, кроме прочего, экономике больших данных можно сравнивать с экосистемой различных типов участников глобального рынка [5]. В общем и целом в современности информационное развитие влияет одинаково на все, но, безусловно, требует не только обучения пользованию и фильтрованию получаемой информации, но и правового регулирования и на уровне отдельно взятых стран, и на мировой арене – в одинаково заданных направлениях, обеспечивающих защиту данных и человека.

### Список литературы

1. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 08.08.2024 года). [Электронный ресурс]. – URL: <https://online.consultant.ru/riv/cgi/online.cgi?from=388534-1964&req=doc&rnd=YxrF6Q&base=LAW&n=482692#4RJH9NU0CLTn62ey>
2. Об информации, информационных технологиях и о защите информации: Федеральный закон Российской Федерации от 27.07.2006 года № 149-ФЗ (ред. от 08.08.2024 года). [Электронный ресурс]. – URL: <https://online.consultant.ru/riv/cgi/online.cgi?req=doc&base=LAW&n=471228&dst=35&cacheid=B9E08FA424553C7E98C62AD11BE9B778&mode=splus&rnd=iD4uLQ#wYD99NUJE6746r0O>
3. Безотосова А. Р., Валитова Д. В., Васин Е. О. (и др.). Глобальный атлас регулирования искусственного интеллекта. / под ред. А. В. Незнамова, 2023 // СПС «КонсультантПлюс» [Электронный ресурс]. – 2023. – URL: <https://online.consultant.ru/riv/cgi/online.cgi?req=doc&base=CMB&n=19146&cacheid=00C2CB4E986DFB61EF8C8EF756FA3876&mode=splus&rnd=iD4uLQ#ozcB9NUyeTto5xyo>
4. Елизарова Е. О., Настич В. М., Чекулаев С. С. Правовое регулирование цифровой безопасности в России и странах АТР и ее соотношение с кибербезопасностью // Юридическая наука [Электронный ресурс]. – 2020. – № 6. – URL: <https://cyberleninka.ru/article/n/pravovoe-regulirovanie-tsifrovoy-bezopasnosti-v-rossii-i-stranah-atr-i-ee-sootnoshenie-s-kiberbezopasnostyu>
5. Parrilla J. A. C. The Legal Regulation of Digital Wealth: Commerce, Ownership and Inheritance of Data. – 2021. [Электронный ресурс]. – URL: <https://kluwerlawonline.com/journalarticle/European+Review+of+Private+Law/29.5/ERPL2021042>

## ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ФИНАНСОВЫХ И НАЛОГОВЫХ ПРАВООТНОШЕНИЙ

**И. О. Антропцева,**

кандидат юридических наук, доцент,  
Российская академия народного хозяйства и государственной службы при  
Президенте Российской Федерации,  
Финансовый университет при Правительстве Российской Федерации

### РОБОТЫ-СОВЕТНИКИ НА ФИНАНСОВОМ РЫНКЕ КАК ПРЕДМЕТ ПУБЛИЧНОГО ФИНАНСОВОГО КОНТРОЛЯ

**Аннотация.** Развитие цифровых технологий способствует роботизации отдельных процессов при оказании услуг финансовыми организациями, примером такого решения являются роботы-советники. В силу особенностей деятельности, осуществляемой финансовыми организациями, применение ими роботов-советников, а также возникновения рисков причинения ущерба интересам потребителей финансовых услуг требует осуществления публичного финансового контроля. С целью организации эффективного публичного финансового контроля за применением роботов-советников финансовыми организациями в рамках настоящего исследования сделана попытка ответить на вопрос, являются ли роботы-советники объектом или предметом цифрового публичного финансового контроля, что оказывает непосредственное влияние на правовое регулирование возникающих общественных отношений в связи с применением роботов-советников. Полученные выводы основаны, с одной стороны, на том, что роботы-советники представляют собой программный продукт, который как используемый инструмент финансовыми организациями подлежит контролю, с другой стороны, на способности роботов-советников накапливать значительные объемы информации о совершении финансовых операций потребителями финансовых услуг.

**Ключевые слова:** потребитель финансовых услуг, публичный финансовый контроль, робот-советник, финансовая организация, финансовый рынок, финансовые услуги, цифровые технологии

### ROBO-ADVISORS ON THE FINANCIAL MARKET AS A SUBJECT OF PUBLIC FINANCIAL CONTROL

**Abstract.** The development of digital technologies promotes robotization of certain processes in the provision of services by financial institutions, an example of such a solution is robo-advisors. Due to the peculiarities of the activities carried out by financial organisations, the use of robo-advisors by them, as well as the emergence of

risks of causing damage to the interests of consumers of financial services requires the implementation of public financial control. In order to organise effective public financial control over the use of robo-advisors by financial organisations, the present research attempts to answer the question whether robo-advisors are an object or a subject of digital public financial control, which has a direct impact on the legal regulation of emerging public relations in connection with the use of robo-advisors. The conclusions obtained by the author are based, on the one hand, on the fact that robo-advisors are a software product, which as a tool used by financial organisations, on the other hand, they are subject to control, on the ability of robo-advisors to accumulate significant amounts of information on the performance of financial transactions by consumers of financial services.

**Keywords:** financial services consumer, robo-advisor, financial organisation, financial market, financial services, digital public financial control, digital technology

**Введение.** Конкурентоспособность финансовых организаций на финансовом рынке напрямую зависит от применения новых технологичных разработок, которые позволяют сократить временные затраты и повысить качество оказания услуг, а также уменьшить их стоимость за счет сокращения затрат финансовой организации.

Цифровые технологии используются в первую очередь для оптимизации выполнения рутинных задач, простых функций. Такая цифровая технология, как искусственный интеллект, способна решать конкретные задачи на основе моделей и алгоритмов, созданных и отлаженных человеком, иногда даже лучше, чем человек [1. С. 36]. Одним из направлений стало применение умных помощников (чат-ботов, голосовых роботов), которые позволяют заменить людей-консультантов.

Компании, оказывающие услуги на финансовом рынке, стали внедрять автоматизированных консультантов, которые способны помочь в выборе банковских продуктов, нужного страхового полиса, а также проконсультировать в сфере инвестирования. На мировом рынке данные технологии используются с 2010 года, в российской практике с 2018 года. Учитывая, что институт роботов-советников продолжает развиваться и активно применяется при оказании посреднических услуг на финансовых рынках, более того, появляются компании, которые оказывают исключительно роботизированные консультации, то возникает вопрос обеспечения публичного финансового контроля за их использованием.

**Основная часть.** Роботы-советники представляют собой автоматизированный инвестиционный сервис, который оказывают финансовые консультации в сфере инвестиций, страхования, потребительского кредитования и в иных секторах финансовых услуг [4]. С технической точки зрения – это программное обеспечение, которым управляет финансовый посредник. Особенность функционирования роботов-советников заключается в том, что они собирают информацию о клиентах, генерируют и исполняют рекомендации, осуществляют постоянный мониторинг инвестиций [5]. Специфика роботов-советников обусловлена тем, что, как правило, они функционируют автономно при консультировании клиентов, а привлечение человека осуществляется периодически и исключи-

тельно как дополнительная услуга. В связи с этим возможность рассмотрения роботов-советников в качестве самостоятельного объекта контроля со стороны регуляторов вызывает сомнение.

Роботы-советники, как было уже указано, представляют собой сервис, который имеет техническую составляющую, то есть совокупность алгоритмов и процессов, которые генерируют персонализированные консультации и решения для клиентов. Соответственно, представляется целесообразным определить требования к функционированию алгоритмов и процессов, поскольку некачественная консультация способная причинить ущерб интересам потребителей финансовых услуг.

Функционирование роботов-советников основано на использовании искусственного интеллекта и машинного обучения, которые позволяют ему принимать решения на основе анализа заполненного клиентом опросника, определения профиль-риска инвестора, алгоритмов автоматического мониторинга. Любопытно предложение, сделанное Т. Бейкером и Б. Делаертом, о необходимости хранения исходных данных клиента и продукта, алгоритма консультирования, интерфейса выбора, рыночных условий и результата каждого взаимодействия с клиентом подобно «черным ящикам», предлагаемым для самоуправляемых автомобилей, которые в дальнейшем способны стать тем источником информации, на основании которой можно будет определить ответственность финансового посредника-владельца роботов-советников [4]. Аналитическая автоматизированная обработка данной информации при проведении контрольно-надзорных мероприятий позволяет определять риски функционирования роботизированного советника, привлечь к ответственности за причинение ущерба потребителям финансовых услуг.

Фактически возникает контроль со стороны одного искусственного интеллекта за другим, в связи с чем видится возникновение отдельного риска объективности работы таких алгоритмов и возможности их выхода из-под контроля с учетом возможности самообучения и самосовершенствования. Фактически получается, что один искусственный интеллект контролирует другой, что не может не вызывать сомнения в результативности такого подхода, отсутствии технологических сбоев, хотя подобные риски скорее всего могут возникнуть при более высоком уровне развития искусственного интеллекта.

Использование роботов-советников влечет возникновение ряда рисков: рекомендация неподходящих продуктов, манипулирование рынком, которое может быть преднамеренным и непреднамеренным [5], причинение ущерба клиентам в связи с ошибками в работе алгоритма, а также репутационные риски для участника рынка, предлагающего такие услуги. Кроме того, необходимо отметить еще один аспект – отдельные услуги, предоставляемые роботами-советниками, не подпадают под действие существующих нормативных актов регуляторов в сфере финансовых рынков. При этом следует обратить внимание, что Управление по финансовому регулированию и надзору Великобритании (FCA) придерживается позиции, что управление рисками – ответственность компании, которая использует роботов-советников независимо от того, является ли она разработчиком или заказчиком данного сервиса [6].

Возникает вопрос, действительно ли необходимо разработать нормы, регулирующие деятельность роботов-советников, и осуществлять поиск иных инструментов для надзора за их деятельностью, чтобы минимизировать риски, которые возникают в связи с их использованием. Международные подходы к правовому регулированию деятельности роботов-советников различны. Например, Европейская служба банковского надзора приняла решение не разрабатывать требования, специфичные для роботизированного консультирования, а наблюдать за его развитием и использовать существующие нормативные акты, регулирующие деятельность субъектов в сфере финансовых рынков [5]. В США регулирующие органы выпустили предупреждение для потребителей о рисках роботизированного консультирования, при этом в 2024 г. Комиссия по ценным бумагам и биржам (SEC) приняла поправки, дающие право инвестиционным консультантам, работающим исключительно через интернет, регистрироваться только в Комиссии [8]. Новая Зеландия рассматривает возможность внесения изменений в действующее законодательство [6, 7]. В Российской Федерации используется сочетание регулирования использования роботов-консультантов со стороны Банка России и саморегулирования посредством возложения обязанности на саморегулируемые организации по разработке базовых стандартов по защите интересов потребителей финансовых услуг, совершения операций на финансовом рынке [3]. Аккредитация программ, лежащих в основе роботизированных консультантов, осуществляется Банком России или саморегулируемыми организациями при делегировании им полномочий регулятором [2].

Учитывая разрозненность правовых подходов в мировой практике, представляется, что при рассмотрении роботов-консультантов как программного продукта, функционирующего в состав финансовых организаций, предлагается рассматривать их как предмет цифрового публичного финансового контроля. При этом видится, что с учетом наличия риска причинения вреда интересам вкладчиков целесообразно именно на уровне регулятора проводить аккредитацию программных продуктов, в том числе проводить оценку риска причинения ущерба, осуществлять непрерывный мониторинг качества консультаций, а также ввести ответственность финансовых организаций за причинение ущерба, возникшего вследствие консультирования роботом-советником.

**Заключение.** Проведенное исследование позволяет сделать вывод о том, что роботы-советники в настоящее время самостоятельно не могут рассматриваться как объекты цифрового публичного финансового контроля, поскольку представляют программный продукт, внедряемый финансовыми организациями, но их использование предполагает изменение подходов к контролю и надзору за деятельностью профессиональных участников рынка ценных бумаг, которые их используют. Учитывая, что роботы-консультанты становятся не просто инструментом оказания услуг, но обладают способностью накапливать и анализировать значительные объемы информации, то для цифрового публичного финансового контроля предлагается их рассматривать именно как предмет контроля. Рассмотрение практики правового регулирования и контроля в зарубежных странах позволит сделать вывод о том, что контроль и надзор закрепляется за регуляторами либо используется механизм сочетания государственного регулирования и само-

регулирования, что отражается и на осуществлении контроля и надзора со стороны регуляторов.

Представляется, что цифровой публичный финансовый контроль за роботами консультантами, с одной стороны, должен носить технический характер, связанный с оценкой корректности работы алгоритмов консультирования и вести постоянный мониторинг их функционирования, с другой стороны, осуществлять надзор для минимизации рисков в части требований к использованию роботов-советников и ответственности за качество консультирования, работы с рисками. Кроме того, видится необходимым при цифровизации контроля и надзора в отношении финансовых организаций, включая использование SupTech, обратить внимание и контролировать риск возникновения конфликта между алгоритмами робота-советника и цифровыми контрольно-надзорными механизмами, используемыми регуляторами.

### Список литературы

1. Галлезе-Нобиле К. Регулирование умных роботов и искусственного интеллекта в Европейском союзе. *Journal of Digital Technologies and Law*. 2023;1(1):33-61. <https://doi.org/10.21202/jdtl.2023.2>. EDN: UNSONV.
2. О порядке аккредитации программ для электронных вычислительных машин, посредством которых осуществляется предоставление индивидуальных инвестиционных рекомендаций: Указание Банка России от 27.11.2018 № 4980-У // Вестник Банка России. – 2019. – № 13.
3. О порядке определения инвестиционного профиля клиента инвестиционного советника, о требованиях к форме предоставления индивидуальных инвестиционных рекомендаций и к осуществлению деятельности по инвестиционному консультированию: Указание Банка России от 17.12.2018 № 5014-У // Вестник Банка России. – 2019. – № 13.
4. Baker T., Delaert B.G.C. Regularizing robo advice across the financial services industry. 2018. – URL: [https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2742&context=faculty\\_scholarship](https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2742&context=faculty_scholarship)
5. EBA Report on prudential risks and opportunities arising for institutions from FinTech. – URL: <https://www.eba.europa.eu/sites/default/files/documents/10180/2270909/02c7859f-576e-421e-b243-a145c0eaa131/Report%20on%20prudential%20risks%20and%20opportunities%20arising%20for%20institutions%20from%20FinTech.pdf>
6. Robo Advice: an FCA perspective. – URL: <https://www.fca.org.uk/news/speeches/robo-advice-fca-perspective>
7. Robo-advisors. How do they fit in the existing EU regulatory framework, in particular with regard to investor protection. Provided by the Policy Department for Economic and Monetary Affairs (ECON). June, 2021. // URL: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662928/IPOL\\_STU\(2021\)662928\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662928/IPOL_STU(2021)662928_EN.pdf)
8. SEC Adopts Reforms Relating to Investment Advisers Operating Exclusively Through the Internet // URL: <https://www.sec.gov/news/press-release/2024-42>

**А. Л. Белоусов,**

кандидат экономических наук, доцент,

Финансовый университет

при Правительстве Российской Федерации

## **ЦИФРОВЫЕ ФИНАНСОВЫЕ АКТИВЫ: ВОПРОСЫ РАЗВИТИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ**

**Аннотация.** Настоящее исследование посвящено актуальным вопросам и проблемам развития цифровых финансовых активов в Российской Федерации. Сделан акцент на формировании соответствующей институциональной основы для обеспечения эффективного функционирования и развития цифровых финансовых активов. Обоснована необходимость дальнейшего совершенствования правового поля и его адаптации к внедряемым на практике новым цифровым технологическим решениям в области финансов.

**Ключевые слова:** финансовые технологии, регулирование, цифровые финансовые активы, криптовалюта, блокчейн, цифровизация, цифровые технологии

## **DIGITAL FINANCIAL ASSETS: ISSUES OF DEVELOPMENT OF LEGAL SUPPORT**

**Abstract.** The study is devoted to the development of digital financial assets in the Russian Federation. The emphasis is placed on the formation of an appropriate institutional framework to ensure their effective functioning and development. The need for further improvement of the legal field and its adaptation to the new technological solutions being implemented in practice in the field of finance is substantiated.

**Keywords:** financial technologies, regulation, digital financial assets, cryptocurrency, blockchain, digitalization, digital technologies

**Введение.** Внедрение новых цифровых решений в ряде сфер может в перспективе кардинально изменить сложившуюся архитектуру финансового рынка. Однако без должного правового обеспечения и регулирования это обуславливает рост рисков уязвимости финансовой системы, которая в современных условиях является одним из базисов экономики.

В связи с этим ключевой задачей и Банка России, и законодателя, и представителей финансового сообщества является выработка новых предложений и пересмотр существующих подходов к регулированию отдельных финансовых технологий. Как представляется, необходима разработка новых юридических конструкций, позволяющих включить цифровые технологии, реализуемые в финансовой отрасли в российское правовое поле. Тем самым это даст возможность минимизировать отдельные риски, оказывающее влияние на устойчивость всего финансового сектора.

**Основная часть.** Очевидно, что цифровые технологии все активнее проникают во все большее число сфер хозяйственной деятельности [1. С. 250]. При

этом, как представляется, именно субъекты финансового сектора наиболее восприимчивы к внедрению новых продуктов на основе цифровых решений. Отрадно отметить, что Банк России также не остается в стороне и пытается своевременно адаптировать регуляторное поле для обеспечения развития новых цифровых инструментов [2. С. 20].

Так, уже на рынке успешно работают финансовые маркетплейсы, готовится к полномасштабному функционированию проект цифрового рубля. Как представляется, на финишную прямую выходит новая концепция регулирования криптовалют в Российской Федерации. При этом, уже четыре года назад при активной работе всего финансового сообщества увидел свет Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Закон о ЦФА).

Однако на сегодняшний день цифровые финансовые активы пока что остаются новым и отчасти еще неизведанным большинством населения инструментом увеличения капитала.

Для начала попытаемся кратко раскрыть сущность цифровых финансовых активов. Во-первых, в Российской Федерации цифровые финансовые активы не признаются криптовалютой [4. С. 35]. Во-вторых, в их состав эмитент может включить достаточно разнообразные по основаниям возникновения и особенностям активы. Это могут быть и денежные требования, и возможность осуществления прав по эмиссионным ценным бумагам, и права участия в капитале непубличных акционерных обществ, а также права требования передачи эмиссионных ценных бумаг.

Ключевой особенностью цифровых и финансовых активов и, одновременно, их конкурентным преимуществом является опора на технологию блокчейн. Это обеспечивает возможность проведения сделок посредством смарт-контрактов, что позволяет повысить безопасность и удобство транзакций.

В рамках формирования необходимой инфраструктуры для успешного оборота цифровых финансовых активов легитимацию получили такие субъекты как операторы информационных систем, которые по сути ведут выпуск и учет цифровых финансовых активов. В свою очередь, Банк России осуществляет полномочия по формированию реестра операторов информационных систем. По состоянию на 04.09.2023 в данном реестре содержится информация уже об одиннадцати операторах информационных систем.

При этом несмотря на то, что Закон о ЦФА был принят в 2020 году, первый оператор информационной системы был зарегистрирован только в начале 2022 года. В свою очередь, в середине 2022 года была проведена первая сделка с цифровыми финансовыми активами.

В настоящее время правовое поле в области регулирования цифровых финансовых активов находится еще в процессе формирования. Однако за последний год были сделаны значимые шаги по легитимации использования цифровых финансовых активов на практике. Так, Федеральный закон от 11.03.2024 № 45-ФЗ разрешил использовать данный инструмент в международных расчетах. В рамках данного акта ЦБ РФ получил полномочия определять условия

и вводить ограничения на совершение операций с цифровыми финансовыми активами. И для государства, и для представителей бизнеса подобная легализация использования цифровых финансовых активов может стать действенной мерой для выстраивания новых контуров взаимодействия с иностранными контрагентами из дружественных стран в условиях санкций.

Также точно для частных инвесторов цифровые финансовые активы, как представляется, могут стать достойной альтернативой традиционных облигаций и депозитарных расписок. Сейчас часть цифровых финансовых активов доступна уже и неквалифицированным инвесторам. При этом и для обычных граждан при удачной маркетинговой политике банков цифровые финансовые активы, имея более высокую доходность, могут по крайней мере частично стать альтернативой банковских вкладов. При этом, помимо законодательного обеспечения функционирования цифровых финансовых активов, о чем говорилось выше, имеет смысл также развивать и финансовую грамотность населения в отношении новых цифровых продуктов. Это обусловлено низким уровнем доверия и консервативным взглядом большей части наших сограждан в отношении новых инструментов управления своими сбережениями.

Важно сказать о том, что летом 2024 года в Закон о ЦФА были внесены важные изменения, касающиеся легализации майнинга в Российской Федерации и одновременном запрете рекламы криптовалют. Это говорит о выборе законодателем концептуального пути дальнейшего развития правового поля в этой сфере.

Стоит согласиться с тем, что на данный момент отсутствует унифицированный подход и возможности применения действующих правовых норм в отношении инновационных цифровых активов [3. С. 121].

**Заключение.** Современные цифровые технологии начинают играть все более весомую роль в развитии российской финансовой системы. Генезис цифровых финансовых активов в правовом поле и их функционирование на практике являются лишь подтверждением данного тезиса.

В связи с этим в случае выбора законодателем удачных правовых конструкций, децентрализованные финансы в российской юрисдикции имеют хороший потенциал для своего дальнейшего развития, что станет значимым шагом на пути обеспечения эффективности работы финансовой системы и повышения уровня экономического суверенитета Российской Федерации.

### Список литературы

1. Белоусов А. Л. Адаптация подходов к регулированию финансового сектора в условиях цифровизации // Цифровые технологии и право: Сборник научных трудов I Международной научно-практической конференции. В 6-ти томах, Казань, 23 сентября 2022 года / Под редакцией И. Р. Бегишева [и др.]. Том 3. – Казань: Издательство «Познание», 2022. – С. 248–251.

2. Белоусов А. Л. Правовые аспекты развития финансового сектора в условиях цифровизации // Цифровые технологии и право : сборник научных трудов II Международной научно-практической конференции В 6 т., Казань, 22 сентября 2023 года. – Казань: Издательство «Познание», 2023. – С. 15–19.

3. Мурадян С.В. Цифровые активы: правовое регулирование и оценка рисков // Journal of Digital Technologies and Law. 2023;1(1):123–151. <https://doi.org/10.21202/jdtl.2023.5>. EDN: RIZOKS

4. Разин И. Д. Криптовалюта в современных российских реалиях / И. Д. Разин, Д. И. Шмелева // Финансовая экономика. – 2023. – № 8. – С. 133–136. – EDN: OIDXBA

**Ю. М. Белякова,**  
кандидат экономических наук,  
председатель Президиума  
Московской коллегии адвокатов «Покровская застава»,  
Президент Автономной некоммерческой организации  
Экспертно-консультационного центра  
«Интернет-технологий, комплаенс-аудита  
и риск-менеджмента» (АНО ИКАР)

### **РОЛЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ И СЕРВИСОВ В ПРОЦЕССЕ СУДЕБНОГО ДОКАЗЫВАНИЯ В СПОРАХ С НАЛОГОВЫМИ ОРГАНАМИ**

**Аннотация.** В статье рассматриваются практические аспекты работы Федеральной налоговой службы с различными цифровыми сервисами, как доступными для информирования налогоплательщиков, так и частично скрытыми от них. Анализируется конкретная методика Федеральной налоговой службы, в том числе ДСП. Раскрываются практические аспекты работы налоговых органов с цифровыми сервисами в рамках проверочных мероприятий налогового контроля, способами доказательств налоговых правонарушений в рамках досудебного урегулирования и судебных процессов. Рассматриваются возможности налогоплательщиков опровергать доводы налоговых органов в условиях ограничения доступности цифровых сервисов.

**Ключевые слова:** федеральная налоговая служба, цифровые сервисы, налогоплательщики, доказательства налоговых органов, АСК НДС, риск

### **THE ROLE OF DIGITAL TECHNOLOGIES AND SERVICES IN THE PROCESS OF JUDICIAL EVIDENCE IN DISPUTES WITH TAX AUTHORITIES**

**Abstract.** The article examines the practical aspects of the Federal Tax Service's work with various digital services, both available for informing taxpayers and partially hidden from them. Various methods of the Federal Tax Service are analyzed, including those intended for official use. The practical aspects of the work of tax authorities with digital services within the framework of tax control verification measures, methods of their use in proving tax offenses, both within the framework of pre-trial settlement and within the framework of lawsuits, are disclosed. And the abil-

ity of taxpayers to refute the arguments of the tax authorities, taking into account the limitation of the availability of many digital.

**Key words:** federal tax service, digital services, taxpayers, evidence of tax authorities, ASK VAT, risk

**Введение.** Федеральная налоговая служба является одним из наиболее активных пользователей различных аналитических инструментов цифрового контроля. Постоянно развивая цифровые сервисы налоговые органы все больше используют в своей работе подходы контрольно-аналитического подразделения, заменяя выездные проверки камеральными, а также комиссиями, которые часто называют побудительными. В рамках такой работы налогоплательщику, по мнению налогового органа, разъясняется доказательная база, указывающая на выявленные нарушения, и предлагается в добровольном порядке уточнить свои налоговые обязательства в установленные налоговым органом сроки. И только в случае отказа рассматривается вопрос о назначении выездной налоговой проверки. В научной статье анализируются теоретические и практические аспекты использования такого методологического инструмента налогового контроля как камеральные проверки. Особенности риск-ориентированного подхода в рамках камеральных проверок, а также анализируется временный порядок проведения риск-ориентированного камерального контроля с применением Информационно-аналитической системы контрольного блока (далее – ИАС КБ) [3. С. 2].

Определяются пробелы и недостатки временного порядка, несущие в себе наиболее критичные риски для налогоплательщиков. Выводы основаны не только на теоретической части исследования, но и с учетом проведенного исследования судебных прецедентов за 2022–2024 годы. В статье предлагаются к рассмотрению изменения, необходимые к внесению в работу налоговых органов с цифровым сервисом ИАС КБ, и позволяющие минимизировать не столько трудозатраты налогового органа на анализ налогоплательщиков, сколько позволит налогоплательщикам своевременно оценивать свои риски с учетом подходов, которые использует регулятор для аналитической работы.

**Основная часть.** На основании временного порядка проведения риск-ориентированного камерального контроля с применением ИАС КБ (далее – временный порядок) закрепляются такие понятия как:

- кооперация – взаимодействие налогоплательщика с другим налогоплательщиком путем выставления счетов-фактур, перечисления денежных средств, документооборота и прочего взаимодействия, свидетельствующего о наличии гражданско-правовых отношений между налогоплательщиками;

- паспорт риска – совокупность информации и данных о профиле риска (шаблоне схемы), мерах, которые необходимы для минимизации риска, и регламенте их применения, включенной в Реестр рисков;

- профиль риска, это алгоритм выявления риска и правила его доведения для отработки;

- подконтрольность – вид связи, при которой один налогоплательщик оказывает или может оказать влияние на действия других налогоплательщиков, а

также обладает информацией о таких действиях, определяемой на основании информации об учредителях, руководителях, владельцах;

- реестр рисков ИАС КБ, представляющий собой модуль ИАС КБ, реализующий функции обеспечения учета паспортов рисков, их статусной модели и взаимодействия с модулями «Типология схем», «Профили расчета рисков» и «Досье проверки»;

- риск – возможное нарушение налогоплательщиком законодательства о налогах и сборах;

- согласованность – вид связи, при которой один налогоплательщик обладает или должен был обладать информацией о действиях других налогоплательщиков, определяемой на основании информации об IP-адресах, о подписантах НД, об общих сотрудниках, об общем адресе регистрации, адреса регистрации учредителя/директора налогоплательщика, общего имущества, родственных связей, банковских счетах, общего представителя [5].

Шаблон схемы – это основной объект типологии схем, который описывает критерии потенциальных участников схем и связей между ними [3. С. 3–4].

ИАС КБ состоит из набора функциональных модулей: система управления рисками (СУР), Типологии схем, Досье проверки, Визуально-сетевое анализа, Реестра рисков. Реестр рисков ИАС КБ реализует автоматизацию технологического процесса «Ведение реестра паспортов рисков налогоплательщиков, возникающих в ходе проведения камеральных налоговых проверок». Целью формирования Реестра рисков ИАС КБ является учет рисков деятельности налогоплательщиков, а также мер по их минимизации в форме паспортов рисков. Модуль СУР реализует автоматизацию технологического процесса «Управление рисками контрольно-надзорной деятельности». СУР осуществляет автоматизированный отбор налоговых деклараций или налогоплательщиков, соответствующих условиям, заданным в профиле риска и характеризующим наличие риска в виде возможного нарушения налогового законодательства. По информации из различных источников, в том числе по ссылкам в самом временном порядке, можно сделать вывод, что программный комплекс работает совместно с единой информационной системой ФНС России АИС Налог-3, автоматизированной системой контроля АСК НДС-3, АСК ККТ, АСК ДФЛ, настроен по образу и подобию АСК НДС-3, используя такой же подход к визуализации объектов и связей информационно-аналитической системы контрольного блока, основная цель которого, это графическое представление потенциальных схем в виде дерева связей с кластеризацией узлов по подконтрольности и (или) согласованности

В ИАС КБ использованы алгоритмы типологии схем, который реализуется автоматизацией технологического процесса «Управление типологией схем уклонения от уплаты налогов». Типология схем осуществляет автоматизированный отбор налоговых деклараций или налогоплательщиков из числа потенциальных выгодоприобретателей и его окружения из числа контрагентов, соответствуют условиям, а также связям, заданным в шаблоне схемы.

Блок «досье проверок» реализует автоматизацию технологического процесса связанного с взаимодействием налоговых органов при проведении мероприятий налогового контроля в отношении потенциальных участников схем. С по-

мощью блока «Досье проверок» осуществляется учет вновь выявленных рисков и потенциальных схем уклонения.

Так же временный порядок вводит обязательную отчетность, в которой явно прослеживаются элементы обвинительного характера любой камеральной проверки. Так положительными проверками считаются только те, где произошло:

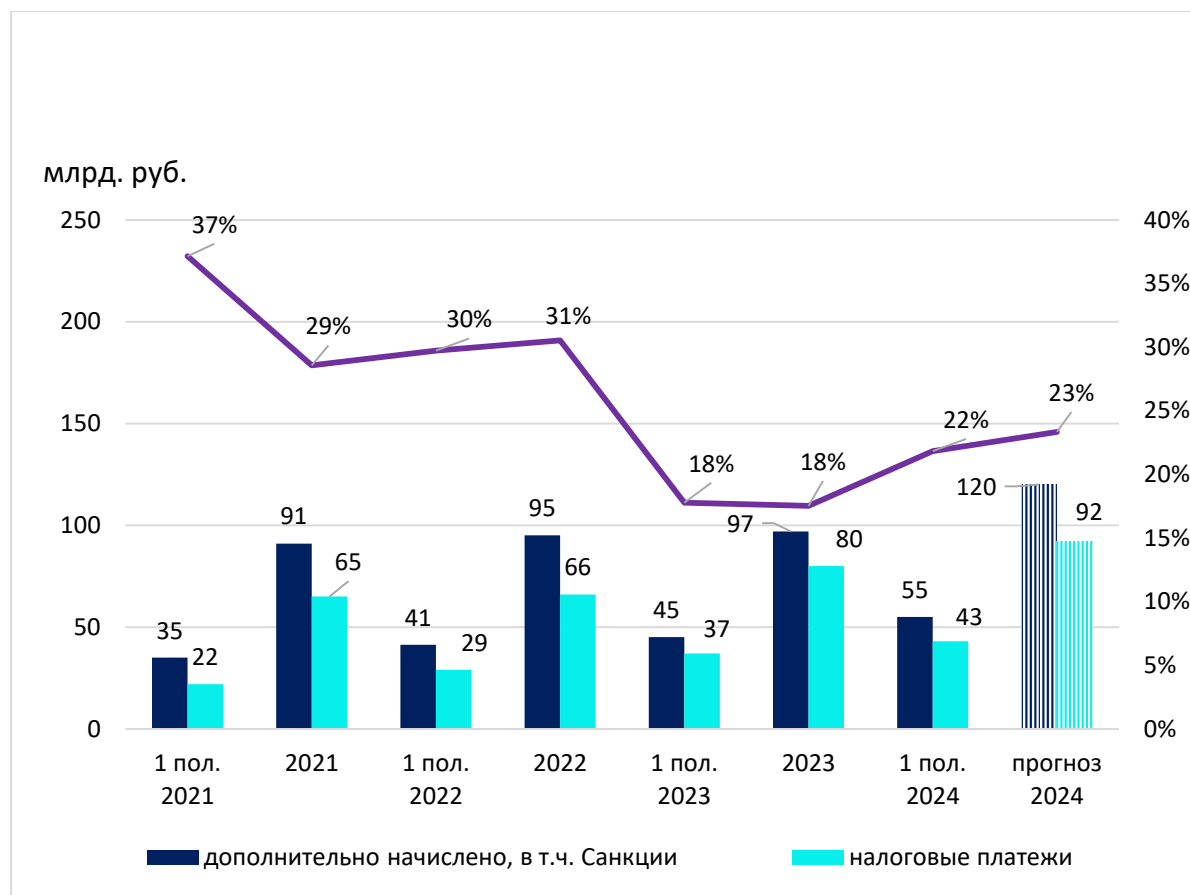
- добровольное уточнение налогоплательщиком налоговых обязательств с последующим устранением выявленной схемы уклонения от уплаты налогов и (или) риска;
- вынесение акта камеральной налоговой проверки с зафиксированными нарушениями налогового законодательства в части выявленной схемы и (или) риска;
- вынесения решения о привлечении к ответственности (об отказе в привлечении к ответственности) с зафиксированными нарушениями налогового законодательства в части выявленной схемы уклонения и (или) риска;
- поступление в доход бюджета суммы неуплаченного налога или не полностью уплаченного налога, квалифицированного как сумма потенциального ущерба бюджету, в случаях, если налогоплательщик преследовал цель неправомерного уменьшения налоговой обязанности либо знал об обстоятельствах, характеризующих контрагента как «техническую» компанию, и об исполнении обязательства иным лицом.

Доказанная судом и/или подтвержденная невиновность налогоплательщика во вменяемом правонарушении трактуется как отрицательный результат работы:

- решение по итогам камеральной налоговой проверки отменено вышестоящим налоговым органом или в судебном порядке;
- схема не доказана по причине сложности (в рамках срока проведения камеральной налоговой проверки доказательная база собрана в недостаточном объеме);
- выявление фактов отсутствия нарушений в ходе камеральной налоговой проверки [1. С. 10].

Безусловно, результатами работы временного порядка и автоматизированных аналитических систем являются цифры поступлений в бюджет. Так, в 2023 году в консолидированный бюджет Российской Федерации поступило налогов, сборов и иных обязательных платежей 26450,4 млн руб., что на 4011,7 млн руб. или на 17,9 % больше поступлений 2022 года ФНС отчиталась, что по итогам контрольно-аналитической работы в 2023 году в бюджет поступило 400 млрд руб. (+2,3% по сравнению с 2022 годом) и 55 % этих поступлений (218 млрд руб.) – это «самостоятельные доплаты» бизнеса без проведения налоговых проверок. То есть «внепроверочные» мероприятия налогового контроля пополняют бюджет даже эффективнее выездных проверок. Например, в Саратовской области, за первое полугодие 2024 года поступило по результатам контрольной и контрольно-аналитической работы более 2,23 млрд рублей, с ростом на 55 млн рублей (2,5 %) по сравнению с первым полугодием 2023 года (2,18 млрд рублей). Дополнительно поступило в бюджет в связи с представлением уточненных налоговых деклараций по результатам проведенной налоговыми органами контрольно-аналитической работы 1,3 млрд рублей, с ростом на 333 млн рублей (34,3 %).

Налогоплательщиками Санкт-Петербурга в бюджетную систему Российской Федерации перечислено более 2 трлн руб. с темпом роста 112,7 %. При этом поступления налоговых платежей по Управлению увеличились к данным прошлого года на 21%, или на 309 млрд и составили 1 814 млрд руб. В федеральный бюджет сумма поступлений составила 444,5 млрд руб., с темпом роста 112,4 % [2].



### Динамика доначислений по результатам камеральных проверок [7]

Счетная Палата Российской Федерации анализируя деятельность Федеральной налоговой службы по итогам 2022 года предложила добавить в аналитическую работу в рамках предпроверочного анализа разработку и включение в систему критериев рисков в целях отбора налогоплательщиков критериев, позволяющих выявлять налоговые риски на основании данных национальной системы прослеживаемости товаров и федерального реестра предполагаемых выгодоприобретателей. Наиболее значимыми выводами Счетная Палата РФ считает отсутствие работы по организации информирования налогоплательщиков о выявленных рисках неуплаты налогов и сборов, в отношении которых рассматривается вопрос о проведении ВМП [1. С. 9; 57–58].

Автор статьи считает, что отсутствие в открытом доступе методологии оценки налогоплательщиков, порядка формирования карт и реестров рисков в системе ИАС КБ делает применение системы контроля порочной практикой и не позволяет налогоплательщикам адекватно оценить свои риски до момента по-

буждения (а иногда и после него) и в добровольном порядке должным образом урегулировать свои налоговые проблемы.

Более того, полностью скрытая методология анализа деятельности как отдельно взятого налогоплательщика, там и возможной группы налогоплательщиков позволяет налоговому органу не только сокращать финансово-хозяйственную деятельность проверяемого, но и в ряде случаев ее полностью аннулировать путем банкротства организации налогоплательщика.

Все выше сказанное приводит к несбалансированному соотношению сторон в споре. Так, для анализа налогоплательщика налоговый орган иногда использует достаточно длительный промежуток времени. Камеральная налоговая проверка хоть и ограничена во времени, тем не менее составляет не менее 3 месяцев со дня предоставления декларации [4. С. 243–244]. При этом время на возражения налогоплательщика по доводам в актах камеральных проверок ограничены 30 днями [4. С. 272–275]. Получая акт камеральной налоговой проверки, налогоплательщик вообще не имеет возможности ознакомиться с материалами модулей ИАС КБ на которых, в том числе основаны претензии, а следовательно не может понять источник, и главное, опровергнуть те или иные выводы и доказательства проверяющих.

Так, автор столкнулся с Актами камеральных проверок и материалами побуждающих комиссий, в которых основаниями выводов налоговых органов были факты, имеющие место в текущем времени, но отсутствующие во время взаимодействия проверяемого лица и так называемого технического контрагента. Подобные доводы налогового органа были рассмотрены в судебных актах. Еще более удивительным случаем был акт камеральной проверки, датированный летом 2024 года, основанный на норме Налогового Кодекса без учета специфических оговорок и анализа специального соглашения, подписанного налогоплательщиком с руководством региона в рамках утвержденных полномочий. В судебных актах появляются формулировки и выводы, говорящие о наличии дополнительных оснований на основе аналитической работы налогового органа. Например, АС Западно-Сибирского округа напоминает, что «помимо указанных пунктом 2 статьи 105.1 НК РФ формально-юридических признаков взаимозависимости суду предоставлено право признать лица взаимозависимыми по иным основаниям» [6. С. 9]. Так же Постановление 12 Арбитражного апелляционного суда мы видим прямое указание на работу аналитической службы: «Как следует из материалов дела, по результатам предварительного изучения документов (сведений, информации) – справок, представленных ООО «СПФК» по форме 2-НДФЛ, сведений содержащихся в информационном ресурсе налогового органа...» Постановление 12 ААС от 17.05.2024 по делу №А57-29831/2023 [6. С. 11].

**Заключение.** Проведенный анализ временного порядка, практическая работа с налогоплательщиками в рамках урегулирования требований налоговых органов позволяет утверждать, что несовершенство существующего механизма взаимодействия в рамках реализации властных полномочий Федеральной налоговой службы, ограниченный порядок работы с информационными ресурсами и аналитическими данными, которые использует Федеральная налоговая служба при анализе работы налогоплательщиков, ставит стороны спора в неравные

условия, при которых, сильная сторона формирует «красивые» деревья связей, основываясь на неких данных, недоступных налогоплательщику ни для анализа своих рисков на досудебных стадиях, ни для защиты своих интересов в судебных инстанциях.

По результатам исследования представляются заслуживающими внимания следующие предложения:

- опубликование методики формирования реестра, паспорта и карты рисков налогоплательщика, используемой ИАС КБ;
- формализование такого мероприятия налогового контроля, как «побудительные» комиссии, формы актов таких мероприятий с указанием доказательной базы, положенной в основу претензий к налогоплательщику;
- гарантированное освобождение налогоплательщика от выездной налоговой проверки того периода, по которому произошло добровольное уточнение по результатам «побудительной» комиссии.

### Список литературы

1. Бюллетень счетной Палаты РФ № 2 (303) [Электронный ресурс]. – URL: <https://ach.gov.ru/upload/iblock/b6d/tc2qar8hzsay610v18epjftmwi9t68oh.pdf/>
2. Данные ФНС России [Электронный ресурс]. – URL: [https://www.nalog.gov.ru/rn15/news/activities\\_fts/14338045/](https://www.nalog.gov.ru/rn15/news/activities_fts/14338045/)
3. Министерство финансов Российской Федерации Федеральная налоговая служба / Письмо от 3 июня 2021 года № ЕА-4-15/7774 // ЭФ Правовых и информационно-технических документов [Электронный ресурс]. – URL: [https://docs.cntd.ru/document/603812543?fbclid=IwAR37U0zc3yeLLSdg8LXrFiMxYtsC8GiEKrqmFixMN7src\\_aOiYJXOYP6VqQ/](https://docs.cntd.ru/document/603812543?fbclid=IwAR37U0zc3yeLLSdg8LXrFiMxYtsC8GiEKrqmFixMN7src_aOiYJXOYP6VqQ/)
4. Налогового кодекса Российской Федерации Часть первая от 31 июля 1998 г. № 146-ФЗ // Система «Гарант» [Электронный ресурс]. – URL: <http://internet.garant.ru/>
5. Письмо Федеральной Налоговой Службы от 3 июня 2021 года № ЕА-4-15/7774 «О направлении временного порядка проведения риск-ориентированного камерального контроля с применением ИАС КБ и формы видов отчетов оценки эффективности отработки шаблонов схем и профилей рисков для использования в работе в рамках пилотного проекта» [Электронный ресурс]. – URL: <https://docs.cntd.ru/document/603812543?ysclid=m14y4tm2lw981338379/>
6. Постановление АС Западно-Сибирского округа в постановлении от 01.07.2024 А45-16859/2023 // Картотека арбитражных дел [Электронный ресурс]. – URL: <https://kad.arbitr.ru/Card/de869000-38da-4be1-9bd4-5f7fd0ae3d8a/>
7. Постановление 12 ААС от 17.05.2024 по делу № А57-29831/2023//Картотека арбитражных дел [Электронный ресурс]. – URL: <https://kad.arbitr.ru/Card/920e8a0c-4073-4e3b-a85a-176225644e01/>
8. Форма № 2-НК Утверждена приказом ФНС России от 11.07.2023 № ЕД-7-1/459@ «Отчет о результатах контрольной работы налоговых органов» [Электронный ресурс]. – URL: [https://www.nalog.gov.ru/rn77/related\\_activities/statistics\\_and\\_analytics/](https://www.nalog.gov.ru/rn77/related_activities/statistics_and_analytics/)

**Е. В. Боровикова,**

доктор экономических наук, доцент,

член Палаты налоговых консультантов,

Российская академия народного хозяйства и государственной службы при

Президенте Российской Федерации

## **ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ГОСУДАРСТВЕННОГО ФИНАНСОВОГО КОНТРОЛЯ**

**Аннотация.** Платформенные цифровые объекты созданы для решения важных задач государства. Финансовый контроль представляет собой одну из таких задач, и в настоящее время оперативность, качество и коммуникативные возможности в данной системе обеспечиваются за счет внедрения специальных сервисов, систем и баз данных. В работе рассмотрены отдельные методы анализа данных, аккумулируемых на платформенных ресурсах, проблемы выбора таких методов. Сформулированы предложения по интерпретации оценки результатов исполнения государственных программ, по внесению изменений в действующее законодательство в связи с переходом к информационным методам реализации государственных функций.

**Ключевые слова:** государственный финансовый контроль, бюджетный контроль, налоговый контроль, государственные информационные технологии, аналитика данных, цифровые системы контроля, государственные программы, государственные проекты, бюджетный процесс

## **DIGITAL TECHNOLOGIES IN THE SYSTEM OF STATE FINANCIAL CONTROL**

**Abstract.** Platform digital objects were created to solve important tasks of the state. Financial control is one of these tasks, and currently efficiency, quality and communication capabilities in this system are provided through the introduction of special services, systems and databases. The paper considers individual methods of analyzing data accumulated on platform resources, and the problems of choosing such methods. Proposals have been formulated on the interpretation of the evaluation of the results of the implementation of state programs, on amendments to the current legislation in connection with the transition to information methods for the implementation of state functions.

**Keywords:** state financial control, budget control, tax control, state information technologies, data analytics, digital control systems, state programs, state projects, budget process

**Введение.** Направлений изменения государственного финансового контроля несколько и одним из них является внедрение цифровых технологий, систем и платформ.

**Основная часть.** Применяемые в настоящее время системы включают: «Электронный бюджет», «Единая информационная система в сфере закупок»,

Информационно-аналитические системы Федерального казначейства Российской Федерации, сервисы ФНС (от онлайн сервисов до систем, предназначенных для проверки налогоплательщиков в дистанционном формате). Данный набор сервисов и систем описан также в трудах ряда исследователей: Костоусовой Ю. А. и Комаровой О. В. [1. С. 842–845], Захаровой Н. М. [2. С. 155–166], Болотновой Е.А. и Храменко А. А. [3. С. 306–310] и др. Каждая из систем позволяет осуществлять определенные функции, которые в настоящее время очень востребованы в государственном управлении и бизнес-среде (табл. 1).

Таблица 1

**Государственные цифровые платформы в системе финансового контроля**

| <b>Подвид государственного финансового контроля</b>                             | <b>Государственный орган</b>                          | <b>Информационная система / Цифровая платформа</b>                    |
|---------------------------------------------------------------------------------|-------------------------------------------------------|-----------------------------------------------------------------------|
| Бюджетный                                                                       | Минфин России (совместно с Федеральным казначейством) | «Электронный бюджет»                                                  |
| Бюджетный                                                                       | Федеральное казначейство                              | ГИС «Единая информационная система в сфере закупок»                   |
| Налоговый                                                                       | ФНС                                                   | АИС Налог-3, ФИАС, ПИК «Таможня», ПИК «Схемы», ПП «Контроль НДС», др. |
| Бюджетный, контроль эффективности управленческой функции (в т. ч., координации) | Счетная палата, Правительство Российской Федерации    | ГАС «Управление», «Электронный бюджет»                                |

Согласно экспертным оценкам, внедрение искусственного интеллекта позволит расширить возможности действующих информационных систем, позиционировать функции запросов в базы данных, сопоставления показателей запланированных бюджетов и их исполнения, проверки иных данных, оказывающих влияние на результаты использования бюджетных средств [4]. Однако, на наш взгляд, наиболее передовым направлением применения современных технологий будет аналитика на основе выгрузки данных, аккумулированных за ряд лет. Поскольку она служит не только задачам текущего контроля исполнения бюджетов, выполнения мероприятий государственных проектов и программ, но и оценке экономического развития, состояния той или иной сферы и даже выявления правонарушений в соответствующих сферах. В этом ключе наиболее востребованными становятся методы систематизации, обработки и анализа получаемых показателей, информации.

Анализ количественных данных о ходе и результатах использования бюджетных средств может строиться как на основе прикладных программ MS Office

(Excel) (наиболее доступных для применения в деловой среде), так и с помощью иных инструментов с элементами программирования, функционального и факторного анализа и т. д. Совокупность проблем, с которыми можно столкнуться при обработке и анализе данных, следующие:

- выгрузка объемных таблиц, с которыми сложно работать, иногда затруднен даже визуальный охват данных;
- получение неструктурированных массивов данных, последующая работа с которыми потребует, прежде всего, сортировки данных, отбора необходимых из них;
- получение неоднородных данных и данных, не отвечающих поставленной задаче;
- трудности в подборе необходимого аналитического и расчетного аппарата к показателям.

В случае применения достаточно простых, но многофункциональных пакетов Excel возможно построение масштабных таблиц, автоматизация их использования. За счет встроенных функций можно улучшить визуализацию представляемых данных. Эффективны такие внутренние функции приложения, как «Фильтр», «Сортировка», проведение расчетов в «Smart-таблицах», выборка данных или результатов расчета с помощью функции «Срез данных».

Формализация анализа (подбор методики, формул) определяется типом задачи, которую необходимо решить, используя массив данных о государственных доходах или расходах. Специфика массива данных определяется непосредственно спецификой управления средствами: многоуровневый характер их распределения, периодичность и этапность исполнения бюджета, видовое разнообразие доходов, программ, составляющих их мероприятий. Все это необходимо учитывать при проведении аналитических процедур в автоматизированном, цифровом или ручном режиме. Наиболее ценным становится анализ эффективности исполнения программ и распределения бюджетных средств в масштабах регионов и государства в целом. Здесь можно рассматривать самостоятельные направления анализа на региональном уровне, уровне муниципальных образований, отдельных программ и мероприятий. Также можно ввести ведомственную аналитику. Примечательно, что если для практики государственного управления такие направления анализа, в целом, ожидаемы, то на теоретическом уровне можно говорить об определенной новизне этих направлений и методов: например, региональная бюджетная аналитика с использованием моделей программирования, искусственного интеллекта. Очевидно, что достаточно высокий интерес будут представлять результаты анализа исполнения бюджетов и программ в субъектах Российской Федерации. Именно по этим результатам можно будет отнести регион к одному из типов с точки зрения эффективности достижения стратегических целей, результативности координационной работы по решению задач федерального центра.

Ценным для практики бюджетного процесса является и то, что получаемые выводы могут стать гораздо более достоверной основой для выработки прогнозов социально-экономического развития, проектов бюджетов на среднесрочную перспективу.

Бюджетный и налоговый контроль развиваются и в направлении основ их регулирования, практики бюджетного учета и отчетности, коммуникаций [5. С. 35–39; 6]. В доработке нуждается и правовая база, в которой в настоящее время не отражены цифровые основы государственного финансового контроля. В данном случае дадим комментарии и пояснения по наполнению бюджетного законодательства назревшими нормами. В частности, считаем целесообразным введение терминов «информационные системы в сфере государственного финансового контроля», «цифровая инфраструктура бюджетного процесса». Перечисленные термины могут найти отражение в ст. 6 Бюджетного кодекса Российской Федерации как понятия и далее в главе 9 упомянутого кодекса. Наполнение соответствующей терминологией федеральных законов (а не только подзаконных актов) позволит создать надежную общероссийскую базу правовых основ регулирования бюджетного процесса, столь важного для сбалансированного развития экономики и координации исполнения масштабных государственных задач. Также требуется согласование вносимых положений с содержанием Федерального закона от 27.07.2006 № 149-ФЗ, который является общим и не спроецирован на отраслевые особенности государственного управления.

Результаты анализа процессов регионального уровня могут быть положены в основу рейтингования территории получение информации о лучшей практике регионов. Когда речь идет о контроле координационных функций при исполнении национальных проектов и необходимости анализа данных, следует говорить о сочетании управленческих, аналитических и коммуникативных компетенций специалистов государственных органов (табл. 2).

Таблица 2

**Пример оценки результатов исполнения бюджетов и федеральной части государственных программ Российской Федерации\***

| <b>Тип бюджета<br/>(два критерия)</b>                                                  | <b>Наличие бюджетных<br/>правонарушений</b> | <b>Средний процент<br/>исполнения<br/>государственной<br/>программы</b> |
|----------------------------------------------------------------------------------------|---------------------------------------------|-------------------------------------------------------------------------|
| Дефицитный, получатель дотаций                                                         | Отсутствуют                                 | 95 %                                                                    |
| Основные данные по доходам                                                             |                                             | Снижение                                                                |
| Основные данные по расходам                                                            |                                             | Рост                                                                    |
| Количество мероприятий, по которым процент исполнения ниже среднего                    |                                             | 19                                                                      |
| Оценка эффективности координационной деятельности по программе по 10-балльной шкале    |                                             | 7                                                                       |
| Количество мероприятий программы с финансированием выше среднего и ниже 150 млн рублей |                                             | 24                                                                      |

| Тип бюджета<br>(два критерия)                                                                           | Наличие бюджетных<br>правонарушений | Средний процент<br>исполнения<br>государственной<br>программы |
|---------------------------------------------------------------------------------------------------------|-------------------------------------|---------------------------------------------------------------|
| Средняя фактическая стоимость реализации мероприятий                                                    |                                     | 15 млн рублей                                                 |
| Основные показатели и соотношения показателей, характеризующие результаты бюджетного процесса в регионе |                                     | Хорошее качество                                              |

*\* Разработано автором.*

Подчеркнем, что в каждом случае необходим подбор аналитического аппарата, если такие возможности не предусмотрены государственной информационной системой или платформой.

Весьма важными остаются вопросы оценки эффективности внутреннего аудита (контроля) в финансовой сфере [7. С. 87–91], частоты и типов правонарушений, причин их совершения, специфики последствий [8. С. 20–35]. Однако данные аспекты далеко не все возможно решить с помощью современных цифровых платформ и технологий, а также алгоритмов, доступных для применения. Возникает еще одна задача встраивания востребованных функций анализа в систему управления.

Заключение. Подчеркнем, что цифровые основы финансового контроля уже заложены, однако они в настоящее время способствуют решению далеко не всех задач. Большую работу следует регулярно проводить в целях подбора методов структурирования, анализа данных, построения прогнозов и получения выводов о результатах управления программами развития и бюджетными средствами. Значимость и объективность контроля в перспективе, безусловно, будет выше, если он будет дополнен общественной оценкой (общественный финансовый контроль), о котором ведется много дискуссий [9. С. 21–32; 10. С. 59–71].

### Список литературы

1. Костоусова Ю. А., Комарова О. В. Цифровизация государственного финансового контроля: институциональный анализ // Журнал экономической теории. – 2019. – Т. 16, № 4. – С. 842–848.
2. Захарова Н.М. Интегрированная информационная система управления общественными финансами «Электронный бюджет»: значение и тенденции развития // Экономика. Налоги. Право. – 2018. – № 2. – С. 155–166.
3. Болотнова Е.А., Храмченко А.А., Анопкин А.В., Никитина К.Р. Цифровизация государственного финансового контроля в Российской Федерации // Вестник Академии знаний. – 2021. – № 45(4). – С. 306–310.
4. Сбер и Минфин внедрят ИИ в бюджетный процесс. 06.06.2024. [Электронный ресурс]. – URL: <https://lenta.ru/news/2024/06/06/sber-i-minfin-vnedryat-ii-v-byudzhethnyy-protsess/?ysclid=m06rjmlaa675180089>

5. Боровикова Е. В. Методы анализа больших данных в интересах проведения налогового контроля // Евразийский Союз Ученых. Серия: экономические и юридические науки Ежемесячный научный журнал. – 2024. – № 03(118), Т. 1. – С. 35–39.
6. Груль Д. В. Анализ современных тенденций в сфере государственного финансового контроля в Российской Федерации // Вестник евразийской науки. – 2023. – № 1, Т. 15. [Электронный ресурс]. – URL: <https://esj.today/PDF/51FAVN123.pdf>
7. Баранова Ю. К. Государственный финансовый (бюджетный) контроль сегодня // Социально-экономические явления и процессы. – 2018. – № 1, Т. 13. – С. 87–91.
8. Лукашов А. И. Государственный финансовый контроль: современные вызовы и направления совершенствования // Вопросы государственного и муниципального управления. – 2023. – № 1. – С. 20–38.
9. Гончаров В. В., Петренко Е. Г., Поярков С. Ю., Борисова А. А. Общественный финансовый контроль в России: современные проблемы и пути совершенствования // Финансы и управление. – 2023. – № 4. – С. 21–32.
10. Кеворкова М. Э. Перспективные подходы к оценке эффективности деятельности органов государственного финансового контроля // Финансовый журнал. – 2024. – № 2. – С. 59–71.

**Е. В. Евсикова,**

кандидат юридических наук, доцент,  
Российский государственный университет правосудия  
(Крымский филиал)

**Т. А. Шкляр,**

кандидат юридических наук,  
Заместитель Председателя Верховного Суда Республики Крым,  
Российский государственный университет правосудия  
(Крымский филиал)

## **ЦИФРОВИЗАЦИЯ ПУБЛИЧНОГО ФИНАНСОВОГО КОНТРОЛЯ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ**

**Аннотация.** В статье раскрываются понятие, сущность, особенности и проблемы цифровизации публичного финансового контроля в современных условиях. Обращается внимание на основные проблемы и преимущества цифровизации правоотношений в сфере финансового контроля, исследуют перспективы дальнейшего развития цифрового финансового контроля в современных реалиях.

**Ключевые слова:** цифровая трансформация, финансовые правоотношения в сфере финансового контроля, публичный финансовый контроль, финансовый контроль, цифровизация, цифровые технологии, цифровая трансформация

## DIGITALIZATION OF PUBLIC FINANCIAL CONTROL: PROBLEMS AND PROSPECTS

**Abstract.** The article reveals the concept, essence, features and problems of digitalization of public financial control in modern conditions. The authors reveal the main problems and advantages of digitalization of legal relations in the field of financial control, explore and reveal the prospects for further development of digital financial control in modern realities.

**Keywords:** digital transformation, financial legal relations in the field of financial control, public financial control, digitalization, digital technologies, digital transformation

**Введение.** В современных реалиях вопросы реализации финансовых правоотношений в сфере финансового контроля с учетом преимуществ инновационных методов, подходов и инструментов, которые предоставляет повсеместная цифровая трансформация, остро стоят на повестке дня и требуют научных исследований и дискуссий, учета опыта правоприменительной практики, разработки и принятия соответствующих законодательных норм, закрепляющих механизм реализации правоотношений в сфере финансового контроля в условиях цифровой трансформации, которая меняет саму суть указанных правоотношений и соответствующей деятельности государства и государственного управления, трансформируя их в «цифровой публичный финансовый контроль» [1].

**Основная часть.** Глобальная цифровизация всех сфер и уровней жизни общества и государства влечет коренные процессы цифровой трансформации экономических, политических, правовых институтов и системы государственного управления в целом, поднимая на поверхность вопросы изменения самой диалектической сути такого управления, основывающегося на автоматизации всех процессов разработки, принятия, исполнения, контроля за соблюдением и исполнением властных управленческих решений, исходящих в условиях цифровизации не от реального человека, а от искусственного интеллекта (далее – ИИ), что породило острую проблему конкуренции живого разума и принятия им управленческих решений с учетом соблюдения базовых принципов правового государства и наделение ИИ функцией контроля, управления и принятия управленческих решений [2], естественно, такая ситуация породила массу дискуссий и вопросов, относительно возможности принятия ИИ управленческих решений, административного усмотрения, электронного правосудия, когда от решений ИИ будет зависеть судьба и жизнь человека, насколько сегодня наше общество и государство готово к такому повороту событий и насколько наша правовая система в целом и финансовая система сможет существовать и реализовывать свои функции с учетом соблюдения прав, свобод и законных интересов личности, общества, государства. Конечно, это – наше будущее, и нам сегодня важно понимать, как все будет складываться дальше и по какому вектору пойдет наше дальнейшее развитие с учетом глобальной цифровой трансформации явлений и процессов жизни, в том числе, и в условиях реализации правоотношений в сфере публично-го контроля.

В научной литературе вполне обосновано высказано мнение, что система управленческого контроля (MCS) является важнейшей областью цифровой революции, повышающей организационные возможности за счет предоставления информации, помогающей менеджерам выполнять свою работу, а также создавать и поддерживать продуктивные модели поведения. Следовательно, цифровизация систем управленческого контроля позволяет осуществлять сбор, обработку и анализ данных в режиме реального времени, что приводит к улучшению процесса принятия решений, ускорению реакции рынка и выявлению недостатков [3].

Следует согласиться с мнением, что сегодня контроль выступает не только функцией государственного управления, направленной на достижение поставленных целей и задач управления при минимальных затратах, а определенную систему более высшего порядка, осуществляющую наиболее значимые функции и операции, состоящую из таких подсистем, как налоговый контроль и бюджетный контроль [4], а также валютный, страховой, кредитно-денежный контроль, что в совокупности образует надсистему публичного финансового контроля, которая в условиях цифровой трансформации использует различные цифровые инструменты и платформы, что помогает минимизировать затраты и ресурсы, финансы, рабочую силу, время выполнения конкретных задач и операций, а также свести к минимуму погрешности и повысить точность, оперативность и объективность полученных данных и информации, ускорить все стадии процесса контроля, на которые раньше у проверяющего физического лица уходили дни и недели (те же самые процессы обработки и анализа информации ИИ делает за несколько минут и выводит на экран те блоки данных, где выявляет ошибки, расхождения, несоответствие указанных данных, риски нарушения финансового законодательства и т. д.).

В рамках данного исследования, можно утверждать, что сегодня возникает новое явление «публичный финансовый контроль в условиях цифровой трансформации» [1. С. 224–236], который представляет собой целый «организм», надсистему публичного финансового контроля в условиях цифровой трансформации, состоящую из ряда важных и взаимосвязанных элементов, каждый из которых представляет собой отдельную самостоятельную систему.

При этом одним из важнейших элементов надсистемы публичного финансового контроля в условиях цифровой трансформации является цифровой налоговый контроль, который является более совершенной формой привычного нам налогового контроля [5], а также публичный бюджетный контроль, что связано с активным внедрением технологий «цифрового бюджета», что, естественно, выдвигает на первый план вопросы усовершенствования всех административных и контрольных процедур в условиях цифровизации, их оптимизации и усовершенствования, повышение и усиление алгоритмов и механизмов защиты персональных данных и информации, аккаунтов, финансов и так далее от киберуязвимостей и кибератак, утечки персональных данных, нарушения прав, свобод и законных интересов всех участников цифровых финансовых правоотношений, противодействие использованию цифровых баз данных и цифровых платформ в преступных целях и отмыывании преступных доходов, а также повышения эффективности взаимодействия и согласованности различных информационных систем,

операторами которых выступают органы публичной власти, повышения квалификации и персональных навыков специалистов в сфере цифровых технологий, что позволит обеспечить более качественную и эффективную реализацию цифровых финансовых правоотношений, в том числе в сфере цифрового финансового контроля.

Таким образом, с учетом достижения «цифровой зрелости» и перехода к «цифровой экономике» цифровой финансовый контроль выступает серьезным инструментом защиты цифровых финансовых правоотношений и обеспечения эффективности их реализации, в том числе, облегчающим их осуществление путем различных цифровых финансовых инструментов, функционирования автоматизированных систем контроля, которые сразу выводят на экран и высвечивают все расходы, ошибки, возможные риски нарушения финансового законодательства, что очень удобно для контролирующих органов в части своевременного выявления и предупреждения финансовых правонарушений и преступлений.

Как видим, в современных реалиях цифровизация способствует дальнейшей трансформации и дифференциации финансовых правоотношений в сфере финансового контроля, значительно упрощая управленческую деятельность в сфере контроля [5].

На основе проведенного анализа, попробуем предположить, что финансовый контроль в условиях цифровой трансформации будет эффективно и динамично развиваться, облекаясь все больше и больше в цифровую форму и «обрасстая» современным цифровым инструментарием различного уровня и различной степени сложности, без которого современная система финансового контроля существовать и быть уже попросту не сможет, поскольку цифровая форма все больше будет «заглатывать» все элементы системы финансового контроля и заменит саму ее суть на цифровую, что видится, как неизбежный процесс развития финансового контроля, который требует продуманного научного подхода, изучения и анализа, с учетом правоприменительной практики и ее опыта, что должно лечь в основу надлежащего правового регулирования такой деятельности по осуществлению финансового контроля в условиях цифровизации путем разработки соответствующего законодательства и внесения изменений и дополнений в уже существующее, но оставляющего не за ИИ, а за человеком право принятия решений и возможность выбора и осуществления процессов и операций в сфере финансового контроля. Поэтому важным является исследование проблем внедрения технологий ИИ в конъюнктуру общественных отношений [6].

**Заключение.** Таким образом, технологизация и финансово-контрольная деятельность в современных условиях неразрывно связаны между собой и продолжают развиваться в качестве цифрового публичного финансового контроля, который, облекаясь в правовую форму, представляет более совершенную надсистему финансового контроля, состоящую из отдельных систем, взаимосвязанных между собой путем цифрового взаимодействия, единых операционных систем и баз данных, нацеленных на оперативное и эффективное выявление нарушений финансового законодательства и принятие качественных управленческих решений с учетом обеспечения базовых принципов правового государства и прав, свобод, законных интересов человека и гражданина.

### Список литературы

1. Евсикова Е. В. Публичный финансовый контроль в условиях цифровой трансформации (теоретико-правовой аспект) // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. – 2023. – Т. 9 (75), № 3. – С. 224–236.
2. Евсикова Е. В. Цифровизация производства по делам об административных правонарушениях: проблемы теории и практики // LegalTech: научные решения для профессиональной юридической деятельности: сборник докладов IX Московского юридического форума. В 4-х частях, Москва, 14–16 апреля 2022 года. Том Часть 2. – Москва: Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), 2022. – С. 50–52.
3. Steering digitalization and management control maturity in small and medium enterprises (SMEs) Laura Broccardo, Andrea Tenucci, Reeti Agarwal, Safiya Mukhtar Alshibani. Technological Forecasting and Social Change. July 2024. – № 204. – С. 123446.
4. Болотнова Е. А., Храмченко А. А., Анопкин А. В., Никитина К. Р. Цифровизация государственного финансового контроля в РФ // Вестник Академии знаний. – 2021. – № 45(4). – С. 306–310.
5. Цинделиани И. А., Гусева Т. А., Изотов А. В. Совершенствование налогового контроля в условиях цифровизации // Правоприменение. – 2022. – Т. 6, № 1. – С. 77–87.
6. Галлезе-Нобиле К. Регулирование умных роботов и искусственного интеллекта в Европейском союзе. Journal of Digital Technologies and Law. 2023;1(1):33-61. <https://doi.org/10.21202/jdtl.2023.2>. EDN: UNSONV

**Ж. М. Корзоватых,**

кандидат экономических наук, доцент,  
Государственный университет управления

### ЦИФРОВЫЕ ТЕХНОЛОГИИ ДЛЯ РЕШЕНИЯ ЗАДАЧ ESG-ПОВЕСТКИ

**Аннотация.** ESG-повестка представляет собой комплексную концепцию устойчивого развития, охватывающую три ключевых направления: Environment (Экологичность), Social (Социальная ответственность), Governance (Уровень корпоративного управления), которая в настоящий момент являются не только критерием определения ответственности за результаты деятельности, но и инструментом для построения долгосрочных стратегий развития бизнеса. Использование цифровых технологий для решения задач ESG-повестки является важным шагом на пути к устойчивому развитию. Они открывают безграничные возможности, способствуя повышению эффективности, оптимизации процессов и в конечном итоге обеспечивают конкурентоспособность экономических субъектов. Цифровые инструменты в данном контексте не просто отражают прогресс

ESG-трансформации, но и выступают катализатором этого процесса. Цель статьи заключается в исследовании применения цифровых технологий для решения задач ESG-повестки, внедряя принципы устойчивого развития в корпоративную культуру, делая их неотъемлемой частью деятельности экономического субъекта.

**Ключевые слова:** цифровые технологии, ESG-трансформация, нефинансовая отчетность, ESG-повестка, устойчивое развитие, социальная ответственность, экологическая ответственность

## DIGITAL TECHNOLOGIES FOR SOLVING THE TASKS OF THE ESG AGENDA

**Abstract.** The ESG agenda is a comprehensive concept of sustainable development, covering three key areas: Environment (Environmental friendliness), Social (Social responsibility), Governance (Corporate governance level), which at the moment are not only a criterion for determining responsibility for performance, but also a tool for building long-term business development strategies. The use of digital technologies to meet the challenges of the ESG agenda is an important step towards sustainable development. They open up limitless opportunities, contributing to efficiency improvement, process optimization and, ultimately, ensure the competitiveness of economic entities. Digital tools in this context not only reflect the progress of ESG transformation, but also act as a catalyst for this process. The purpose of the article is to study the use of digital technologies to solve the tasks of the ESG agenda, introducing the principles of sustainable development into corporate culture, making them an integral part of the activities of an economic entity.

**Keywords:** digital technologies, ESG transformation, non-financial reporting, ESG agenda, sustainable development, social responsibility, environmental responsibility

**Введение.** В современном мире, сталкивающимся с беспрецедентными вызовами внутренней и внешней среды, оказывающими непосредственное влияние на деятельность экономических субъектов, ESG-концепция приобретает все большее значение, позволяя компаниям не просто адаптироваться к вызовам современности, но и открывает путь для долгосрочных стратегий устойчивого развития бизнеса, ответственного и этического корпоративного управления. Интеграция ESG-принципов в деятельность экономических субъектов, акцентирует внимание на следующие составляющие:

- Environment (Экологичность). Этот аспект ESG фокусируется на минимизации негативного воздействия на окружающую среду. Компании, стремящиеся к экологической ответственности, внедряют меры по сокращению выбросов парниковых газов, препятствованию истощению природных ресурсов, оптимизации потребления ресурсов, управлению отходами, внедрению безотходных производств и экологически чистых технологий.

- Social (Социальная политика), проявляется в заботе о людях, являющихся частью бизнеса. Компании, ориентированные на ESG, внедряют практики безопасных условий труда, равноправия, доступа к образованию. Кроме

того, они стремятся к позитивному влиянию на местные сообщества, поддерживая инициативы по улучшению инфраструктуры, социальной интеграции и развитию.

– Governance (Уровень корпоративного управления). Данный аспект ESG подразумевает прозрачность и этичность в управлении компанией. Компании с высоким уровнем корпоративного управления демонстрируют информационную прозрачность в отчетности, внедряют механизмы контроля и предотвращения коррупции, обеспечивают независимость совета директоров, а также развивают культуру этичного поведения среди сотрудников.

**Основная часть.** «Сложившаяся геополитическая обстановка переориентировала российские компании от американских и европейских партнеров и западных инвесторов в сторону инвесторов из стран Персидского залива, Азиатско-Тихоокеанского региона и азиатских партнеров, но соблюдение ESG-повестки продолжается, так как и сами российские компании, и новые инвесторы, и контрагенты осознают преимущества трансграничного ESG-сотрудничества» [14. С. 302–309].

При этом невозможно выделить приоритетный критерий устойчивого развития, так как важна совокупность всех составляющих:

- экономической, позволяющей эффективно управлять имеющимися ресурсами, расширять инвестиции в инновации;
- социальной, направленной на обеспечение и сохранение безопасности в сфере охраны труда, поддержку образования, инвестирование социальных программ;
- управленческой, охватывающей разработку этических и прозрачных политик управления, деловую этику, корпоративную структуру, риск-менеджмент, недопущение коррупции и финансовых махинаций, повышение прозрачности, независимости и профессионализма [1. С. 22–23].

Однако ESG-трансформацию невозможно представить без развивающихся современных технологий, которые в последнее время становятся неотъемлемой частью любого бизнеса. Они открывают безграничные возможности, способствуя повышению эффективности, оптимизации процессов и, в итоге, обеспечивают конкурентоспособность экономических субъектов [7. С. 99–102]. Цифровые инструменты в данном контексте не просто отражают прогресс трансформации для решения задач ESG-повестки, но и выступают катализатором этого процесса.

Российские компании не в полной мере используют возможности цифровых технологий для решения задач в области ESG-повестки. Цифровые решения способны не только повысить производительность и эффективность бизнес-процессов, но и значительно ускорить переход к устойчивому развитию.

В области социальной ответственности («S»-компонента) цифровые технологии обеспечат реализацию решений по обеспечению безопасных условий труда для сотрудников.

Результаты исследования компании «Технологии доверия» также выявили приоритетные виды цифровых технологий для решения задач ESG-повестки, а именно: 29 % руководителей отдают предпочтение использованию искусствен-

ного интеллекта (ИИ), 23 % – интернету вещей (IoT), 14 % – технологии блокчейн и 10 % – роботизация [17].

Цифровых инструментов, которые могут быть внедрены для реализации концепции устойчивого развития, в настоящее время недостаточно. Согласно последним исследованиям, отмечается спрос на цифровые решения в сфере экологической ответственности:

- 16 % опрошенных экспертов признали нехватку цифровых инструментов при решении вопросов, связанных с климатическими изменениями. Цифровые платформы могут помочь в мониторинге выбросов парниковых газов, оптимизации энергопотребления, развитии возобновляемых источников энергии и планировании адаптации к изменению климата;

- 15 % экспертов отметили дефицит цифровых инструментов при решении проблем утилизации отходов и их переработки. Цифровые решения могут оптимизировать сбор и сортировку отходов, отслеживать их движение, внедрять системы замкнутого цикла и стимулировать вторичную переработку;

- 13 % опрошенных экспертов заявили о недостатке цифровых инструментов в сфере сохранения биоразнообразия. Снижение биоразнообразия угрожает стабильности экосистем и устойчивому развитию. Цифровые платформы могут помочь в мониторинге биоразнообразия, управлении особо охраняемыми природными территориями и разработке стратегий по сохранению исчезающих видов;

- 11 % экспертов отметили дефицит цифровых инструментов для борьбы с загрязнением окружающей среды. Загрязнение воздуха, воды и почвы представляет серьезную угрозу для здоровья человека и окружающей среды. Цифровые решения могут помочь в контроле выбросов загрязняющих веществ, мониторинге качества окружающей среды, разработке систем раннего предупреждения о загрязнении и внедрении технологий по очистке загрязненных территорий;

- 11 % экспертов подчеркнули недостаток цифровых инструментов в сфере ресурсосбережения. Рациональное использование природных ресурсов является ключевым фактором для устойчивого развития. Цифровые платформы могут помочь в оптимизации использования воды, энергии, материалов и других ресурсов, внедрении систем замкнутого цикла и разработке стратегий по снижению потребления [5].

Несмотря на растущий спрос на цифровые инструменты для решения задач ESG-повестки, рынок все еще находится в начальной стадии развития. Ключевые вызовы, стоящие перед разработчиками таких решений связан с нехваткой специалистов, обладающих необходимыми знаниями и опытом в области ESG-трансформации и цифровых технологий. Разработка и внедрение цифровых технологий для решения задач в области ESG требуют значительных инвестиций, которые далеко не всегда доступны, особенно для малых и средних предприятий. Интеграция цифровых решений в существующие системы управления и бизнес-процессы может быть сложной задачей, требующей изменения традиционного мышления и перехода к более сложным бизнес-моделям.

Важная роль в стимулировании развития цифровых инструментов для решения задач ESG-повестки должна отводиться государству. Необходимость разработки и реализации государственных программ, направленных на стимулиро-

вание инноваций в области ESG и цифровых технологий, в том числе предоставление финансовой поддержки, создание благоприятных условий для развития стартапов и малых предприятий, развитие инфраструктуры для цифровых решений должны стать приоритетными направлениями, реализуемыми государством.

Однако нельзя не затронуть и обратную сторону использования цифровых технологий для решения задач ESG-повестки. Это связано с использованием огромных вычислительных мощностей, оставляющих углеродный след, что негативно сказывается на раскрытии ESG-факторов в деятельности экономического субъекта. Также необходимо обратить внимание и на этические дилеммы, которые возникают при использовании цифровых технологий.

Основным инструментом информирования инвесторов, партнеров о результатах деятельности компании в рамках внедрения ESG-практик выступает нефинансовая отчетность компании. Нефинансовая отчетность является важным шагом к повышению информационной прозрачности и устойчивости бизнеса. Она позволяет компаниям не только демонстрировать свою финансовую эффективность, но и показывать свою ответственность перед обществом и окружающей средой. Один из видов нефинансовой отчетности – отчет о деятельности в области устойчивого развития дает детальный обзор подходов и результатов деятельности компании в области экологической и социальной ответственности и устойчивого развития. Он адресован широкому кругу заинтересованных сторон, включая инвесторов, потребителей, сотрудников, поставщиков, органы государственной власти и общественные организации. Другой вид нефинансовой отчетности – интегрированный отчет позволяет инвесторам оценить не только финансовую ситуацию компании, но и ее стратегическую ориентацию, устойчивость бизнес-модели, социальную ответственность, управление рисками и другие факторы, которые могут влиять на будущую ценность экономического субъекта.

Интегрированный отчет обращает внимание потенциальных инвесторов и стейкхолдеров на способность компании создавать стоимость в долгосрочной перспективе, путем разъяснений влияния ESG-факторов на бизнес-стратегию экономического субъекта посредством отражения информации о:

- профиле экономического субъекта, учете специфики его деятельности на результативные показатели, выявляя причинно-следственные зависимости и прогнозируя возможные отклонения финансовых показателей;
- результатах деятельности, для выявления отклонений в выполнении плановых показателей, определения направленности тренда для выявления влияния основных факторов и выявления резервов развития бизнес-стратегии компании;
- бизнес-стратегии, дающая возможность смоделировать перспективы развития в ближайшей перспективе и долгосрочном прогнозе, под влиянием скрытых, непрогнозируемых событий, отражающие изменения ключевых финансовых показателей;
- влиянии рисков и возможностей устойчивого развития на финансовые показатели деятельности экономического субъекта, способностью противостоять рискам и определять способы управления ими;

- социальных и корпоративных составляющих, характеризующих кадровый потенциал экономического субъекта, обеспечение необходимых условий труда, защиту прав работников, стиль управления;
- экологической деятельности, позволяющей определить уровень расходов на мероприятия, связанные с экологической безопасностью, ресурсосбережением, снижением углеродного следа, управления отходами, сохранения биоразнообразия, возможных рисках возникновения дополнительных затрат на устранение экстренных ситуаций и восстановление окружающей среды;
- особенностях постановки системы бухгалтерского и управленческого учета в компании, обоснованности и правильности применения нормативного регулирования бухгалтерского учета, позволяющих привести данные учетно-аналитического обеспечения к реальным значениям;
- конкурентоспособности экономического субъекта, положении на рынке, что позволяет выявить факторы, влияющие оценку компании, спрогнозировать ее способность расти и развиваться в течение определенного периода времени.
- других специфических направлениях деятельности экономического субъекта [8. С. 26–32].

Развитие нормативно-правовой базы формирования нефинансовой отчетности в России начинается с 2017 года с последовательным принятием Концепции развития публичной нефинансовой отчетности и плана мероприятий по ее реализации [10]. Для широкомасштабной реализации ESG-повестки в России были разработаны и введены в действие следующие документы: Федеральные законы [15; 16], распоряжения Правительства [11; 12; 13], Письма Банка России [2; 3; 4], Приказ Минэкономразвития [9].

Наличие действующих нормативных актов в области устойчивого развития и их исполнении свидетельствует о сложностях в их реализации и не проработанности законодательной базы по многим ключевым вопросам. На сегодняшний день назрел вопрос о выведении отчетности, отражающей нефинансовую информацию о деятельности экономических субъектов в правовое поле. Носящие рекомендательный характер требования по составу, содержанию и раскрытию нефинансовой аналитики в отчетности о деятельности компаний приводит к затруднению трактовок и интерпретаций данных, предоставленных экономическими субъектами, сложностям в проведении сравнительного анализа по кастомизированным показателям, оценке достигнутых результатов по ESG-факторам. Данные вопросы могут быть сняты с повестки дня при формировании четко проработанной нормативно-законодательной базы в области устойчивого развития, обеспечив заинтересованных пользователей и стейкхолдеров прозрачной, надежной и достоверной информацией по реализации ESG-инициатив [6. С. 51–55].

Не проработанность нормативно-законодательной базы по формированию нефинансовой отчетности связана с проблемами, которые могут нести негативные последствия:

- сложность объективной оценки ESG-рисков и перспектив развития в области устойчивого развития затрудняет принятие инвестиционных решений;

- отсутствие прозрачности в вопросах раскрытия ESG-факторов вызывает недоверие со стороны потребителей, стейкхолдеров и общественности;
- неэффективное использование ресурсов в связи с отсутствием четких ESG-ориентиров;
- снижение конкурентных преимуществ в долгосрочной перспективе для компаний, которые не раскрывают информацию о ESG-факторах и их влиянии на свою деятельность;
- повышение рисков и вероятности наступления негативных последствий вследствие невозможности оценить влияние деятельности компании на общество и окружающую среду;
- увеличение разрыва в развитии между компаниями, которые формируют нефинансовую отчетность, и теми, кто это игнорирует.

**Заключение.** Внедрение цифровых технологий при решении задач ESG-трансформации имеет ряд преимуществ, связанных с повышением информационной прозрачности и эффективности процессов управления ресурсами и производственными цепочками, снижением рисков и увеличением возможностей развития. И несмотря на барьеры, стоящие на пути к цифровой ESG-трансформации, инновационные инструменты для решения задач ESG-повестки становятся ключевым аспектом развития компаний. Органы власти не должны оставаться в стороне при решении данных задач. Поддержка и поощрение компаний к внедрению ESG-принципов с использованием цифровых технологий со стороны государства может осуществляться путем создания специальных программ для развития и распространения инноваций в этой области, введением налоговых льгот и других финансовых инструментов. Именно консолидация усилий бизнеса, государства и общественности в разработке и внедрении цифровых решений для ESG-трансформации является фактором к успеху этого процесса. Внедрение ESG-практик не только способствует устойчивому развитию России, но и является ключом к успеху российских компаний на глобальном рынке.

### Список литературы

1. Анюшенкова, О. Н. Environmental, Social, Governance (ESG) и бизнес: современные тенденции и вызовы / О. Н. Анюшенкова, В. Х. Мкртчян // Самоуправление. – 2023. – № 6(139). – С. 22–23.
2. Информационное письмо Банка России от 12.07.2021 № ИН-06-28/49 «О рекомендациях по раскрытию публичными акционерными обществами нефинансовой информации, связанной с деятельностью таких обществ» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: <http://www.consultant.ru>
3. Информационное письмо Банка России от 15.07.2020 № ИН-06-28/111 «О рекомендациях по реализации принципов ответственного инвестирования» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: <http://www.consultant.ru>
4. Информационное письмо Банка России от 16.12.2021 № ИН-06-28/96 «О рекомендациях по учету советом директоров публичного акционерного общества ESG-факторов, а также вопросов устойчивого развития» (вместе с «Рекомендациями по учету советом директоров (наблюдательным советом) публично-

го акционерного общества факторов, связанных с окружающей средой, социальных факторов и факторов корпоративного управления (ESG-факторов), а также вопросов устойчивого развития») // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: <http://www.consultant.ru>

5. Как цифровизация помогает ESG-трансформации бизнеса // [Электронный ресурс]. – URL: <https://trends.rbc.ru/trends/green/63512ca29a79477492c63be0>

6. Корзоватых Ж. М. Нефинансовая отчетность как инструмент повышения эффективности бизнеса // Актуальные проблемы финансового менеджмента, бухгалтерского учета, анализа, контроля и налогообложения в нефтегазовом комплексе: Межвузовский сборник научных трудов и результатов совместных научно-исследовательских проектов, представленных на 8-й национальной научно-практической конференции, Москва, 15 марта 2023 года. – Москва: Общество с ограниченной ответственностью «Русайнс», 2023. – С. 51–55.

7. Корзоватых Ж. М. Искусственный интеллект в условиях цифровой экономики: угрозы и перспективы развития / Ж. М. Корзоватых, В. Г. Бардина // Львовские чтения – 2020: Сборник статей VIII Всероссийской научной конференции. К 90-летию академика РАН Д.С. Львова, Москва, 18 июня 2020 года / Под научной редакцией Г.Б. Клейнера. – Москва: Государственный университет управления, 2021. – С. 99102.

8. Одинцова Т. М. Проблемы и перспективы применения интегрированной отчетности для российских экономических субъектов / Т. М. Одинцова, А. А. Красноручкая, А. С. Алиева // Вестник экономики и менеджмента. – 2023. – № 1. – С. 26–32.

9. Приказ Минэкономразвития России от 01.11.2023 № 764 «Об утверждении методических рекомендаций по подготовке отчетности об устойчивом развитии» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: <http://www.consultant.ru>

7. Распоряжение Правительства РФ от 05.05.2017 № 876-р «Об утверждении Концепции развития публичной нефинансовой отчетности и плана мероприятий по ее реализации» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: <http://www.consultant.ru>

8. Распоряжение Правительства РФ от 14.07.2021 № 1912-р (ред. от 30.12.2023) «Об утверждении целей и основных направлений устойчивого (в том числе зеленого) развития Российской Федерации» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: <http://www.consultant.ru>

9. Распоряжение Правительства РФ от 22.10.2021 № 2979-р «Об утверждении перечня парниковых газов, в отношении которых осуществляется государственный учет выбросов парниковых газов и ведение кадастра парниковых газов» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: <http://www.consultant.ru>

10. Распоряжение Правительства РФ от 29.10.2021 № 3052-р «Об утверждении стратегии социально-экономического развития Российской Федерации с низким уровнем выбросов парниковых газов до 2050 года» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: <http://www.consultant.ru>

11. Третьякова, Е. А. ESG-трансформация в России: особенности современного этапа / Е. А. Третьякова // Менеджмент в современном обществе: технологии будущего и наставничество : материалы XXII Международной научно-практической конференции, Орел, 24–25 октября 2023 года. – Орел: Орловский государственный университет имени И.С. Тургенева, 2024. – С. 302–309.

12. Федеральный закон от 02.07.2021 № 296-ФЗ «Об ограничении выбросов парниковых газов» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: <http://www.consultant.ru>

13. Федеральный закон от 06.03.2022 № 34-ФЗ «О проведении эксперимента по ограничению выбросов парниковых газов в отдельных субъектах Российской Федерации» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: <http://www.consultant.ru>

14. Цифровые решения для ESG-трансформации. // [Электронный ресурс]. – URL: <https://journal.ecostandard.ru/esg/keysy/tsifrovye-resheniya-dlya-esg-transformatsii/>

**Д. В. Кривин,**

магистр экономических наук,  
экономист по бухгалтерскому учету и анализу  
хозяйственной деятельности ООО «КСК»

## **ИСПОЛЬЗОВАНИЕ ИТ-ТЕХНОЛОГИЙ В ЦЕЛЯХ ПРАВОМЕРНОГО ВОЗМЕЩЕНИЯ НДС**

**Аннотация.** В статье рассматривается возмещение НДС как разновидность налогового вычета. Основополагающую роль в данном процессе играет автоматизированная система контроля налога на добавленную стоимость (далее по тексту – АСК НДС), которая постоянно обновляется и совершенствуется. Анализируется работа и применение «СУР АСК НДС-2» для оценки налогоплательщика, определения налоговых рисков и доказательства недобросовестности налогоплательщиков. Отмечается проблема отсутствия правового регулирования в части использования информационных технологий в налоговой сфере в целом и возмещения НДС в частности. Делается вывод о необходимости принятия нормативного правового акта в данном аспекте, об отражении в нем порядка взаимодействия налоговых органов с банковскими структурами для выявления рисков, их снижения в совершении крупных сделок и порядка доступа к информации об имуществе участников сделки. Данная статья будет полезна представителям налоговых органов, а также студентам экономических и юридических специальностей в изучении проблем налогообложения.

**Ключевые слова:** налоговый вычет, налоговый риск, бухгалтерский учет, АСК НДС-2, мошеннические действия, налоговое правонарушение, налоговые льготы, выгодоприобретатель, предпринимательская деятельность налоговый мониторинг

## IT USING FOR THE PURPOSES OF LEGAL VAT REFUND

**Abstract.** The article considers VAT refund as a type of tax deduction. The fundamental role in this process is played by the automated value added tax control system (hereinafter referred to as the VAT Control System), which is constantly being updated and improved. The article analyzes the working procedure and application of the "SUR ASK VAT-2" for assessing the taxpayer, determining tax risks and proving the taxpayers' dishonesty. The problem of the lack of legal regulation regarding the information using technologies in the tax sphere in general and VAT refund in particular is noted. It is concluded that it is necessary to adopt a law in this aspect, to reflect in it the order of interaction between tax authorities and banking structures in order to identify risks, reduce them in making large transactions and the order of access to information about the participants' property in the transaction. This article will be useful to representatives of the tax authorities of our state, as well as students of economic and legal specialties in the study of taxation problems.

**Keywords:** tax deduction, tax risk, financial accounting, ASK VAT-2, fraudulent actions, tax violation, tax benefits, beneficiary, entrepreneurial activity, tax monitoring

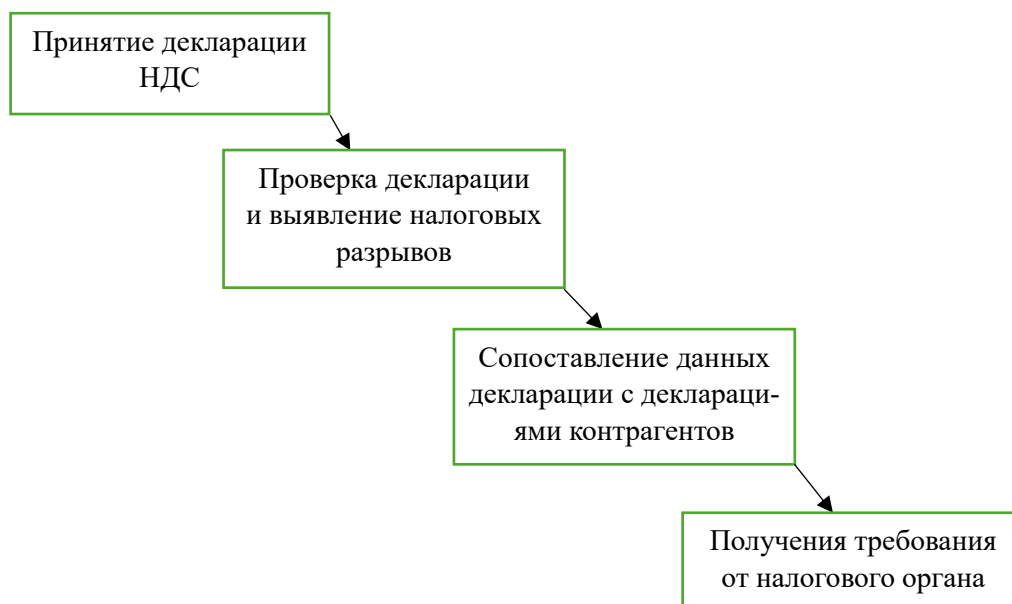
**Введение.** После начала пандемии COVID-19 в 2020 году стартовал процесс активного внедрения в жизнедеятельность общества цифровых технологий, что стало оказывать несомненное влияние на изменение отечественного законодательства. Цифровизация коснулась каждой сферы права, в частности и налогового, начиная с упрощенного порядка получения вычета из НДС на покупку жилья и заканчивая налоговыми льготами для бизнеса. В настоящей статье речь пойдет о возмещении НДС, который является одним из главных налогов в деятельности каждого хозяйствующего субъекта.

**Основная часть.** Налоговый агент, который выбрал общую систему налогообложения, обладает правом на определенные налоговые льготы. Одной из таких льгот является возмещение НДС. Налоговый кодекс РФ (далее – НК РФ) в статье 173 определяет возмещение НДС как «положительную разницу между суммой налоговых вычетов и суммой налога, исчисленной по операциям, признаваемым объектом налогообложения» [1]. Следует также отметить, что право на возмещения НДС для налогового агента имеет срок давности – три года после окончания соответствующего налогового периода с момента образования возможности для такого возмещения.

Экономико-правовая природа НДС такова, что это не налог, который облагает добавленную стоимость и является ее изъятием, а налог, который уплачивает конечный выгодоприобретатель за реализованный им продукт пропорционально цене. В зарубежной практике данный аспект именуется принципом нейтральности НДС [12. С. 40]. Европейский суд обращается к экономическому анализу международной модели НДС, как налога на потребление. Суд ЕС в решении от 18 ноября 2021 года по делу C-358/20 [3] отметил, что при подаче на возмещение НДС важно соблюдение материально-правовых условий. Если не были соблюдены формальные требования законодательства, содержащие, в част-

ности, требования о регистрации для целей НДС, это не может быть основанием для отказа в возмещении налога со стороны соответствующих органов.

Федеральная налоговая служба с 2013 года разработала для сотрудников налоговых органов и начала применять АСК НДС – инструмент контроля за неправомерным возмещением НДС. АСК НДС является компонентом автоматизированной информационной системы «ПП Контроль НДС». Всего через два года вышла более усовершенствованная версия продукта – АСК НДС 2. Данная программа позволяет выявлять расхождения по налогоплательщикам в части учета НДС в рамках принятых к бухгалтерскому (финансовому) учету счетов-фактур. Следует отметить, что такая система оснащена специальной «надстройкой» под названием «СУР АСК НДС-2». Порядок ее работы от принятия декларации НДС до получения требования от налогового органа представлен на рисунке ниже.



### Порядок работы СУР АСК НДС-2

В письме ФНС России от 03.06.2016 № ЕД-4-15/9933@ «Об оценке признаков риска СУР» [2] содержится определение налогоплательщиков высоким и низким налоговым рисками, а средний риск определен по остаточному принципу – с целью недопущения неопределенности в работе с налогоплательщиками в части возмещения НДС. Таким образом, каждый налоговый агент, исходя из наличия тех или иных признаков, будет относиться к определенной группе налогового риска.

В отечественной практике анализ автоматизированной системы контроля НДС-2 используется в качестве обоснования фиктивного документооборота, когда данный информационный ресурс служит доказательством недобросовестности налогоплательщиков. Очевидно, в данном случае проблема в том, что правовая база отстает от темпов цифровизации в сфере налогового администрирова-

ния. А одним из условий эффективного функционирования налоговой системы является требование рациональной организации механизма налогового администрирования, о чем отмечалось в предыдущих исследованиях автора. Налоговое администрирование включает в себя процедуры налогового учета и контроля, процедуру реализации прав и обязанностей налогоплательщиков, порядок вменения и реализации ответственности за совершение налоговых правонарушений, а также порядок обжалования актов и действий налоговых администраций [7. С. 122]. На наш взгляд, АСК НДС-2 – это одна из систем, которая дает наиболее четкий и быстрый способ проверки налогоплательщика на предмет уплаты НДС и позволяет своевременно реагировать даже на попытки налогового агента совершить неправомерное возмещение данного налога.

Как мы видим, перечень закрыт, но, на наш взгляд, подобные случаи злоупотребления данным правом гораздо шире и разнообразнее. В качестве примера такого случая можно привести фактор мошеннических действий, рассмотренных в более ранних исследованиях автора. Причем спектр действий, обуславливающих риск мошенничества, очень широк: от прямого хищения активов до разнообразных манипуляций с показателями всех форм отчетности [13. С. 48] и отдельных документов бухгалтерского учета.

Особенно часто такие схемы встречаются в предприятиях строительной сферы, связано это прежде всего с ее особенностями, такими как выполнение работ, оказание услуг генерального подрядчика. Основная проблема состоит в определении конечного выгодоприобретателя, потому как работы очень часто передаются на субподряд, вследствие чего может быть неограниченное количество продавцов-посредников. АСК-НДС 2 довольно успешно решает данную задачу путем встроенного компонента «Дерево связей», что позволяет взыскать НДС по каждой операции в рамках такой цепочки.

Следует заметить, что налоговый учет неразрывно связан с бухгалтерским (финансовым) учетом и его автоматизацией в организациях. Именно счет-фактура является документом, служащим основанием для принятия покупателем предъявленных продавцом сумм НДС к вычету. Некоторые авторы отмечают положительные аспекты в части перехода на электронные счета-фактуры по НДС, что снижает уход от налогообложения и повышает «эффективность налоговых проверок наряду с сокращением их количества, а также уменьшить число подставных компаний и возможности использования схем теневого администрирования в налогообложении» [5. С. 19]. В результате внедрения системы «СУР АСК НДС-2» появился термин «налоговый разрыв» – ситуация, при которой на определенной стадии обращения товара (работ или услуг) счет-фактура не встречается с последующим, что является сигналом о возможном наличии в цепочки фирмы-«однодневки» [6. С. 15]. Таким образом, цифровизация – это один из факторов, который может сдерживать риск мошеннических действий в организации, сразу выявить разрывы в цепочках контрагентов и снизить доли расхождения в НДС. Благодаря этому увеличиваются поступления НДС в бюджет, которые мы можем видеть в представленной ниже таблице.

**Динамика поступлений по НДС на товары, работы, услуги, реализуемые на территории Российской Федерации в 2020–2023 гг., млрд рублей**

| Показатель      | 2020      | 2021      | 2022      | 2023      |
|-----------------|-----------|-----------|-----------|-----------|
| Поступления     | 4 320,3   | 5 788,7   | 6 888,6   | 7 653,2   |
| Темп роста, %   | х         | 134,0     | 119,0     | 111,1     |
| Номинальный ВВП | 107 658,1 | 135 773,8 | 155 188,9 | 172 148,3 |
| Темп роста, %   | х         | 126,1     | 114,3     | 109,3     |

Из таблицы также можно увидеть, что темпы роста поступлений по НДС на товары, работы, услуги, реализуемые на территории Российской Федерации, превышают темпы роста номинального ВВП. Исходя из этого можно сделать вывод о повышении качества налогового администрирования за счет внедрения АСК НДС-2.

Но существуют и негативные факторы влияния цифровых технологий на процесс возмещения НДС, когда не анализируется информация, содержащаяся в информационном ресурсе, а просто прикладываются фотографии из базы данных. Широкое применение искусственного интеллекта, по мнению Д. М. Челнокова, «ведет к снижению эффективности профессионального уровня сотрудников, которые воспринимают информационные системы как источник готовых ответов, что негативно сказывается на качестве оценки налоговых правонарушений» [11. С. 31]. Конечно, остается множество способов уйти от налогообложения даже после внедрения и активного использования АСК НДС-2, и каждый из них заслуживает отдельного внимания.

Одним из способов по уходу от НДС является занижение выгодоприобретателем налоговой базы, когда создается оборот с одним или несколькими юридическими лицами, которые управляются из единого центра. В профессиональной среде получил распространение термин «бумажный НДС» [8. С. 46], когда в результате подобных действий происходит уклонение от уплаты налога путем подачи заведомо ложных сведений, основанных на формировании искусственного документооборота для исчисления уплаты НДС. В отечественной практике принимаются попытки решить проблему низкой налоговой дисциплины и незаконного использования налоговых вычетов в части возмещения НДС. Директор ООО «Буровые и нефтепромысловые насосы» г. Казани Т. Г. Давлетшин предлагает для малого и среднего бизнеса взимать местный бюджет НДС онлайн в режиме реального времени по оплате с оборота по расчетной ставке, которая варьируется в зависимости от группы товаров [4. С. 38]. Таким образом, необходимо проводить качественную работу с налогоплательщиками, побуждая их добровольно уплатить налог.

Также нужно привести в порядок законодательство о налогах и сборах, издав специальный нормативный правовой акт об информационных системах в сфере налогообложения. При создании законопроектов необходимо опираться на

прогноз последствий, сопоставляя доходы и расходы субъектов предпринимательской деятельности и учитывая возможные риски. Так как налоговая сфера пронизывает как экономическую, так и юридическую составляющую, то законодательные акты должны быть основаны на так называемом критерии экономической эффективности. Он в себя должен включать экономическую обоснованность (экономический аспект) и фактические обстоятельства дела (юридический аспект), потому что именно от них зависит конечный результат принятия закона и его вступления в силу. Законодательная инициатива должна исходить именно от государства, потому что, во-первых, не все субъекты федерации обладают достаточной технической оснащенностью, а во вторых, арбитражные суды просто забиты делами о недоброкачественной работе налоговых инспекторов, так как не существует определенной системы критериев оценки работы инспектора налоговой службы [9. С. 81]. Следствием этого является недоверие субъектов предпринимательской деятельности к налоговым органам, которые зачастую могут выносить решения не в пользу предпринимателей как в части расчета налогов и их последующей уплаты, так и собственно налогового мониторинга.

Для проведения налогового мониторинга необходимо учитывать особенности отдельной сферы деятельности с учетом изменений законодательства. Действующие нормы налогового законодательства, по справедливому замечанию А. В. Тихоновой, применяются «либо исходя из их буквального прочтения, либо не применяются вообще ввиду правовой неопределенности» [10. С. 27]. Правовое регулирование использования информационных технологий в части возмещения НДС в настоящее время отсутствует. Однако предпосылки, для того чтобы урегулировать данный процесс, были предприняты заместителем руководителя Федеральной налоговой службы Д. Е. Егоровым путем издания письма об оценке признаков риска СУР. Пункт 3.1.2 письма содержит отсылку, что, если уровень риска «СУР АСК НДС-2» не соответствует уровню риска «АСК НДС», для оценки налогоплательщика необходимо использовать уровень риска «СУР АСК НДС-2». Одной императивной нормы для урегулирования такого актуального явления, как возмещение НДС, на наш взгляд, недостаточно, чтобы в дальнейшем не создавать неправомерных действий в данном аспекте.

Таким образом, необходимость принятия закона об использовании информационных технологий в налоговой сфере, в нашем случае в части возмещения НДС, становится потребностью. На сегодняшний день уже активно практикуется так называемая «убийца» налоговых схем АСК НДС-3, введенная в эксплуатацию 1 февраля 2018 года. АСК НДС-3 может не только максимально быстро выявить нарушения в уплате налогов и их возмещении, но и выявить субъекты теневого рынка, которые и вовсе уклоняются от уплаты налогов. При этом сокращается время на налоговые проверки, так как все сведения о налогоплательщике собираются АСК НДС-3 автоматически. В частности, формируются сведения разделов 8-12 налоговой декларации по НДС по требованию налогового органа и контрагентов налогоплательщика. Благодаря автоматизации и использованию современных информационных технологий, налоговые органы могут более эффективно бороться с неправомерным возмещением НДС в частности и его последу-

ющей уплате в целом. Этот момент способствует увеличению поступлений в бюджет по НДС и выявить частоту расхождений по декларациям по налогу.

В новом нормативном правовом акте также будет необходимо, на наш взгляд, отразить порядок взаимодействия налоговых органов с банковскими структурами, который будет включать в себя процедуру взаимодействия в части передачи и электронной обработки сведений об остатках, суммах, датах открытия, назначении расчетных счетов юридических лиц. Также необходимо обозначить процедуру предоставления доступа к расчетному счету учредителей – физических лиц, направления денежных потоков и условий платежа. Помимо этого, с 2018 года база ЗАГС также передается в ведение налоговой системы с целью вычисления связей физических лиц по признакам родства, что, на наш взгляд, усилило возможности АСК НДС-3.

Но для того, чтобы предложения воплотились в реальность, необходимо провести грамотную и последовательную законодательную работу. Конечно, следует ожидать того, что при более детальных налоговых проверках под последние попадут организации строительного, фармацевтического и алкогольного сектора. Именно в них, как показывает практика, больше всего разнообразных схем ухода от налогообложения, а использование отраслевого подхода повышает прозрачность и законность ведения бизнеса в нашем государстве. Решить данную проблему, на наш взгляд, можно путем проведения экстерриториальных проверок, когда, например, налоговые инспекторы находятся в одном населенном пункте, а организация в другом либо же если в другом субъекте находится филиал или представительство организации.

**Заключение.** Таким образом, цифровая трансформация налоговой системы – это платформа для совершенствования законодательства и его адаптация под современный уклад жизни общества и ведения предпринимательской деятельности, что позволяет уменьшить административные проблемы для бизнеса и повысить его прозрачность. Приносимые трансформацией новшества смогут способствовать борьбе с налоговыми злоупотреблениями и уклонением от уплаты налогов, вследствие чего поступление доходов в государственный бюджет повысится. В дальнейшем это поможет стимулировать развитие налоговой политики российского государства.

### Список литературы

1. Налоговый кодекс Российской Федерации (часть вторая) от 05.08.2000 №117-ФЗ (ред. от 08.08.2024 № 294-ФЗ) // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_28165/](https://www.consultant.ru/document/cons_doc_LAW_28165/)
2. Об оценке признаков риска СУР: Письмо ФНС России от 03.06.2016 № ЕД-4-15/9933@ // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_199628/96c60c11ee5b73882df84a7de3c4fb18f1a01961/](https://www.consultant.ru/document/cons_doc_LAW_199628/96c60c11ee5b73882df84a7de3c4fb18f1a01961/)
3. Решение Суда ЕС от 18.11.2021 по делу C-358/20. – URL: <https://nalogoved.ru/resheniya-suda-es/9909.html?ysclid=Izte69q6y7327019786>

4. Давлетшин Т. Г. Реформирование системы налогов: от специальных налоговых режимов к общей системе налогообложения // Бухгалтерский учет в бюджетных и некоммерческих организациях. – 2023. – № 8. – С. 26–41.
5. Евневич М. А., Иванова Д. В. Исследование реформ налогового управления в российской практике // Бухгалтерский учет в бюджетных и некоммерческих организациях. – 2023. – № 3. – С. 7–20.
6. Жутаев А. С. Налоговый контроль за операциями по налогу на добавленную стоимость в эпоху цифровизации // Налоги. – 2024. – № 1. – С. 14–16.
7. Кривин Д. В. Налог на профессиональный доход в предпринимательской деятельности: проблемы и перспективы эксперимента в науке и практике // Известия высших учебных заведений. Поволжский регион. Общественные науки. – 2020. – № 3. – С. 113–126.
8. Лошкарев В. В. От незаконного обналичивания к «бумажному НДС» // Законность. – 2021. – № 1. – С. 45–47.
9. Магальяс А. В., Сорокина Н. С. Налоговый контроль в условиях развития информационных технологий // Ползуновский альманах. – 2024. – № 2. – С. 80–82.
10. Тихонова, А. В. Становление российской практики налогового регулирования технологий Индустрии 4.0 // Налоги. – 2020. – № 4. – С. 23–27.
11. Челноков Д. М. Провалы неопределенности в правовом регулировании налогового контроля в условиях применения искусственного интеллекта // Налоги. – 2024. – № 2. – С. 28–32.
12. Шелкунов А. Д. Экономический анализ и толкование норм налогового права об НДС // Закон. – 2022. – № 5. – С. 37–42.
13. Krivin D. V., Meleshenko S. S., Usanova D. Sh. Internal Fraud as a Threat to the Liquidity of a Commercial Organization // International Journal on Emerging Technologies. – 2019. – № 10(2a). – Pp. 47–51.

**Н. В. Куркина,**  
преподаватель,

Волгоградский институт управления – филиал Российской академии  
народного хозяйства и государственной службы при Президенте Российской Фе-  
дерации

### **ИНДИВИДУАЛЬНЫЙ ИНВЕСТИЦИОННЫЙ ВЫЧЕТ ПРИ ИСЧИСЛЕНИИ НАЛОГА НА ДОХОДЫ ФИЗИЧЕСКИХ ЛИЦ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

**Аннотация.** В статье рассматривается механизм предоставления налоговых вычетов на налог на доход физических лиц в связи с пополнением индивидуального инвестиционного счета, а также налоговые вычеты по получению прибыли в результате финансовых операций по индивидуальному инвестиционному счету. Делается вывод о том, что гибкая система налоговых льгот, а также простота их оформления, в основе которой лежит цифровой информационный обмен между налоговыми органами и финансовыми организациями, является

одним из стимулов налоговых резидентов России при открытии индивидуального инвестиционного счета, что способствует притоку частных инвестиций в российскую экономику.

**Ключевые слова:** налоговое администрирование, налоговые льготы, цифровизация налогообложения, индивидуальный инвестиционный счет, налоговый вычет

## INDIVIDUAL INVESTMENT DEDUCTION WHEN CALCULATING INCOME TAX FOR INDIVIDUALS IN THE CONDITIONS OF DIGITIZATION

**Abstract.** The article discusses the mechanism for providing tax deductions for personal income tax in connection with replenishing an individual investment account, as well as tax deductions for receiving profit as a result of financial transactions on an individual investment account. It is concluded that the flexible system of tax benefits, as well as the simplicity of their registration, which is based on digital information exchange between tax authorities and financial organizations, makes this form of investment attractive for tax residents of Russia, which contributes to the influx of private investment into the Russian economy.

**Keywords:** tax administration, tax benefits, digitalization of taxation, individual investment account, tax deduction

**Введение.** В связи со сложившейся в настоящее время экономической ситуацией особенно остро стоит задача стимулирования инвестиционной активности населения в целях развития российской экономики.

Работа по привлечению сбережений населения в инвестиции на фондовом рынке началась задолго до санкционного давления на Российскую Федерацию в 2010-х годах, в результате чего появился такой инвестиционный инструмент как индивидуальный инвестиционный счет (далее – ИИС), однако особой популярности среди населения ИИС не получил.

**Основная часть.** Согласно статистике, представленной Центральным Банком России, «несмотря на увеличение открытых ИИС в период с 2015 по 2022 гг., количество получивших налоговый вычет инвесторов в последние годы снижалось. Налоговые вычеты были предоставлены инвесторам, которые обеспечили более трети всех взносов на ИИС. Оставшиеся взносы приходятся в основном на клиентов, которые расторгли договоры ИИС досрочно, либо на инвесторов с небольшими вложениями, которые не планируют обращаться за вычетом» [4]. Указанная статистика указывает, на тот факт, что сам механизм ИИС, а также процесс оформления и получения налоговых вычетов в связи с использованием ИИС требовал изменений.

Начиная с 2022 года Минфином России совместно с Центральным Банком России повторно началась работа по актуализации и создания инвестиционно привлекательного для населения и одновременно выгодного для российской экономики инструмента привлечения денежных средств. В результате в 2023 году в федеральный закон № 39 «О рынке ценных бумаг» были внесены соответствующие

щие изменения. В соответствии с введенными изменениями создан новый формат ИИС третьего поколения, направленный на долгосрочное инвестирование денежных средств, владельцам которых доступен широкий круг преференций, в том числе, налоговых в виде налогового вычета по налогу на доход физических лиц (далее – НДФЛ).

Согласно статье 10. 2-1 Федерального закона № 39 «О рынке ценных бумаг», индивидуальный инвестиционный счет – это «счет внутреннего учета, который предназначен для обособленного учета денежных средств, драгоценных металлов, ценных бумаг клиента – физического лица, обязательств по договорам, заключенным за счет указанного клиента, и который открывается и ведется в соответствии с настоящим Федеральным законом и нормативными актами Банка России» [6].

Первый тип ИИС включал возможность получения его владельцем налогового вычета, однако этот вычет составлял 13 % от взносов на счет и не мог превышать 52 тыс. руб. в год, второй типа ИИС предполагал освобождение от уплаты НДФЛ по доходам от сделок по таким счетам, при этом сумма освобождения не была ограничена.

В связи со снижением привлекательности банковских вкладов до 2022 года ИИС имели большую популярность среди населения, особенно ИИС первого типа, однако в связи с геополитическими событиями и уходом иностранных участников фондового рынка востребованность ИИС среди россиян резко сократилась, что послужило предпосылкой разработки государством ИИС нового типа с более выгодными условиями инвестирования, а также выгодным налоговым вычетом, при этом инвестиционные счета старого поколения продолжают действовать, но открывать такие ИИС с 2024 возможность не предусмотрена.

Наличие индивидуального инвестиционного счета нового поколения, согласно положениям ст. 219.1 Налогового кодекса РФ позволяет лицам, открывшим его после 1 января 2024 года, получать сразу два вида налоговых вычетов:

- вычет на взнос на ИИС, которая предоставляет владельцу ИИС вернуть часть денежных средств, ранее внесенных на счет, но не более 52 тыс. в год;
- вычет на доход позволяет не платить владельцам ИИС НДФЛ с прибыли по финансовым операциям.

Для получения новых вычетов ИИС должен быть открытым не менее десяти лет с даты заключения договора, но с учетом переходного периода (от 5 лет). Максимальный размер налогового вычета в сумме прибыли по всем ИИС, которые были закрыты в один год составляет 30 млн руб.

Рассматривая указанные налоговые льготы для владельцев ИИС, можно сделать вывод о том, что фактически ИИС третьего типа является неким гибридом ИИС первого и второго типа, что, несомненно, должно положительно сказаться на его привлекательности среди населения, а также будет способствовать улучшению инвестиционного климата и привлечению инвестиций в российскую экономику.

Согласно статистическим данным Центрального Банка России, по итогам первого квартала 2024 года открыто порядка 5,9 млн ИИС, что немного меньше, чем в 2023 (6 млн ИИС), однако общая сумма активов в 2024 году оказалось

больше, чем в 2023 году – 545,4 млрд руб. [5]. Однако, думается, что часть открытых ИИС третьего типа, это ИИС первого и второго типа, срок действия которых истек, в связи с чем произошел переход на ИИС нового формата, кроме того, по данным Центрального Банка России, количество открытых в первом квартале 2024 года ИИС третьего типа на настоящий момент не компенсирует ранее закрытых ИИС прошлого поколения, что и вызвало снижение общего количества открытых счетов.

Необходимо отметить также тот факт, что в связи с условиями использования ИИС, а также нормами действующего законодательства, к покупке доступны лишь активы отечественных компаний. С одной стороны, действия законодателя направлены на привлечение инвестиций в российскую экономику. Однако данные ограничения могут отрицательно сказываться на прибыльности ИИС.

Также негативным фактором при вложении инвестиций налогоплательщиком является факт отсутствия страхования такого счета по аналогии с банковским вкладом, который на фоне высокой ключевой ставки может стать для граждан привлекательнее с позиции прибыльности.

Налоговые вычеты являются важной составной частью процесса стимулирования населения инвестировать денежные средства в российскую экономику посредством ИИС. С трансформацией самого механизма ИИС, произошли изменения в порядке оформления и предоставления налоговых вычетов владельцам ИИС, что в первую очередь связано с цифровизацией многих процессов в рамках налогового регулирования, что, по оценкам многих авторов, является положительной тенденцией. Так, О. И. Лютова отмечает, что «цифровые сервисы упрощают взаимодействие их сторон и нивелируют отдельные ситуации возможных злоупотреблений» [3]. Данный тезис подтверждается также в работе Дирксен Т. В, которая отмечает, что именно цифровизация налогового администрирования (применения налоговыми органами различных программ) позволяет предотвращать случаи злоупотребления налогоплательщиками своих прав и уклонения от уплаты налогов [2]. Как отмечается в литературе, «цифровые системы стали доминирующим элементом в работе налоговых органов во всем мире» [1].

В связи внедрением цифровых решений в налоговое администрирование, процесс получения ИИС также реализуется посредством цифровых механизмов, а именно через личный кабинет налогоплательщика. В личном кабинете налогоплательщика владельцу ИИС в целях получения налогового вычета в упрощенном порядке требует от налогоплательщика заполнения налоговой декларации 3-НДФЛ в упрощенной форме, в связи с тем, что остальная необходимая информация сервисами налоговых органов необходимая информация формируется автоматически путем обмена информацией с внешними источниками данных (банки, исполнительные органы государственной власти), что значительно оптимизирует весь процесс.

После заполнения необходимой информации в личном кабинете налогоплательщика и подтверждении факта наличия права на получения права на налоговый вычет, сервисами Федеральной налоговой службы РФ автоматически формируется заявление на предоставление налогового вычета, которое заявите-

лю необходимо акцептировать путем использования неквалифицированной электронной подписи. После направления указанного заявления, налоговые органы проводят проверку по указанным фактам, в результате чего на указанный в личном кабинете налогоплательщика банковский счет заявителю поступают денежные средства в счет налогового вычета по индивидуальному инвестиционному счету.

Оперативное информационное взаимодействие по предоставлении информации в части наличия у заявителя индивидуального инвестиционного счета, а также информации о его пополнении и прибыли осуществляется на основе цифровой среды, поэтому ФНС России для обработки информации использует технологии искусственного интеллекта, различные нейросети и big data. В настоящий момент информационное взаимодействие осуществляется с 21 финансовой организацией, обладающей лицензией на осуществление банковских операций, а также лицензии на осуществление брокерской деятельности.

При этом благодаря цифровой обработке данных, а также цифровому информационному обмену информацией, камеральная налоговая проверка также проводится в сокращенные сроки: так по упрощенной цифровой процедуре получения налогового вычета камеральная налоговая проверка проводится 1 месяц, вместо стандартных 3, а на практике денежные средства в счет налогового вычета зачисляются в пределах 10 дней, что дает возможность сделать вывод о том, что процессы цифровизации налогового контроля и оказания услуг налогоплательщика повышают как качество обслуживания, так и снижают нагрузку на налоговые органы минимизируя при этом личное взаимодействие сотрудников налоговых органов и налогоплательщиков.

**Закключение.** Таким образом, на уровне институтов налогового права в условиях цифровизации экономики происходят весьма глобальные изменения [4. С. 173]. Модернизация такого инвестиционного инструмента, как индивидуальный налоговый счет, открывать и использовать который существует возможность посредством онлайн-сервисов в совокупности с электронной процедурой получения налоговых вычетов в связи с их использованием с начала 2024 года демонстрирует положительную динамику в части привлечения в российскую экономику частных инвестиций. Для обеспечения притока в экономику частных инвестиций необходимо разработать стимулы для использования гражданами индивидуальных инвестиционных счетов, в связи с чем, основным механизмом такого стимулирования стали налоговые вычеты как на суммы пополнения счета, так и на прибыли по результатам инвестиционной деятельности.

Цифровизация процесса получения налогового вычета, которая обеспечивает простоту и доступность данной налоговой льготы для подавляющего большинства инвесторов, является также одним из сильнейших стимулов вложения денежных средств в долгосрочное инвестирование.

Вместе с тем налоговое регулирование такого относительно молодого инвестиционного инструмента требует совершенствования, в том числе, в части процедуры получения налоговых вычетов, и будет требовать корректировки по ходу использования его налогоплательщиками.

### Список литературы

1. Bassey E., Mulligan E., Ojo A. A conceptual framework for digital tax administration-A systematic review // *Government Information Quarterly*. – 2022. – Т. 39, № 4. – С. 101754.
2. Дирксен Т.В. Меры профилактики уклонения от уплаты налогов в условиях цифровизации налогового администрирования // *Финансовое право*. – 2024. – № 7. – С. 31–34.
3. Лютова О.И. Права налогоплательщиков: трансформация в условиях цифровизации // *Налоги*. – 2020. – № 5. – С. 10–12.
4. Лютова О.И. Цифровая трансформация принципов налогового права // *Journal of Digital Technologies and Law*. – 2024. – № 2(1). – С. 163–180. <https://doi.org/10.21202/jdtl.2024.9>. EDN: zuaihn
5. Тенденции сегмента индивидуальных инвестиционных счетов в I квартале 2024 года. – Текст : электронный // Банк России [Электронный ресурс]. – URL: [https://www.cbr.ru/analytics/rcb/iis\\_1q\\_2024](https://www.cbr.ru/analytics/rcb/iis_1q_2024)
6. О рынке ценных бумаг: Федеральный закон от 22.04.1996 № 39-ФЗ (ред. от 08.08.2024) // Собрание законодательства Российской Федерации. Собрания законодательства Российской Федерации. – 1996. – № 17. – Ст. 1918.

**Я. О. Кучина,**

кандидат юридических наук, доцент, LL.M., Ph.D.  
Дальневосточный федеральный университет

### РЕГУЛИРОВАНИЕ ЦИФРОВОЙ ВАЛЮТЫ В КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКЕ

**Аннотация.** В предлагаемом анализе рассматривается ЦВЦБ КНР, его особенности, технологические и не технологические компоненты. Основным источником анализа служит Программный документ – «белая книга ЦВЦБ КНР», на данный момент являющаяся единственным официальным источником информации о том, как построено регулирование валюты. Этот документ относится к числу устанавливающих регуляторные принципы, и является примером общепринятого метода регулирования инновационных финансовых технологий в стадии пилотного запуска. На основании проведенного анализа в статье предлагаются выводы, текущие и итоговые, о том, что же такое ЦВЦБ КНР, какова ее структура и каковы особенности и направления применения ЦВЦБ КНР, правовой эффект от ее внедрения.

**Ключевые слова:** цифровые валюты Центробанков, цифровой юань, ЦВЦБ, криптовалюта, стейблкоин, финтех, фиатные деньги, монетарная политика, финансовое регулирование, право технологий, цифровая экономика, цифровизация

## REGULATION OF DIGITAL CURRENCY IN THE PEOPLE'S REPUBLIC OF CHINA

**Abstract.** The proposed analysis examines the CBDC of the PRC, its features, technological and non-technological components. The main source of analysis is the the Whitepaper of the CBDC of the PRC, which is currently the only official source on how currency regulation is structured. This document is one of those establishing regulatory principles and is an example of a generally accepted method of regulating innovative financial technologies at the pilot stage. Based on the analysis, the article offers conclusions, current and final, on what the CBDC of the PRC is, what its structure is, what are the features and areas of application of the CBDC of the PRC, the legal effect of its implementation.

**Keywords:** Central Bank Digital Currencies, Digital Yuan, Central Bank Digital Currency, Cryptocurrency, Stablecoin, Fintech, Fiat Money, Monetary Policy, Financial Regulation, Technology Law, Digital Economy, Digitalization

Китай – один из несомненных лидеров цифровизации в мире. Автор фактической концепции регулирования электронной коммерции, пионер создания торговых платформ и термина «цифровой суверенитет», он также находится в авангарде развития инновационных технологий «смены парадигм». При этом Китай относится к сравнительно небольшому количеству государств, которые ввели полный запрет криптовалют.

Одновременно Китай является государством с самым большим числом мобильных платежей в мире, особенно после того, как в пандемию стремительно упал оборот наличных средств. Это привело к тому, что Китай столкнулся с доминированием бигтеха – мультифункциональных экосистем WePay и Alipay. Эти системы мобильных платежей практически монополизировали сектор потребительской торговли, и сервисы онлайн-банкинга не способны с ними конкурировать. По сути, Китай на практике доказал предположение, что население, удаленное от банковской инфраструктуры (обычно сельское население, не имеющее физического доступа к банкам), компенсирует этот недостаток мобильными платежными технологиями и финтехом, доступ к которым обеспечивается в рамках технологического принципа «доступ по требованию» [6. С. 255]. Однако это же создает угрозу экономике, поскольку мобильные платежные системы становятся незаменимыми. Как любая форма финтеха, такого рода инновации разрушают традиционный финансовый рынок. И любой сбой в функционировании способен повлечь непредсказуемые последствия для него.

Именно этот риск стал причиной, по который был разработан «цифровой юань» – цифровая валюта Центробанка КНР.

16 июля 2021 г. Народный Банк Китая выпустил «белую книгу» – Программный документ о процессе разработки ЦВЦБ. Из него, прежде всего, стало известно наименование проекта – e-CNY («электронный китайский юань») [1], что отличает его от официального наименования «фиатного юаня» – жэньминьби или RMB. До того проект был известен как Digital Currency/Electronic Payment или DCEP [1].

В Китае фиатные валюты, даже в безналичной форме, проигрывают финтех-системам мобильных платежей. Население предпочитает их банковским сервисам из-за удобства. Мобильные платежные платформы характеризует высокая степень интеграции в цифровую торговлю, простота использования, скорость транзакций, возможность пополнения при отсутствии банковского счета и прочие упрощающие их использование характеристики. В 2019 г. 66 % платежей совершались посредством мобильных сервисов (что составило 59% от всего денежного потока), 23 % – составляли наличные платежи и 7 % – платежи банковскими картами [2]. То есть даже при наличии банковской карты она редко используется для платежей, а более – как способ снятия наличных денежных средств в банкомате без обращения в офис банка.

Как показывает анализ финансовых отчетов и документов Народного Банка Китая, основной официальной целью разработки ЦВЦБ КНР является стремление создать альтернативу криптовалютам и мобильным платежам, устранив микрофинансовый и макрофинансовый риск, а также сбалансировать рынок, как потребительский, так и транзакций.

В СМИ предполагаемые цели разработки и внедрения ЦВЦБ зачастую излагаются спекулятивно и без должной достоверности. Пресса и научные работы [5, С.107] приводят информацию без ссылок на первоисточники в виде заявления представителей Центробанка КНР или финансовых органов. Из-за чего существует две большие группы теорий относительно того, для чего разработан «цифровой юань». Первая касается его прозрачности и, соответственно, способности отслеживать транзакции, в том числе бороться с преступностью, вторая – потенциальной возможности создать независимую платежную систему по принципу P2P (или S2S, «государство – государству»). Имеется в виду разработка альтернативы SWIFT, защита от возможных финансовых санкций и основное оружие в новом раунде торговых войн.

В Программном документе указано, что разработка ЦВЦБ продиктована переходом Китая от стадии «стремительной цифровизации» к качественной, основой для которой должны стать технологии и сервисы «смены парадигм» – искусственный интеллект, облачные технологии, блокчейн, бигтех и прочие. Эта цель подчеркивается дважды, с указанием, что сфера финансовых технологий Китая переходит на новую технологическую ступень и меняет направление развития.

Программный документ от 16 июля 2021 г. до сих пор является единственным документом, определяющим правовой статус «цифрового юаня», что объяснимо при внедрении экспериментального финансово-технологического решения. Какое-либо регулирование более императивного характера не будет действовать применительно к развивающемуся объекту регулирования.

В Программном документе подтверждается основная цель разработки ЦВЦБ – сбалансировать потребительский рынок. Справедливо отмечается, что банковская система способна предоставить более защищенную систему платежей, одновременно поддерживая конкуренцию и предоставляя потребителю выбор. То есть побочной целью разработки является противодействие монополии мобильных платежных бигтех-систем без привлечения антимонопольных мер

воздействия, а посредством диверсификации предложений. Это, как можно предположить, было также продиктовано желанием сбалансировать экономику и избежать серьезных кризисов как из-за регуляторного воздействия на монополистов, так и при отсутствии реакции на монополию.

Также упоминается высокая стоимость управления наличными средствами – традиционные банковские услуги характеризуются дороговизной в сравнении с финтехом, это общеизвестный факт. Дороговизна определяется как эмиссией фиатных валют (что, совершенно очевидно, тоже стоит денег, в том числе дизайн купюр и их защита от подделки), так и иными затратами, особенно на так называемый «человеческий фактор» и процедурный порядок оказания финансовых услуг. Так что, разрабатывая ЦВЦБ, Китай, как совершенно очевидно, руководствовался данными, полученными при исследовании не только финансового сектора, но и сектора финтеха, причинами и условиями его возникновения, развития и эффектом, производимым на рынок (как отрицательным, так и положительным).

Далее в числе причин перечислено стремительное развитие криптовалют. Как уже было сказано выше, такая причина является универсальной – противодействие криптовалютам основная цель, побудившая Центробанки всех стран заинтересоваться проектами по разработке ЦВЦБ. Китай в этом случае не уникален, тем более, при условии примененного в полном объеме метода регуляторного запрета. Как указано в документе, высокий спекулятивный потенциал криптовалют и способность обходить гарантии финансовой безопасности, в том числе правило «знай своего клиента», может представлять опасность даже для мировой финансовой системы. Как показывает сравнение хронологии разработки ЦВЦБ и стадий введения запрета, они осуществлялись параллельно и, судя по всему, были взаимно продиктованы. Китай начал исследовать криптовалюты (к которым технологически относится ЦВЦБ) в 2014, начал проект – в 2017, а первые тестовые пробы сервиса начались в 2019. В 2021 г. была выпущена «белая книга цифрового юаня».

Третьей причиной является нежелание Китая отставать в развитии ЦВЦБ. Такое основание для его действий можно увидеть не только в этой сфере – иные технологические инициативы также продиктованы стремлением быть в авангарде цифровизации. Кроме того, как уже также упоминалось, регуляторный запрет на криптовалюты существенно затормозил развитие блокчейна в Китае, потому опыт в проектировании и запуске ЦВЦБ потенциально может восполнить возникший пробел.

Иных целей, причин и задач для разработки и внедрения «цифрового юаня» не приводится.

ЦВЦБ существуют в нескольких видах, описание которых разнится терминологически, но одинаково технологически. Наиболее часто встречается разделение ЦВЦБ на две модели – ЦВЦБ-токены и ЦВЦБ-счета.

ЦВЦБ-токены используют цифровой токен, эмитируемый и распределяемый Центробанком. Для авторизации от пользователя требуется знание криптографической пары – открытого и закрытого ключей. Этот вид обеспечивает высокую степень анонимности, так как кроме криптографической пары и иденти-

фикатора кошелька на базовом уровне пользователю не требуется ничего. Однако центральные банки могут принять решение о внедрении дополнительных требований к идентификации. Предполагается, что в таком случае защиты анонимность будет внешней – между сторонами по транзакции, но не внутренней, так как Центробанк будет видеть идентификационные данные пользователей. Это отличает ЦВЦБ-токен от криптовалюты.

Платеж (транзакция) ЦВЦБ при такой модели цифровой валюты зависит от способности отправителя проверить действительность второй стороны и объекта платежа, то есть требует наличия определенной формы технологии распределенного реестра для проверки цепочки владения каждым токеном и проверки платежных транзакций. Это означает более высокий риск для конечного пользователя при потере ключа, утрате доступа к кошельку и его содержимому, то есть требует дополнительных гарантий владения и идентификации.

При выборе модели этого вида банки должны будут стать первой линией защиты для соблюдения правила «знай своего клиента» (KYC) и борьбы с отмыванием денег/финансированием терроризма (AML/CFT). Этот метод может обеспечить универсальный доступ к ЦВЦБ, сохранить анонимность как максимально привлекательное (для пользователя) свойство, повысить конкурентоспособность ЦВЦБ. То есть помочь достигнуть тех целей, что поставил перед собой Китай в начале проекта. Однако при выборе базовой модели, а также при наличии отдельных особенностей процессуальной деятельности, это никак не облегчает правоохранительную деятельность.

ЦВЦБ-счета представляют собой более классическую версию цифровой валюты, так как по сути являются банковским счетом на основе учетной записи, привязанной к личности владельца счета. То есть он представляет собой сочетание традиционных банковских отношений и инновационного объекта этих отношений. Для перевода средств банки обрабатывают каждый платеж, дебетуя счет отправителя и кредитуя счет получателя. Транзакции необходимо проверять с использованием идентификаторов пользователей, и поэтому необходимы надежные системы управления идентификацией для поддержания уникального идентификатора каждого человека во всех платежных системах.

При выборе модели ЦВЦБ-счетов ответственность за соблюдение требований «знай своего клиента» и требований к противодействию отмыванию денежных средств и финансированию терроризма возлагается на Центральный банк. Проверка переводов в системе на основе учетных записей зависит от установления соответствующих мер защиты от кражи личных данных, мошенничества и несанкционированных переводов денежных средств с активных учетных записей (ЦВЦБ-счетов).

Возникает вопрос, какую же из моделей предпочел Китай? Ответ прост, если принять во внимание предпочтение использования китайским регулятором метода ожидания и метода тестирования в сфере финансовых инноваций. Цифровой юань представлен в двух видах – как токен и как счет. Это объективно подтверждает то, что цели, заявленные в качестве основных для разработки ЦВЦБ, таковыми и являются. С позиции технологии оценить возможное преимущество какой-либо из моделей перед мобильными платежами можно только

внедрив обе. Каждая из них обладает уникальным набором достоинств и недостатков, каждая, как технологическое решение, требует массового тестирования, чтобы оценить возможные технологические проблемы, устойчивость, предпочтения потребителей, удобство и прочее.

В целом, как показывает анализ программного документа, гибридизация является основой проекта ЦВЦБ Китая. Так, между двумя моделями платформы – основанной на распределенном реестре и на механизме центрального подчинения, КНР предпочел гибридную систему. Прямо указывается, что распределенный реестр не является классической моделью блокчейна, потому что она не является удобной по ряду причин, в частности, по энергозатратности и доступности. Также выбор модели платформы, ее архитектуры, был сделан с расчетом длительности использования и возможности технологического развития. То есть, очевидно, что проект «цифрового юаня» заранее рассматривался как долгоживущий, а не пилотный с возможностью прекращения после тестирования, как это случилось в ряде стран (например, в Эквадоре).

Указано, что технологические компоненты ЦВЦБ основаны на сочетании распределенной и централизованной архитектур, и двойственности состояния проекта – стабильном и аджайл-состоянии. Последнее означает, что «цифровой юань» относится к гибким проектам, реализуемым в итеративно-инкрементальном ключе. Здесь итеративный подход допускает получение обратной связи на ранних стадиях готовности продукта проекта для его доработки. А инкрементальный предусматривает поставку продукта небольшими частями по мере готовности. Проект ЦВЦБ КНР, таким образом, сочетает оба подхода и, одновременно, имеет стабильную часть, которая в меньшей степени подвержена модернизации по мере тестирования.

Из Программного документа также очевидно, что при разработке учтен и внедрен компонент «доступа по требованию», а также повышенные требования к криптографической защите. В частности, указывается, что с целью обеспечить надежность и работоспособность системы было использовано сочетание ТРМ-технологий и специальных методов шифрования, внедренных на основе интеграции аппаратного и программного обеспечения. Такие многоуровневые системы безопасности и специальные разработки в области обработки данных гарантируют доступность и круглосуточное обслуживание, непрерывность предоставления услуги, в том числе устойчивость к стихийным бедствиям.

Кроме того, технологические компоненты ЦВЦБ и их модели зависят от того, к какому виду относится цифровая валюта – национального и трансграничного средства платежа. Если исходить из того минимума технологических деталей, что представлен в Программном документе, ЦВЦБ был запущен как национальный проект с соответствующей архитектурой. Однако его гибридный характер, в том числе аджайл-состояние, позволят в будущем развить платформу и как средство для трансграничных финансовых операций.

Что касается нетехнологических компонентов, то первое, на что следует обратить внимание, это безусловное утверждение о природе ЦВЦБ. «Цифровой юань» приравнен к национальной валюте и описывается как «цифровая фиатная валюта».

Некоторые полагают, что это означает признание ЦВЦБ формой электронного банковского платежа (лишь в ином виде) за пределами ДБС. Однако в рамках данной статьи будет высказано иное мнение. Сочетание в термине признаков «цифровая» и «фиатная» позволяет предположить, что в КНР признается факт существования двух видов валют – аналоговой и цифровой в виде, соответственно, фиатной наличной и фиатной цифровой. Как известно, для совершения электронного платежа требуется наличие эквивалентного объема наличных денег. То есть приравнять цифровую фиатную валюту и традиционный электронный платеж не следует, так как цифровая фиатная валюта не требует эквивалентного объема наличных денег на счете. Иными словами, в КНР существует два равных вида национальной валюты – это цифровая и аналоговая национальные валюты. Судя по всему, их курс и обеспеченность имеют одинаковое происхождение, а регулирование и правовой статус как объекта права также должен быть приблизительно равным за исключением тех положений, что продиктованы формой самой валюты и особенностями ее эмиссии.

Для этого устанавливается принцип технологической нейтральности, который, напомним, означает отсутствие правового приоритета у какой-либо из форм, что прямо указано в Программном документе.

Применительно к «цифровому юаню» также введен в действие принцип регуляторной нейтральности, который означает, что в отношении ЦВЦБ действуют все те же нормы и правила, что в отношении аналоговой фиатной валюты, и на банки, участвующие в операциях, возлагаются те же обязанности. То есть на ЦВЦБ распространяются все нормы банковского права КНР, в том числе об идентифицируемости клиента, противодействии отмыванию денежных средств и финансированию терроризма. Иными словами, ЦВЦБ заранее соответствует национальным и международным требованиям, что существенно отличает «цифровой юань» от криптовалют.

При этом ЦВЦБ КНР предоставляет уникальную возможность оценить потенциал внедрения соответствия нормативно-правовому регулированию на уровне технологии. Тут стоит напомнить, что это основная проблема финтех-разработанное технологическое решение зачастую настолько уникально и экспериментально, что не может соответствовать действующему в этой области праву. Это обуславливает основные проблемы, связанные с финтехом, в частности, проблему правоприменности – способность регулятора к правоприменительной интервенции, когда вмешательство способно привести к остановке сервиса, но не к следованию закону, особенно если технологическое развитие регулятора ниже, чем сервиса, который он регулирует.

Так, указывается, что применительно к ЦВЦБ используется принцип полунанонимности, то есть напрямую устанавливается возможность анонимных транзакций в небольшом объеме. Это связано с целью конкурировать с мобильными платежами и криптовалютами и, тем самым, снизить монополию бигтех-платформ в секторе. При этом крупные транзакции не могут быть анонимными, что, опять же, доказывает, что соответствие нормам о противодействии отмыванию и финансированию встроено в технологию ЦВЦБ на момент ее пилотного запуска.

Как очевидно из технологии ЦВЦБ, прозрачность цифровых валют такого типа высока. ЦВЦБ, по сути, представляют собой криптовалюты, эмитируемые центральным единокличным субъектом, которым является Центробанк страны. Однако попытки обвинить Китай в желании повысить уровень контроля за гражданами нельзя считать обоснованным. Дело в том, что ЦВЦБ односторонне прозрачны независимо от страны эмиссии – это их объективное технологическое свойство.

Оно основано на том, что анонимность в традиционном банковском секторе не существует как таковая – при желании банка быть частью международной финансовой системы он должен соответствовать трем основным принципам: «знай своего клиента», противодействие отмыванию денежных средств и финансированию терроризма. Из этого следует объективный вывод, что банковская деятельность и деятельность с фиатными валютами, независимо от формы, обязана быть прозрачной для регулятора. Степень этой прозрачности в случае с ЦВЦБ Китая прямо описывается в Программном документе и обосновывается выбором моделей ЦВЦБ.

ЦВЦБ КНР имеет те же характеристики анонимности, что «физическая» валюта, то есть наличная. Также указывается, что счета ЦВЦБ соединены с банковскими счетами, что особенно важно применительно к модели ЦВЦБ-счетов. Это значит, что идентификация владельца счета происходит по тем же правовым принципам, что и обычного банковского счета – для банков не должно быть разницы. В случае с ЦВЦБ-токенами абсолютная прозрачность является односторонней – субъекта, владеющего токенами, видит банк-эмитент, Народный Банк Китая.

Количество услуг и объем транзакций в ЦВЦБ-кошельке зависит от количества предоставленных персональных данных. Такая модель используется многими неанонимными и полуанонимными криптовалютными платформами и не является уникальной. При этом объем данных для ЦВЦБ-счета, привязанного к банковскому аккаунту владельца в силу технологической архитектуры, больше, чем у ЦВЦБ-токена.

Внешний вид приложения-кошелька и его внутренние спецификации разрабатываются отдельными банками Китая, Народный Банк Китая как эмитент разрабатывает требования к ним, которым они должны соответствовать. На коммерческие банки также возлагается сбор статистики – то есть оценка обратного эффекта введения ЦВЦБ в оборот. Это означает, что система ЦВЦБ, независимо от модели, является двухуровневой и информация, поступающая об использовании ЦВЦБ доступна разным участникам правоотношений в дифференцированном объеме.

Разумеется, беспокойство относительно прозрачности существует и среди населения КНР. В частности, особенностью ЦВЦБ является прямой доступ эмитента как к кошельку, так и к данным о получателе ЦВЦБ. Это позволяет моментально приводить в исполнение распоряжения об аресте и конфискации – побочный эффект технологических особенностей любых криптовалют. В ситуации с истинными криптовалютами он нивелируется децентрализацией или самим фактом эмиссии небанковским субъектом, то есть процедура удлиняется при соблю-

дении всех процессуальных норм и требует технических возможностей. В случае с ЦВЦБ она, наоборот, сокращается, так как при наличии данных о ЦВЦБ-счете, требуется лишь обратиться в Центробанк. Это универсальное свойство ЦВЦБ и эффект от сокращения количества посредников при дистрибуции национальной валюты.

Несомненно, это заставляет задуматься о соблюдении прав собственности и их защите. Однако эффект в борьбе с преступностью, в частности, с коррупцией, сомнителен. Как показывают данные, в КНР, в котором уровень прозрачности финансовых поступлений государственным служащим отслеживается чрезвычайно пристально, способы обхода этого слежения давно сугубо аналоговые – это использование посредников, наличности, получение подарков или взятки услугами. То есть рассматривать ЦВЦБ как инструмент слежки за противоправной деятельностью граждан все же не следует, судя по всему, результат будет ниже ожидаемого.

В заключительной части статьи коснемся еще одной предполагаемой цели введения ЦВЦБ в КНР – ее возможной способности заменить SWIFT.

Сразу стоит отметить, что таких утверждений прямо или косвенно в государственных программных документах нам обнаружить не удалось. Анализ Программного документа показывает, что создание ЦВЦБ рассчитано на трансграничное использование, однако оно не является приоритетным на текущих стадиях внедрения. С правовой точки зрения это вполне объяснимо – трансграничные платежи в банковской системе должны соответствовать международным требованиям. В случае с централизованной криптовалютой, которой, по сути, является любая ЦВЦБ, эти требования не определены, так как такие платежи сочетают в себе признаки правовой природы (нетехнологический компонент) национальных валют и технологическую форму криптовалют. Это само по себе создает правовой парадокс.

Как показывает анализ опыта трансграничной локализации централизованных финтех-сервисов, это обычно происходит на основе двусторонних или многосторонних соглашений, включающих унификацию требований к соблюдению норм, лицензированию и так далее. Это так называемые «процедуры приземления», при которых финтех-провайдер открывает филиалы или дочерние представительства в конкретной стране, адаптирует национальное право и ограничивает сервис в соответствии с ним, прочее. Есть также примеры платформ, позволяющих упростить процесс, но их использование гарантировано теми же многосторонними соглашениями между странами-участниками.

Но ЦВЦБ – это национальная валюта в цифровой форме и к ней в связи с этим, согласно аналогии права, должны применяться требования в отношении национальных валют. Поэтому, на данной стадии, относительно ЦВЦБ Китая и их адаптации известно следующее.

В январе 2021г. между Обществом всемирных межбанковских финансовых телекоммуникаций (более известным как SWIFT) и Народным Банком Китая, а также иными субъектами, в том числе Исследовательским институтом цифровых валют, было заключено венчурное соглашение и создана компания Financial Gateway Information Services Co., Ltd [3]. Конкретные цели создания

венчурной компании не ясны, согласно пресс-релизу, она будет заниматься агрегированием информационных систем, обработкой данных и консультированием по технологиям.

Одновременно в прессе появились рассуждения о том, будет ли компания заниматься вопросами исследований трансграничного внедрения цифрового юаня, в частности, способствовать его интернационализации как средства платежа. Действительно, предполагать подобное позволяет как тот факт, что филиал SWIFT в Пекине не имеет китайского соучастника, а целиком принадлежит Обществу, а также заявлениями отдельных представителей о том, что цель компании «интегрировать юань в мировую торговлю как свободно-конвертируемую валюту». О какой форме юаня может идти речь – не уточнялось.

Китай неоднократно высказывал желание как можно сильнее интегрироваться в международную финансовую систему и открыть свои финансовые рынки. В марте 2021 г. в официальном пресс-релизе об открытии венчурной компании указано, что основной целью открытия является следование рекомендациям международных финансовых институтов, желание усилить гарантии по прозрачности и надежности трансграничных платежей, защита прав граждан, дополнительные гарантии юридическим лицам, а также «обеспечение услугами финансовых шлюзов» [3]. Сюда включены создание и эксплуатация локальных сетевых точек концентрации данных для служб обмена финансовыми сообщениями, создание и эксплуатация локальных хранилищ данных и другие сопутствующие услуги. Совместная разработка со SWIFT услуг финансовых шлюзов «способствует достижению взаимной выгоды и взаимовыгодной динамики, а также предоставит пользователям более стабильные, более устойчивые, более безопасные и более совместимые услуги». В качестве следующего шага Народный банк Китая обязался усилить надзор и руководство в названных областях, а также будет способствовать стандартизированному развитию услуг финансовых шлюзов всеми сторонами. Иных сообщений или информации не было.

Из сказанного очевидно, что не существует прямых исследований распространения «цифрового юаня» за пределы границ КНР, а иные утверждения являются не более чем гипотезами. Тем более, что трансграничное использование национальных ЦВЦБ для расчета в национальных интересует не только Китай или Россию, таких инициатив множество. Однако замедленность процесса развития проектов делает их реализацию практически невозможной.

Дело в том, что 27 марта 2024 года SWIFT заявила о создании единой платформы интеграции цифровых валют для трансграничной торговли, запуск которой ожидается в срок от 12 до 34 месяцев [4]. Это приведет к тому, что роль SWIFT в трансграничной торговле станет максимальной ведущей.

Более того, согласно этому заявлению, уже 38 государств принимают участие в тестировании, которое длилось шесть месяцев и осуществлялось на уровне Центробанков. Цель тестирования – определить технологическую совместимость, то есть способность различных по технологическим компонентам и архитектуре ЦВЦБ взаимодействовать в рамках одной платформы. Как известно со слов Ника Керригана, руководителя проекта, минимум два коммерческих банка Китая принимают участие в проекте. Помимо этого, в проекте участвуют

Сингапур, Таиланд, Германия, Чехия, иные страны Европы. Согласно утверждению, отключение от услуг платформы, как от услуг SWIFT, не является исключением, хотя SWIFT надеется этого избежать.

Потому возможно заключить, что потенциал санкционного обхода при помощи ЦБЦБ, равно как развитие трансграничной торговли в национальных валютах на основе двусторонних соглашений и платформ, существенно снижается, а такая цель не является объективно-подтверждаемой. Во-первых, репутация SWIFT как провайдера услуг связи неизменно выше. Во-вторых, многостороннее соглашение является большей гарантией, чем двустороннее, а глобальная платформа с технологической точки зрения будет функционировать стабильнее, чем двусторонний шлюз. Иными словами, если цели заменить SWIFT при помощи ЦБЦБ у Китая и были, их следует воплотить как можно скорее, не позднее двенадцати месяцев с момента заявления SWIFT.

### Список литературы

1. Белая книга о ходе исследований и разработок китайского цифрового юаня. Прогресс исследований и разработок китайского цифрового юаня (Рабочая группа по исследованиям и разработкам цифрового юаня Народного банка Китая, июль 2021 г.) от 16 июля 2021 г. [中国数字人民币的研发进展白皮书 (中国人民银行数字人民币研发工作组 2021 年 7 月) 中国数字 人民币的 研发进展]
2. Общая работа платежной системы в четвертом квартале 2019 года. Отчет Народного Банка Китая (2019 年第四季度支付体系运行总体情况) [Электронный ресурс]. – URL: <http://www.pbc.gov.cn/zhifujiesuansi/128525/128545/128643/3990502/2020031714071484308.pdf>
3. Официальный пресс-релиз 中国人民银行有关部门负责人就金融网关服务有关问题答记者问 [Электронный ресурс]. – URL: <http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4212373/index.html>
4. Jones M. SWIFT planning launch of new central bank digital currency platform in 12-24 months [Электронный ресурс] // Reuters, 27 марта 2024. – URL: <https://www.reuters.com/business/finance/swift-planning-launch-new-central-bank-digital-currency-platform-12-24-months-2024-03-25/>
5. Kshetri N. Wholesale Central Bank digital currencies in Asia: current status and motivation // Computer, 2024. – T. 57, № 2. – С. 105–110.
6. López L. B. Trends on virtualisation with software defined networking and network function virtualisation' // IET Networks, 2015. – № 4(5). – С. 255.

**С. М. Миронова,**

доктор юридических наук, доцент,  
Волгоградский институт управления – филиал Российской академии  
народного хозяйства и государственной службы  
при Президенте Российской Федерации

## **РОЛЬ НАЛОГОВЫХ ОРГАНОВ В ПРОТИВОДЕЙСТВИИ НЕЛЕГАЛЬНОЙ ЗАНЯТОСТИ: ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ**

**Аннотация.** Увеличение числа самозанятых лиц, привело к тому, что их работа начала активно использоваться предпринимательским сообществом для подмены трудовых отношений, что ведет как к уменьшению собираемых налоговых и страховых взносов, так и необходимости защиты трудовых и социальных прав таких лиц. Налоговые органы, обладая большим объемом сведений и информации о самозанятых и компаниях, с которыми они работают, не только самостоятельно осуществляют налоговый контроль, но и предоставляют эти сведения органам, осуществляющим надзор за соблюдением трудового законодательства, а также вновь создаваемым межведомственными комиссиям по противодействию нелегальной занятости. При этом возникает ряд вопросов, как по содержанию предоставления сведений, так и по сохранению налоговой тайны теми лицами, которые будут работать с этими сведениями и информацией, что требует соответствующих дополнений в налоговом законодательстве. В работе проведен анализ последних изменений законодательства, связанных с созданием межведомственных комиссий по противодействию нелегальной занятости и определена роль налоговых органов в обеспечении таких комиссий сведениями и информацией, необходимыми для их эффективной работы.

**Ключевые слова:** Федеральная налоговая служба; самозанятые; налог на профессиональный доход; подмена трудовых отношений; нелегальная занятость; налоговая тайна; информационное взаимодействие

Статья подготовлена 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/>

## **THE ROLE OF TAX AUTHORITIES IN COUNTERING ILLEGAL EMPLOYMENT: INFORMATION INTERACTION**

**Abstract.** The increase in the number of self-employed persons has led to the fact that their work has begun to be actively used by the business community to replace labor relations, which leads to both a decrease in collected tax and insurance contributions, and the need to protect the labor and social rights of such persons. Tax authorities, having a large amount of data and information about the self-employed and the companies they work with, not only independently exercise tax control, but also provide this information to the bodies supervising compliance with labor legisla-

tion, as well as newly created interdepartmental commissions to combat illegal employment. At the same time, a number of questions arise, both on the content of the provision of information, and on the preservation of tax secrecy by those persons who will work with this information and data, which requires appropriate additions to the tax legislation. The paper analyzes the latest changes in legislation related to the creation of interdepartmental commissions to combat illegal employment and defines the role of tax authorities in providing such commissions with the data and information necessary for their effective work.

**Keywords:** Federal Tax Service; self-employed; professional income tax; substitution of labor relations; illegal employment; tax secrecy; information interaction

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.** Последние годы в России высокими темпами растет число самозанятых-плательщиков налога на профессиональный доход, что обуславливает интерес к данной теме [5]. По состоянию на 5 августа 2024 года их число достигло 11 миллионов человек, что намного выше тех показателей, которые изначально планировались при проведении эксперимента и введении данного налогового режима. Это обусловлено не только тем фактом, что налог на профессиональный доход очень удобен и прост в использовании за счет максимального цифрового взаимодействия между налоговым органом и налогоплательщиком, но в первую очередь тем фактом, что самозанятых стали использовать для подмены трудовых отношений [4]. Компаниям выгодно вместо того, чтобы нанимать сотрудников в штат по трудовому договору, заключать договоры гражданско-правового характера с самозанятыми на выполнение работ или оказание услуг, что дает возможность экономии на налогах и страховых взносах. На практике это приводит к многочисленным ситуациям подмены трудовых отношений, то есть фактически идет искажение правоотношений, что ведет к переквалификации этих отношений и доначислению налогов.

При этом должны быть сформулированы четкие критерии, позволяющие разграничить трудовые отношения от договоров по выполнению работ/оказанию услуг. На основе общих положений, закрепленных Трудовым кодексом РФ, еще до введения налога на профессиональный доход такие критерии были сформулированы Верховного суда РФ от 29 мая 2018 г. № 15.

**Основная часть.** Федеральная налоговая служба РФ, осуществляющая налоговый контроль и заинтересованная в наполнении бюджета налогами (реализуя фискальный интерес государства), в своих письмах также неоднократно формулировала критерии разграничения отношений самозанятых плательщиков налога на профессиональный доход от трудовых отношений и высказывала свою позицию на предмет недопустимости подмены трудовых отношений отношениями с самозанятыми лицом.

С одной стороны, такие критерии выработаны сложившейся российской практикой. С другой стороны, поскольку использование зависимых подрядчиков

вместо заключения трудовых договоров это не только российская, но и общемировая проблема, то можно анализировать и использовать опыт других стран, в которых сформирован свои критерии определения степени зависимости работника и уклонения таких компаний от уплаты налогов в связи с этим.

Например, в США изучают отношения работника и компании в целях определения, является ли он сотрудником или независимым подрядчиком. При определении данного факта учитывают два обстоятельства: степень контроля и степень независимости. Такие факты делят на три категории: поведенческий контроль, финансовый контроль и тип отношений сторон.

Так при поведенческом контроле выявляют факты, которые показывают, имеет ли бизнес-право направлять и контролировать, как работник выполняет задачу, для которой он нанят, включают тип и степень следующего. Инструкции, которые бизнес дает работнику. Сотрудник, как правило, подчиняется инструкциям бизнеса о том, когда, где и как работать. Все нижеперечисленное является примерами типов инструкций о том, как выполнять работу:

- Когда и где выполнять работу.
- Какие инструменты или оборудование использовать.
- Каких рабочих нанимать или помогать в работе.
- Где приобретать расходные материалы и услуги [1].

В Российской Федерации такие критерии сформулированы письмами ФНС России, на их основе решаются вопросы о том, какие отношения имели место быть на самом деле: гражданское-правовые или трудовые. За последние несколько лет сложилась судебная практика по данной категории дел, суды часто соглашались с позицией налоговых органов по доначислению налогов (например, постановление Арбитражного суда Северо-Западного округа от 13.08.2024 № Ф07-9143/2024 по делу № А56-122624/2022; постановление Арбитражного суда Дальневосточного округа от 08.12.2023 № Ф03-5254/2023 по делу № А04-2860/2023; постановление Арбитражного суда Поволжского округа от 10.07.2024 № Ф06-4539/2024 по делу № А57-10956/2023 и др.). И это только подтверждает тот факт, что компании часто используют труд самозанятых для подмены трудовых отношений.

За последние годы у налоговых органов сформировалась обширная база сведений о самозанятых – плательщиках налога на профессиональный доход, субъектах предпринимательской деятельности, с которыми они работают, сведения о сделках между ними и оплате по таким сделкам, иные сведения, которые позволяют определить фактические правоотношения между самозанятыми и их клиентами. Федеральная налоговая служба становится одной из самых больших цифровых платформ, аккумулирующих сведения, необходимые не только для осуществления налогового контроля, обеспечения налоговой безопасности государства, но и для иных целей, что предопределяет необходимость тесного информационного взаимодействия между налоговыми органами и иными органами публичной власти [2; 3].

Несмотря на то, что вопросы работы с самозанятыми, когда они фактически вступают в трудовые отношения с компанией, возникают уже не первый год, в части других вопросов, не связанных с доначислением налогов и страховых

взносов, должного контроля до последнего времени не осуществлялось, что приводило все к возрастающей подмене трудовых отношений. Такие категории занятых лиц (самозанятые, фактически вступившие в трудовые отношения) ведут не только к недоплате налогов и страховых взносов, что уменьшает поступления в бюджет и внебюджетные фонды, но и нарушает трудовые и социальные права таких работников, поскольку им не предоставляются гарантии, закрепленные трудовым законодательством, они не могут рассчитывать на будущую пенсию, они не могут получить пособие по временной нетрудоспособности и др.

Все это привело к необходимости установления правовых норм законодательством о борьбе с нелегальной занятостью, что нашло свое отражение в закреплении в Федеральном законе от 12 декабря 2023 года № 565-ФЗ «О занятости населения в Российской Федерации» главы 13, посвященной противодействию нелегальной занятости в России. Данная глава состоит из двух статей, в которых дается понятие нелегальной занятости, определяются полномочия Правительства РФ и органов власти всех уровней в данной сфере (ст. 66). Большое внимание уделяется созданию и деятельности межведомственных комиссий субъектов РФ по противодействию нелегальной занятости (ст. 67).

Как определяется в статье 67 закона, большую роль в работе межведомственной комиссии играют сведения и информация, которые они получают у налоговых органов (данные сведения составляют налоговую тайну, в связи с чем на них должны распространяться требования по работе с налоговой тайной). Очевидно, что налоговые органы обладают максимальным объемом информации, на основании которой может быть сделан вывод о признаках нелегальной занятости. Ведь именно эти признаки ложатся в основу доначисления НДС и страховых взносов тем компаниями, которые работают с самозанятыми – плательщиками налога на профессиональный доход.

Какие именно сведения и информация должны передаваться в межведомственные комиссии было определено приказом Минтруда России от 2 февраля 2024 г. № 40н, который вступил в силу с 1 марта 2024 года. Данный приказ вызвал большой резонанс среди предпринимателей, работающих с самозанятыми лицами, поскольку определил ряд критериев, на которые будут обращать внимание, и которые, как следует, из запрашиваемых сведений, могут привести к вызову организации на межведомственную комиссию по нелегальной занятости.

В отличие от критериев, используемых налоговыми органами, которые на основе общих признаков трудового законодательства, позволяют разграничить трудовые и гражданско-правовые отношения в каждом конкретном случае, в приказе Минтруда установлены критерии, по которым у налоговых органов запрашиваются сведения. К числу такой информации относятся сведения о работе организации (ИП) более чем с десятью самозанятыми (независимо от того, являются ли они физическими лицами без статуса ИП, или зарегистрированы в качестве индивидуального предпринимателя), если они отвечают также таких критериям продолжительность работы с организацией более трех месяцев и среднемесячный доход которых более 20 тысяч рублей. Из данного положения следует, что все эти три критерия должны соблюдаться одновременно. Таким образом, если у компании, например, один-два самозанятых, то такие сведения подавать

не нужно. В то же время вызывает вопрос ситуация с крупными компаниями, которые работают с большим числом самозанятых индивидуальных предпринимателей, оказывающих компании услуги, выполняющих для них работы, имеющие признаки гражданско-правовых, а не трудовых отношений. Представляется, что в тех случаях, когда такой договор между компанией и самозанятым лицом не содержит никаких признаков трудовых отношений, он не должен рассматриваться как повод проверки использования нелегальной занятости, даже если таких самозанятых с компанией работает несколько. Это касается в том числе и тех случаев, когда такая работа носит особый характер и не совпадает с трудовой функцией работников, занятых по трудовому договору.

То есть предоставление таких сведений от налоговых органов межведомственным комиссиям по противодействию нелегальной занятости не должно автоматически делать такие организации виновными в использовании нелегальной занятости, а должно являться лишь основанием для дополнительной проверки на предмет подмены трудовых отношений, выявления признаков трудовых отношений. И только в этом случае в отношении таких компаний могут быть применены какие-то меры ответственности. В ином случае это противоречило бы самой сути предпринимательских отношений, когда компании и индивидуальные предприниматели вправе выбирать способ заключения ими договоров между собой.

Вопрос также вызывает пункт о необходимости предоставления информации о фактах нелегальной занятости на основании решения, принятых по результатам проведенных налоговых проверок. Остается не раскрытым вопрос, должна ли предоставляться информация, если решение еще не вступило в законную силу и пока находится в стадии обжалования налогоплательщиком. С другой стороны, еще до вынесения решения налоговый орган, как правило, уже обладает информацией, которая может являться основанием для вывода о нелегальной занятости, и которая может быть использована межведомственной комиссией.

Поскольку часть сведений, передаваемых налоговыми органами, может содержать налоговую тайну, необходимо рассмотреть, какие именно передаваемые сведения будут подпадать под режим налоговой тайны, и какие последствия в случае нарушения такого режима могут быть для лиц, входящих в состав межведомственной комиссии. Институту налоговой тайны в Налоговом кодексе РФ посвящена только статья 102, которая определяет перечень сведений, которые исключаются из налоговой тайны. Кроме того, устанавливаются особенности применения налоговой тайны к отдельным сведениям, а также случаи взаимодействия между налоговыми органами, органами государственной власти, органами местного самоуправления, другими лицами, на которые режим налоговой тайны будет распространяться. Данные нормы постоянно дополняются, что обусловлено широким информационным взаимодействием налоговых органов с иными органами власти и должностными лицами: в условиях цифровой трансформации происходит и трансформация института налоговой тайны [6; 7].

Следует сделать вывод, что не все сведения и информация, содержащиеся в приказе Минтруда России от 02.02.2024 № 40н, будут подпадать под режим налоговой тайны, например сведения об ИНН или нарушениях налогового законодательства, включая суммы задолженности и мерах ответственности за эти

нарушения. Все остальные сведения будут составлять режим налоговой тайны, а это значит, что лицам, которым это сведения передаются, обязаны соблюдать этот режим.

В практике встречаются случаи привлечения должностных лиц налоговых органов к уголовной ответственности по ст. 183 Уголовного кодекса РФ за незаконное получение или разглашение сведений, составляющих налоговую тайну. Например, передача третьим лицам сведений, содержащих налоговую тайну, из базы АИС «Налог-3», посредством мессенджера «WhatsApp» (Постановление Седьмого кассационного суда общей юрисдикции от 19.01.2023 № 77-540/2023).

В то же время п. 2 ст. 183 УК РФ предусматривает возможность привлечения к уголовной ответственности за незаконное разглашение или использование сведений, составляющих налоговую тайну, лица, которому такая информация стала известна по службе или работе. Так в состав межведомственной комиссии по противодействию нелегальной занятости в Волгоградской области, утвержденному постановлением Администрации Волгоградской обл. от 12.08.2024 № 469-п, включены семьдесят три человека, в том числе председатели областных комитетов, начальники отделов территориальных органов федеральных органов исполнительной власти, глав муниципальных образований и др. Следует предположить, что комиссия будет собираться в усеченном составе и не все из обозначенных лиц будут получать информацию по конкретному делу в отношении конкретного налогоплательщика. В то же время остается не ясным вопрос, по каким каналам связи будет передавать информация, как будет обеспечена сохранность данных, предоставляемых налоговым органом в межведомственную комиссию. Следует также предложить оповещать членов межведомственной комиссии и рабочих групп, которые в целях противодействия нелегальной занятости будут работать со сведениями, составляющими налоговую тайну, о рисках возможного разглашения таких сведений и привлечения к уголовной ответственности.

Исходя из структуры статьи 102 Налогового кодекса РФ необходимо внести в нее дополнения в части включения пункта о распространении норм Налогового кодекса РФ о налоговой тайне на информацию и сведения, которые передаются межведомственным комиссиям по противодействию нелегальной занятости. Проект Федерального закона № 533106-8, содержащий такие дополнения, был принят Государственной Думой РФ в первом чтении 29 мая 2024 года, после этого больше не рассматривался из-за необходимости корректировки ряда положений. При этом представляется необходимым принятие данного закона в ближайшее время, поскольку межведомственные комиссии уже начинают свою работу, сведения передаются, а это значит, что режим налоговой тайны может быть нарушен.

**Заключение.** По итогам исследования можно сделать следующий вывод. Увеличение числа самозанятых лиц, привело к тому, что их работа начала активно использоваться предпринимательским сообществом для подмены трудовых отношений, что ведет как к уменьшению собираемых налоговых и страховых взносов, так и необходимости защиты трудовых и социальных прав таких лиц. Налоговые органы, обладая большим объемом сведений и информации о самозанятых и компаниях, с которыми они работают, не только самостоятельно осу-

осуществляют налоговый контроль, но и предоставляют эти сведения органам, осуществляющим надзор за соблюдением трудового законодательства, а также вновь создаваемым межведомственным комиссиям по противодействию нелегальной занятости. При этом возникает ряд вопросов, как по содержанию предоставляемых сведений, так и по сохранению налоговой тайны теми лицами, которые будут работать с этими сведениями и информацией, что требует соответствующих дополнений в налоговом законодательстве.

### Список литературы

1. Employer's Supplemental Tax Guide (Supplement to Pub. 15, Employer's Tax Guide) [Электронный ресурс]. – URL: <https://www.irs.gov/charities-non-profits/exempt-organizations-independent-contractors-vs-employees>
2. Лютова О. И. ФНС России как цифровая платформа: особенности и перспективы правового регулирования // Современное общество и право. – 2023. – № 1(62). – С. 37–41.
3. Маслов К. В. Взаимодействие между налоговыми органами и органами, осуществляющими оперативно-розыскную деятельность, при обеспечении налоговой безопасности государства // Конституционализация оперативно-розыскной деятельности: Материалы международной научно-практической конференции, Омск, 4 октября 2021 года. – Омск: Омская академия Министерства внутренних дел Российской Федерации, 2022. – С. 76–80.
4. Миронова С. М. Налог на профессиональный доход – пять лет эксперимента: промежуточные итоги // Финансовое право. – 2023. – № 12. – С. 10–14.
5. Пономарева К. А. Налог на профессиональный доход: дискуссионные вопросы с точки зрения субъектного состава налогового режима / К. А. Пономарева, А. А. Батарин, С. Д. Шаталов // Вестник Московского университета. Серия 26: Государственный аудит. – 2024. – № 1. – С. 34–45.
6. Родыгина В.Е. Трансформация института налоговой тайны в условиях цифровой экономики: правовые аспекты // Финансовое право. – 2019. – № 10. – С. 20–24.
7. Цифровая экономика: актуальные направления правового регулирования: научно-практическое пособие / М. О. Дьяконова, А. А. Ефремов, О.А. Зайцев и др.; под ред. И. И. Кучерова, С. А. Сеницына. – Москва: ИЗиСП, НОРМА, 2022. – 376 с.

**С. П. Першин,**

кандидат экономических наук, доцент,  
Краснодарский университет Министерства внутренних дел Российской  
Федерации

## **ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ С УЧЕТОМ СТЕПЕНИ ОБЩЕСТВЕННОЙ ОПАСНОСТИ ДЕЯНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

**Аннотация.** Целью исследования являлась выработка направления разрешения сложных вопросов обеспечения экономической безопасности в условиях широкого применения цифровых технологий. На примере инструментов кредитования рассмотрено значение степени общественной опасности при реализации проверочных мероприятий, в том числе правоохранительными органами, в случаях неисполнения заемщиками принятых обязательств, рассмотрено соотношение характера и тяжести административного давления на хозяйственную среду и интересов соблюдения прав и свобод субъектов экономических отношений при стимулировании развития экономики. Предложено применение единой учетной системы, обеспечивающей пользователей информацией, необходимой для контроля и мониторинга экономической активности, предупреждения недобросовестного поведения вовлеченных в хозяйственные взаимоотношения лиц.

**Ключевые слова:** экономическая безопасность, правоохранительная система, кредитно-финансовая сфера, заем, цифровые технологии, искусственный интеллект, общественная опасность, единая учетная система, контроль

## **ENSURING ECONOMIC SECURITY, TAKING INTO ACCOUNT THE DEGREE OF PUBLIC DANGER OF THE ACT**

**Abstract.** The purpose of the study was to develop a direction for solving complex issues of ensuring economic security in the context of widespread use of digital technologies. Using the example of lending instruments, the importance of the degree of public danger in the implementation of verification measures, including by law enforcement agencies, in cases of non-fulfillment of obligations by borrowers, the relationship between the nature and severity of administrative pressure on the economic environment and the interests of respect for the rights and freedoms of subjects of economic relations in stimulating economic development is considered. It is proposed to use a unified accounting system that provides users with the information necessary to control and monitor economic activity, prevent unfair behavior of persons involved in business relationships.

**Keywords:** economic security, law enforcement system, credit and financial sphere, loan, digital technologies, artificial intelligence, public danger, unified accounting system, control

**Введение.** Обеспечение экономической безопасности остается актуальной задачей государства в суровых условиях новой экономической реальности, обусловленной массой факторов, прямо не связанных с обстоятельствами присущи-

ми теории рыночной экономики, напротив, политически мотивированные решения власти недружественных России государств побудили необходимость глобального перестроения деловых связей, направлений движения товаров, состав контрагентов, соответственно правил и обычаев делового оборота. Ситуация неминуемо сказывается на внутренней экономической конъюнктуре государства, создает вызовы на пути развития современных деловых отношений, основанных на цифровых технологиях, роста доли рынка услуг, значения и содержания информационных потоков. Обозначенные обстоятельства требуют соответствующего развития правовой системы и внутригосударственных деловых связей, адаптации правоохранительной системы к условиям цифровой и информационной трансформации социума. Неотъемлемым условием реализации мер государственного регулирования экономических отношений, остается оценка степени общественной опасности и обеспечение ее соответствия методикам и действиям государственного механизма. Неотъемлемым элементом технологии принятия управленческих решений государственными органами является механизм учета особенностей деловой культуры, отражающий реакцию всех участников экономических отношений на принимаемые меры государственного регулирования. В указанных обстоятельствах и с учетом сложности, многофакторной зависимости многих решений в области обеспечения экономической безопасности, процесс адаптации используемых приемов к изменяющимся условиям требует научной интерпретации. Значительные резервы вопросов безопасности видятся в использовании цифровых технологий в правоохранительной системе государства.

**Основная часть.** Рассмотрение вопросов обеспечения экономической безопасности в заданной тематике произведен на примере кредитных отношений. Рост спроса на банковские продукты, в том числе предоставление заемных средств на фоне повсеместного и обширного распространения цифровых технологий, доступность таких продуктов посредством мобильных устройств и удаленного доступа к сервисам кредитных организаций, монетизация работы так называемого искусственного интеллекта, обусловили применение технологии автоматизированного принятия решений об оказании услуги и ее характере. В частности, решение о предоставлении займа сегодня может приниматься без прямого, а то и вовсе в отсутствии, участия реального человека, кредитного менеджера. Программный комплекс получив заявку, рассмотрение осуществляет согласно установленному алгоритму, который технически производит сравнение заявленных данных и предоставленных потенциальным заемщиком сведений с имеющейся в распоряжении программы информации о личности заемщика, известных и вероятных рисках, кредитной истории, согласованности с заявленными направлениями и другими характеристиками использования средств, сроком и способом их получения, возврата, величиной и системой расчета и взимания платы за пользование, многими другими параметрами. Программой могут быть рассчитаны экономические показатели и оценено их значение в динамике, в том числе путем прогнозирования величины на весь период займа. Анализ может быть произведен технически путем сопоставления с нормативными значениями, ожидаемыми величинами, которые изначально закладываются в программный комплекс и нередко подвергаются корректировке в зависимости от изменения

экономической конъюнктуры и (или) иных решений менеджмента кредитной организации. Как итог заявитель имеет возможность посредством взаимодействия с кредитной организацией с применением специального программного продукта направить заявку на получение займа с указанием требуемой информации, получить одобрение заявки на основе решения, вынесенного алгоритмом программы и без участия кредитного инспектора. Обозначенная технология позволяет значительно расширить возможности банка по обслуживанию заявок клиентов и предоставлению им займа, увеличив объем предоставления услуг, охвата большего числа потенциальных клиентов. Эта возможность позволяет конкурировать на рынке за привлечение клиента, предоставляя ему возможности удобного обслуживания, снижения требований для принятия положительного решения о кредитовании. Очевидно, что сам факт применения указанного сервиса свидетельствует о его экономической целесообразности, когда выгода превышает возникающие риски невозврата заемных средств.

В рассматриваемой связи следует учесть характер хозяйственной конъюнктуры, определившей спрос на расширение банковского кредитования. Неопределенность в экономике, смена логистических траекторий, перечня контрагентов, значительные темпы инфляции с неблагоприятными прогнозами, стимулируют массовое потребление среди конечных покупателей, стремление скорее произвести инвестиции в ценности, способные сохранять и преумножать свою стоимость, обеспечить производство необходимым запасом мощностей и материально-производственных запасов на перспективу. Соответственно, наблюдается ажиотаж на рынке ликвидных активов, существенное превышение спроса над предложением, негативный эффект имеют большие государственные расходы, в том числе и прежде всего в социальную сферу и коммунальную инфраструктуру, не дающие сопоставимого возврата стоимости в виде добавленной стоимости. Внутреннее производство и импорт, а также темпы их наращивания не способны обеспечить стремительно возрастающий спрос, подогревая активность конечного потребителя, деятельности хозяйствующих субъектов. Значительное повышение ключевой ставки Центрального банка не приводит к ожидаемому эффекту. Несмотря на рост депозитов, расширение рынка ценных бумаг, наблюдается значительный и устойчивый спрос на ликвидность. Потребители кредитных продуктов готовы принимать повышенный риск, только бы использовать текущую ситуацию, возможно не столько в целях извлечения быстрых экономических выгод, сколько обеспечения себя необходимыми активами для дальнейшей работы под угрозой их удорожания и недоступности в будущем.

Неотъемлемым риском расширения кредитного портфеля, объема и широты охвата рынка заимствований, является неплатежеспособность заемщика. Классические подходы к принятию решений о предоставлении займа предусматривают работу по оценке вероятности возврата средств с учетом дохода займодавца, наличие имущества и обязательств, его кредитной истории, связей в деловых кругах и с недобросовестными контрагентами, также работу по анализу изменения имущественного и финансового положения. Значение придается цели займа, сроки, источники и порядок его возврата и уплаты процентов и платежей за пользование средствами. Кредитный инспектор, принимая решение о предо-

ставлении займа, берет на себя ответственность за реализацию взаимоотношений с клиентом в запланированном ключе, осуществляет мониторинг состояния расчетов в течение всего периода заимствования, принимает меры по предупреждению случаев невозможности внесения очередных платежей, утраты активов, приобретенных за счет предоставленных клиенту средств, имущества, переданного в обеспечение возврата займа. Заемщику, не имеющему должного обеспечения, поручительства, находящемуся в состоянии близком к неплатежеспособности, ведущему связанную с повышенным риском деятельность, имеющему низкие значения показателей финансовой устойчивости, соотношения собственных и привлеченных средств, высокую долю дебиторской или кредиторской задолженности, как правило, достаточно сложно убедить кредитного инспектора в способности рассчитаться по взятым на себя обязательствам в установленные сроки. Известны случаи мошеннических действий в сфере кредитования, когда заемщиком предоставляются заведомо ложные сведения о хозяйственной деятельности, своем имущественном и финансовом положении и другие, в целях получения кредитных средств, также случаи фиктивного и преднамеренного банкротства, совершаемые в целях избегания обязанности по возврату средств займодавцу.

Экономист кредитной организации рассчитывает маржу, экономическую выгоду от предоставления средств в больших масштабах, производит сопоставление величин с объемом средств, не возвращенных заемщиками, и, судя по темпам роста рынка кредитования, объема выданных заемных средств, такой анализ показывает на целесообразность политики кредитной организации в направлении расширения объема выдаваемых средств с высоким уровнем риска. Прием реализации таких решений является использование автоматизированных технологий, способных производить исследование большого объема информации и сигнализировать о возможности принятия положительного решения по заявлению потенциального заемщика без участия кредитного инспектора. Это не только сокращает затраты на содержание штата высококвалифицированных специалистов, но, прежде всего позволяет в ускоренном режиме обслужить большое количество клиентов, подавших заявление на получение займа.

Прозрачность механизма, алгоритма программного комплекса, принятия решения о выдаче займа, снижение условий и требований к заемщику, доступность и удобство средств взаимоотношений с кредитной организацией, безучастность реального специалиста в оценке платежеспособности заемщика и ее мониторинге, создают условия для злоупотребления заемщиком. Последний может предоставить недостоверные сведения, либо кредитование и вовсе осуществляется без необходимости документально подтверждать финансовую состоятельность, целевое использование заемных ресурсов. Неплатежеспособность заемщика оказывается установленной только по истечении значительного времени просрочки платежей, создавая возможность применения клиентом механизмов сокрытия активов и ценных в части платежеспособности обязательств, провоцировать банкротство и побег ответственных лиц о взаимоотношений с кредитором. Следовательно, видим некоторое соотношение между обстоятельствами экономической конъюнктуры, стимулирующей наращивание и упрощение про-

цедуры получения займа и злым умыслом заемщика, злоупотребляющим доверием, легко вводящим в заблуждение кредитора. Пресечение преступного умысла, связанного со злоупотреблением доверием и предоставлением недостоверных случаев, подчиняется установленному порядку и процессуальной практики привлечения лица к ответственности. Правоохранительный орган должен показать состав преступного деяния, в частности показать характер умысла подозреваемого и способ совершения недобросовестных действий. Это требует проведения проверочных мероприятий, в частности, неминуемо проведение документального исследования, направленного на анализ имущественного и финансового состояния заемщика, установление признаков недостоверности предоставленных сведений, определение направлений и характера использования полученных средств. Такая работа требует затрат труда специалистов, времени, многие проверочные мероприятия обусловлены границами прав и свобод физических и юридических лиц, защитой коммерческой, банковской, налоговой тайны, тенденциями законодателя по снижению административной, контрольной нагрузки на хозяйствующие субъекты, что снижает возможности быстрого реагирования на случаи неисполнения заемщиком своих обязательств. Эта работа неминуемо влечет задействование значительного ресурса правоохранительной системы. К тому же значительная масса из них оказывается в рамках гражданско-правовых отношений и влечет рассмотрение споров исключительно в судебном порядке. Уголовную перспективу имеют материалы дела, в которых определены установленные законом признаки преступного деяния. Случаи, когда действия заемщика имеют отдельные признаки правонарушения, но не отождествленные с преступлением, также которые не подтверждены в ходе проведения процессуальных действий, провоцируют стереотип недобросовестного поведения, создают иллюзию безнаказанности, безответственности, приводят к разрушению базовых основ института прав и свобод хозяйствующих субъектов и физических лиц в рыночных условиях. К примеру, когда заемщик, предоставив неполные и (или) искаженные сведения о своем имущественном положении и платежеспособности, в последующем не исполняет обязательства по возврату заемных средств, и при этом оказывается не привлеченным к ответственности в результате невозможности установления отдельных искомых обстоятельств, необходимых для квалификаций действий в соответствии с нормами уголовного права. Возникает ожидание от правоохранительной системы более решительных действия для пресечения подобных случаев, ускорение работы по проверке обстоятельств, связанных с неисполнением обязательств в сфере кредитования. Очевидно, что устное заявление искаженной величины своих доходов, с согласия кредитора без документального подтверждения, является способом ведения в заблуждение этого кредитора, злоупотребления доверием, но, как правило, не имеет уголовной перспективы в связи с тем, что сам кредитор согласился на значительный риск оказаться введенным в заблуждение, степень общественной опасности такого деяния по итогу оценивается как не достаточная для применения мер уголовной ответственности. Это сказывается на характеристике о общественной оценке уровня экономической безопасности. Усиление критериев оценки общественной опасности влечет значимые последствия в виде административного давления на хо-

зяйственную среду, затрагивает права и свободы участвующих субъектов, должно осуществляться с большой осторожностью, чтобы не привести к дисбалансу общественных отношений.

Обеспечение экономической безопасности строится на внимательной поддержке и актуализации соотношения оценок общественной опасности деяния с учетом их последствий и требований состояния, развития общественных отношений в области экономики в целом и отдельных ее сегментов. Важно не допустить чрезмерного давления на хозяйственные отношения, чтобы не препятствовать их становлению и развитию. В значительном количестве случаев анализ обстоятельств рассматриваемых сделок по предоставлению займа, проверочных материалов сводится к даче оценочного суждения, применяемая версия которого устанавливается в суде. Сложности процессуального разбирательства, обозначенные выше, а также неоднозначность восприятия одних и тех же событий участниками проверочных действий и ответственными лицами – сторонами сделок и представителями государственной правоохранительной системы, не способствуют разрешению исследуемых обстоятельств, связанных с применением развитых программных продуктов и мероприятий по расширению рынков кредитования, требуют поиска современного инструмента разрешения соотношения интересов участников хозяйственной среды.

Решению рассматриваемых сложностей, по мнению автора, призвано применение автоматизированных технологий в формате единой учетной системы [2]. Цифровые технологии привели к значительному преобразованию порядков документирования фактов хозяйственной жизни, накоплению, систематизации и группировке данных с построением требуемой пользователем системы отчетных показателей. Сегодня факты хозяйственной жизни, совершаемые, имевшие место быть в деятельности хозяйствующих субъектов и связанной с ней деятельностью физических лиц находят свое отражение в сложившемся множестве баз данных, информационных систем, начиная от продуктов автоматизации хозяйственного учета предприятий и домашних хозяйств, вплоть до государственных информационных систем, реестров, сервисов. Потребность в контроле за совершаемыми сделками и операциями заемщика со стороны займодавца, оценке и мониторинге его деловой активности, имущественного и финансового состояния, а также осуществлении контрольной и надзорной деятельности со стороны государственных органов за экономической конъюнктурой, создают потребность в формировании единого цифрового учетного пространства хозяйственной и экономически значимой деятельности, инструментарий которой мог бы в значительной степени обеспечить заинтересованных пользователей в информации, способной обеспечить предупреждение правонарушений в финансовой среде и дисциплине, ускорить проведение проверочных мероприятий. Так, качество процедуры принятия решения о предоставлении займа применяемым автоматизированным продуктом на основе технологии искусственного интеллекта в значительной степени возрастает с использованием сведений предлагаемой единой учетной системы. Значимое значение в этой связи принимает использование цифрового рубля, создающего возможности для контроля за движением предоставленного ресурса. При подаче заявления кредитору о предоставлении заемных средств заявитель может одновременно обозна-

чить согласие на обработку займодавцем информации, формируемой единой учетной системой и позволяющей осуществлять мониторинг использования средств, что, как видится, в значительной степени способно предупредить вероятность нарушения договорных обязательств. Деятельность заемщика становится прозрачной, его намерения осуществлять деятельность по обозначенным направлениям могут быть подтверждены автоматическим анализом движения денежных средств, прочими учтенными фактами его хозяйственной жизни. Правоохранительные органы получают широкие возможности для контроля за соблюдением законодательства в кредитно-финансовой сфере, на основе анализа учетных данных делать вывод о характеристиках состава преступления, проводить исследование в целях выявления его признаков [1]. Важной особенностью учетной системы становится упрощение доступа к учетным данным заинтересованных лиц в рамках отведенных законом полномочий и допусков, не усиление административного давления на хозяйственную среду, организация и функционирование автоматизированной системы, способной не только повысить степень экономической безопасности, но и предложить современные цифровые инструменты хозяйствования. Система способна предупредить искажение балансирующего соотношения между вмешательством в деловую среду правоохранительных органов, определением степени общественной опасности деяний ее субъектов и общественными интересами, уровнем адаптации общества к изменяющимся условиям практики обеспечения экономической безопасности.

**Заключение.** Современные цифровые технологии открывают широкие возможности для развития способов хозяйствования. В кредитно-финансовой сфере применение автоматизированного продукта по обслуживанию заявок на получения займа с использованием технологий искусственного интеллекта позволили значительно увеличить доступность, скорость и удобство взаимоотношений заявителя с кредитором, а, следовательно, расширить рынок сбыта услуг кредитования. Однако применение таких технологий актуализирует внимание к возникающим сложностям в оценке степени общественной опасности в случаях привлечения правоохранительной системы государства к разрешению конфликтов, связанных с неисполнением заемщиком своих обязательств. Возможности проведения проверочных мероприятий и реализация процессуальных полномочий ограничены ресурсами государственного механизма, сложившимся соотношением административного давления на экономическую среду, принятым обществом с уровнем прав и свобод физических и юридических лиц, деловой культурой, задающими основу для развития хозяйственных связей, доверия к субъектам экономических отношений. В целях решения задач обеспечения экономической безопасности в условиях адаптации правоохранительной системы к тенденциям использования цифровых технологий в экономике может служить внедрение единой учетной системы, построенной на базе принципов бухгалтерской науки и позволяющей обеспечить учетной информацией о фактах хозяйственной и иной деятельности, результатах ее автоматизированного анализа пользователей согласно установленным компетенциям и допуску. Это позволит в значительной степени предупредить недобросовестное поведение субъектов экономических отношений, не препятствуя развитию автоматизированных технологий в деловой практике.

### Список литературы

1. Першин С. П. Администрирование экономических отношений на основе инструментов учетной системы / С. П. Першин, Ю. И. Сигидов. – Краснодар: Кубанский государственный аграрный университет имени И. Т. Трубилина, 2018. – 237 с. – ISBN 978-5-91692-608-8. – EDN PNXCMJ.

2. Першин С. П. Предупреждение мошенничества с применением учетных цифровых технологий на примере долевого строительства // Инновационное развитие современной экономики: ключевые проблемы и направления их решения: Материалы международной научно-практической конференции, Краснодар, 5–7 декабря 2023 года. – Краснодар: Кубанский государственный аграрный университет имени И. Т. Трубилина, 2024. – С. 227-232. – EDN DRNSTF.

**К. А. Пономарева,**

доктор юридических наук, доцент,

Научно-исследовательский институт

Министерства финансов Российской Федерации

**А. О. Симонов,**

эксперт Центра налоговой политики,

Научно-исследовательский финансовый институт

Министерства финансов Российской Федерации,

аспирант факультета права,

Национальный исследовательский университет

«Высшая школа экономики»

### **О ПРАВОВОЙ ПРИРОДЕ ДОХОДОВ ПО ОПЕРАЦИЯМ С ЦИФРОВЫМИ ФИНАНСОВЫМИ АКТИВАМИ С ТОЧКИ ЗРЕНИЯ МЕЖДУНАРОДНОГО НАЛОГООБЛОЖЕНИЯ**

**Аннотация.** Разработка и совершенствование правил налогообложения цифровых финансовых активов представляются важными с точки зрения обеспечения налоговой безопасности государства в контексте ответов на вызовы цифровой экономики. В представленной актуальной статье рассмотрены варианты подходов к цифровым финансовым активам с точки зрения соглашений об избежании двойного налогообложения и предложены направления совершенствования налогового законодательства.

**Ключевые слова:** налоговое право, налоговая безопасность, новые вызовы, международное налогообложение, цифровая экономика, цифровые финансовые активы, налог на прибыль

Исследование выполнено за счет гранта Российского научного фонда № 23-78-10160, <https://rscf.ru/project/23-78-10160/>

## ON LEGAL NATURE OF INCOME FROM TRANSACTIONS WITH DIGITAL FINANCIAL ASSETS FROM THE POINT OF VIEW OF INTERNATIONAL TAXATION

**Abstract.** The development and improvement of rules of taxation of digital financial assets are important from the point of view of ensuring the tax security of the state in the context of responding to the challenges of the digital economy. The article considers options for approaches to digital financial assets from the point of view of double tax treaties and suggests ways to improve tax legislation.

**Keywords:** tax law, tax security, new challenges, international taxation, digital economy, digital financial assets, corporate income tax

The research was carried out at the expense of a grant of the Russian Science Foundation No 23-78-10160, <https://rscf.ru/project/23-78-10160/>

**Введение.** Развитие цифровых технологий приводит к появлению новых финансовых инструментов, среди которых особое место занимают цифровые финансовые активы (далее – ЦФА). В последние годы они привлекли внимание не только инвесторов и пользователей, специалистов [9] и самого законодателя. При этом в законодательстве и научных исследованиях подходы к налоговому регулированию ЦФА неоднозначны, что порождает правовую неопределенность [3]. По этой причине участники рынка сталкиваются с трудностями в понимании своих прав и обязанностей, а также в исполнении налоговых обязательств. С другой стороны, многие вопросы остаются открытыми и для государства из-за отсутствия правил налогового администрирования ряда активов. Во многом устранению неопределенности способствовало принятие Федерального закона от 14.07.2022 № 324-ФЗ «О внесении изменений в часть вторую Налогового кодекса Российской Федерации» [1]. Однако ряд вопросов остается неурегулированным.

**Основная часть.** Вопросы соответствия правил налогообложения цифровых финансовых активов статьям соглашений об избежание двойного налогообложения. В частности, нет четкого понимания, как квалифицировать доход по операциям с ЦФА для определения соответствующей статьи соглашений об избежание двойного налогообложения (далее – СИДН) между Россией и страной резидентства иностранной компании.

Для ответа на данный вопрос необходимо остановиться на правовой природе ЦФА. Это позволит разграничить доход по ЦФА и иные предложенные виды доходов.

Сравним их, например, с ценными бумагами. В связи с тем, что ЦФА не признаются ценными бумагами и квалифицируются в качестве обязательственных прав, то применение к ним правил налогообложения доходов от операций с ценными бумагами не представляется возможным. ЦФА лишь удостоверяют такие же права, как и акции и облигации, а также другие эмиссионные ценные бумаги. Несовпадение данных категорий проявляется не только в их природе, но и в содержании. ЦФА «расширяет возможности инвесторов финансового рынка,

позволяя "расщепление" такой совокупности. Право голоса по акции может быть передано обладателю ЦФА. При этом акционер остается субъектом корпоративного права и осуществляет право управления акционерным обществом» [4].

Подобное осуществление права он обязан производить исключительно с учетом мнения обладателя ЦФА, дающего акционеру обязательное для последнего указание о том, как именно он должен проголосовать на общем собрании.

Проводя параллель между ЦФА и возвратом займа (процентами), отметим следующее. Заемные отношения обладают характерными признаками, ключевым из которых является реальность. Другими словами, чтобы отношения были признаны заемными, лицо должно фактически передать денежные средства или иной актив в пользование и распоряжение другому лицу. Прочими признаками являются возвратность, срочность и платность. При этом платность не всегда является обязательным признаком, так как закон предполагает и беспроцентные займы.

Между тем приобретение ЦФА не обладает ни одним из признаков займа:

- отсутствует срочность. ЦФА может принадлежать лицу неограниченное время, в то время как заемные отношения требуют четкого определения срока возврата;

- отсутствует возвратность. ЦФА является активом, то есть взамен денежных средств лицо приобретает право требования.

Если квалифицировать приобретение ЦФА как заемные отношения, то в таком случае в качестве заемных отношений можно также квалифицировать и приобретение права требования по договору цессии, что юридически неверно.

- отсутствует платность. В данном случае при приобретении ЦФА лицо получает равноценный актив и при его реализации, даже в пользу эмитента, не должно уплачивать какие-либо дополнительные средства за период, пока такой актив ему принадлежал.

При этом квалифицировать доход от операций с ЦФА в качестве «иного дохода» (ст. 21 Модельной Конвенции ОЭСР в отношении налогов на доходы и капитал, далее – МК ОЭСР) [6] не представляется целесообразным. Статья 21 МК ОЭСР, по замечанию И. А. Хавановой, «распространяется на виды дохода, которые не рассматриваются в предыдущих статьях (например, алименты, доход от участия в лотерее, деривативы), а также доход из источников, которые в них не упомянуты (например, рента, выплачиваемая резидентом одного Договаривающегося государства за использование недвижимого имущества, расположенного в третьем государстве)» [5. С. 28]. Поскольку ст. 21 МК ОЭСР применяется по остаточному принципу, представляется, что модель учета ЦФА по этой статье создаст излишнюю правовую неопределенность, которая и без того осложняет регулирование ЦФА.

Также не представляется возможным утверждать, что для налогообложения ЦФА подошла бы ст. 22 МК ОЭСР (налоги на капитал), поскольку положения данной статьи применяются исключительно в отношении дохода на капитал. При этом источник такого дохода также ограничен и обозначен как доход от использования недвижимого имущества или движимого имущества, нахо-

дящегося на территории государства. Подобная позиция соответствует комментариями к ст. 22 МК ОЭСР: статья касается только налогов на капитал, за исключением налогов на имущество и наследства, а также на подарки и трансфертные пошлины. Налоги на капитал, к которым применяется данная статья, указаны в статье 2 [5].

Таким образом, формально действующие нормы СИДН не позволяют использовать механизмы зачета удержанного налога у источника. В данном случае, применяя национальное законодательство, можно предложить два варианта решения спорной ситуации:

- исключение подп. 9.2 п. 1 ст. 309 НК РФ из НК РФ и применение правил налогообложения по аналогии с договорами цессии;
- включение в текст НК РФ оговорки о том, что для целей налогообложения и применения СИДН операции с ЦФА будут квалифицироваться по аналогии с ценными бумагами в соответствии с положениями п. 4 и 5 ст. 13 МК ОЭСР (доход от прироста капитала).

Второй вариант видится предпочтительным с точки зрения защиты национальной фискальной базы и находит поддержку среди исследователей. Так, профессор Е. А. Суханов отмечает, что согласно ст. 4 Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [2] ЦФА, «подобно бездокументарным ценным бумагам, подлежат учету в информационной системе и существуют только в виде записей в ней, а поэтому и сделки с ними могут совершаться исключительно «через оператора обмена цифровых финансовых активов» и по правилам, согласованным с Банком России (ст. 10 и 11 названного Закона). Но указанные технологические обстоятельства никак не влияют ни на юридическую природу регулируемых отношений, ни на содержание соответствующим им имущественных (цифровых) прав» [6].

**Заключение.** В заключение отметим, что разработка и совершенствование правил налогообложения ЦФА представляются важными с точки зрения обеспечения налоговой безопасности государства в контексте ответов на вызовы цифровой экономики. В частности, действующее налоговое законодательство регулирует исключительно порядок налогообложения операций с ЦФА и УЦП для целей налога на прибыль организаций, налога на доходы физических лиц и НДС. Представленные предложения могут быть учтены при совершенствовании налогового законодательства.

### Список литературы

1. О внесении изменений в часть вторую Налогового кодекса Российской Федерации: Федеральный закон от 14.07.2022 № 324-ФЗ // СЗ РФ. – 2020. – № 31 (ч. I). – Ст. 5018.
2. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31 июля 2020 г. № 259-ФЗ // СЗ РФ. – 2022. – № 29 (ч. III). – Ст. 5291.

3. Пономарева К. А., Симонов А.О. Налогообложение операций с цифровыми финансовыми активами в контексте классических правил налогообложения // Правоприменение. – 2023. – Т. 7, № 4. – С. 35–44.
4. Абрамова Е.Н. Цифровой финансовый актив как цифровая ценная бумага // Гражданское право. – 2024. – № 1. – С. 10–3.
5. Хаванова И.А. «Иные доходы»: непростая логика статьи 21 налоговых конвенций // Финансовое право. – 2022. – № 12. – С. 27–29.
6. Суханов Е.А. О гражданско-правовой природе «цифрового имущества» // Вестник гражданского права. – 2021. – № 6. – С. 7–29.
7. Commentaries on the Articles of the Model Tax Convention. Art. 22 [Электронный ресурс]. – URL: [https://doi.org/10.1787/mtc\\_cond-2017-en](https://doi.org/10.1787/mtc_cond-2017-en)
8. Model Tax Convention on Income and on Capital: Condensed Version 2017, OECD Publishing [Электронный ресурс]. – URL: [https://doi.org/10.1787/mtc\\_cond-2017-en](https://doi.org/10.1787/mtc_cond-2017-en)
9. Перетолчин А.П. Генезис и перспективы развития правового регулирования цифровых финансовых активов в Российской Федерации. Journal of Digital Technologies and Law. 2023;1(3):752-774. <https://doi.org/10.21202/jdtl.2023.33>. EDN: hlhzbu

**Л. М. Файзрахманова,**

кандидат юридических наук, доцент,  
Казанский (Приволжский) федеральный университет  
Казанский инновационный университет  
имени В. Г. Тимирязова

## **ЦИФРОВЫЕ ТЕХНОЛОГИИ В НАЛОГОВОМ АДМИНИСТРИРОВАНИИ ГОСУДАРСТВ БРИКС**

**Аннотация.** В статье рассматриваются системы налогового администрирования стран БРИКС под влиянием цифровизации. Цифровая повестка входит в список приоритетных направлений работы БРИКС. Проанализирован механизм взаимодействия и сотрудничества между налоговыми администрациями государств БРИКС. Осуществлен анализ действующих цифровых систем ФНС РФ, ЮАР, интеллектуальной налоговой системы Китая на основе больших данных (Big Data) и искусственного интеллекта.

**Ключевые слова:** государства БРИКС, налоговое администрирование, налогообложение, налоговый орган, сотрудничество, цифровые технологии, цифровизация

## **DIGITAL TECHNOLOGIES IN THE TAX ADMINISTRATION OF THE BRICS COUNTRIES**

**Abstract.** The tax administration systems of the BRICS countries under the influence of digitalization are considered. The digital agenda is included in the list of priority areas of BRICS work. The tools of interaction and cooperation between the tax

administrations of the BRICS member states are considered. The analysis of the existing digital systems of the Federal Tax Service of Russia, South Africa, China's intelligent tax system based on big data and artificial intelligence is presented.

**Keywords:** BRICS states, tax administration, taxation, tax authority, cooperation, digital technologies, digitalization

**Введение.** Внедрение цифровых технологий в условиях промышленной трансформации всего миропорядка способствует эффективному функционированию экономики любого государства. Государства БРИКС выделяют развитие цифровой экономики и ИКТ среди приоритетов национального развития. Цифровая повестка в последние годы также входит в список приоритетных направлений работы БРИКС. В преддверии подготовки саммита БРИКС, запланированного на октябрь 2024 года в г. Казани исследование нынешних достижений и позиций стран-партнеров по этому вопросу приобретают особенную актуальность. Практически все сферы общественных отношений пронизаны цифровыми технологиями, в т. ч. финансовыми технологиями. Они являются инструментом, способствующим успешному регулированию финансовых правоотношений. Так, за последние 10 лет произошло активное внедрение цифровых технологий в налоговое и бюджетное администрирование, в систему финансового рынка, финансового мониторинга. Это привело к тому, что в юридической литературе финансовые технологии стали рассматриваться как объекты финансово-правового регулирования [6]. Цифровизация в целом оказала колоссальное влияние на принципы налогового права, трансформируя их [9. С. 163].

**Основная часть.** Наибольшей трансформации под воздействием применения цифровых технологий подверглась система налогового администрирования как в России, так и в других странах БРИКС. За годы существования этой организации между странами-участниками было подписано большое количество дипломатических документов, среди которых, в 2017 году Меморандум о сотрудничестве между налоговыми администрациями стран БРИКС. В соответствии с этим документом государства БРИКС должны создать механизм укрепления налогового потенциала (Capacity Building Mechanism) [5]. Однако начало было положено еще в г. Нью-Дели в 2013 году, когда была достигнута договоренность о расширении сотрудничества в сфере налогового администрирования [1. С. 69]. В последующем были предусмотрены ежегодные встречи руководителей и экспертов налоговых администраций государств-участников БРИКС на территории председательствующей страны. Также взаимодействие осуществлялось на площадках ОЭСР.

На прошлогодней встрече в ЮАР (г. Кейптаун) были выделены три основных блока сотрудничества налоговых администраций стран БРИКС:

- 1) проектная работа (кадровый потенциал, налоговые технологии и использование данных);
- 2) гуманитарная повестка;
- 3) стратегическое направление (создание постоянного налогового органа управления объединения стран БРИКС) [4].

В сентябре 2024 г. в Москве пройдет очередная встреча глав налоговых администраций и рабочих групп всех государств БРИКС. Основные векторы взаимодействия сторон направлены на обмен опытом и лучшими практиками в области налогового контроля и администрирования, а также повышения качества информационного обмена в целях налогообложения. По мнению руководителя Управления международного сотрудничества и валютного контроля ФНС России Е. Балта результатом этой встречи будет утверждение соглашения о налоговом механизме БРИКС с участием расширенного состава стран БРИКС, а также дальнейшее развитие коммуникаций между налоговыми администрациями.

Процесс интегрирования ФНС России и ее структурных подразделений в цифровую экономику начался более 15 лет назад. Налоговый орган один из первых среди органов исполнительной власти стал внедрять и широко использовать в своей деятельности цифровые технологии. В последующем этот процесс был стимулирован рядом важнейших правовых актов, таких как Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в РФ на 2017–2030 годы» [7], а также ежегодные планы действия ФНС России, утверждаемые министром финансов РФ.

В настоящее время на сайте ФНС России функционирует более 70 налоговых сервисов. На рисунке представлены основные сервисы. С каждым годом их количество увеличивается.



Основные сервисы ФНС России

Кроме этого на службе ФНС России множество высокотехнологических разработок, таких как АИС «Налог-3», «АСК НДС», ФГИС ЕРН, ЕГР ЗАГС [8].

Как и Россия, КНР активно внедряет различные цифровые технологии, цифровые платформы для повышения эффективности налогового администрирования. Например, в Китае внедрена система электронного инвойсинга или электронных счет-фактур.

С 2022 года в КНР осуществляется процесс создания интеллектуальной налоговой системы на основе больших данных (Big Data) и искусственного интеллекта. Это система называется Golden Tax IV. Подобно гигантскому рентгеновскому аппарату он способен сканировать и обрабатывать огромные объемы персональных и финансовых данных. Эта система дает возможность доступа к информации о юридических лицах, их руководителях для проверки налоговыми органами. В рамках данной системы сведения компаний, а также информация от их владельцев, кредитных организаций и различных регуляторов рынка будут связаны и доступны для проверки налоговыми органами [8; 9]. Налоговые органы интегрируются с другими государственными информационными системами для обмена данными и улучшения координации между различными ведомствами.

Следует отметить, что механизм налогового контроля в Китае имеет свою специфику в виде односторонней коррекции налоговых обязательств компании при выявлении фактов уклонения от уплаты обязательных платежей.

Система налогового декларирования в Китае очень схожа с Россией, поскольку порядка 99 % налоговых деклараций подается онлайн. Благодаря цифровизации и оптимизации администрирования, в основу взаимодействия между налоговыми органами и частно-правовыми субъектами налоговых отношений положен принцип бесконтактной работы. Расширился также спектр доступных бесконтактных услуг, включая пилотные функции, такие как «интеллектуальное предварительное заполнение» для возмещения НДС и «бесплатное заполнение и отчетность» для льгот по экспортному НДС [7]. Такие механизмы позволяют упростить процедуру сдачи отчетности и повышают уровень комплаенс организаций.

Современная финансово-правовая повестка Китая получила новый импульс в виде успешной пилотной программы по внедрению цифрового юаня для уплаты налогов. Так, благодаря цифровой платформе юаньминби, за пять месяцев 2024 г. была осуществлена оплата около 12 тыс. налогов на сумму 25,9 млрд юаней [3].

Таким образом, повсеместное внедрение цифровых технологий в КНР способствует повышению эффективности, прозрачности и доступности налогового администрирования.

Южная Африка 24 августа 2023 года дала новый импульс налоговой политики, представив Руководство по программе добровольного раскрытия информации (VDP), разработанное Службой доходов Южной Африки (SARS). Эти директивы призваны улучшить систему налогового соблюдения в стране и обеспечить более эффективное использование ресурсов SARS.

Плательщики налогов, которые могут участвовать в VDP (после заключения соответствующего соглашения), получают определенную льготу по штрафным санкциям за скрывание сведений в сторону занижения, административным штрафным санкциям, преследованию в рамках уголовного законодательства относительно действительного раскрытия данных на добровольной основе и подписания такого соглашения.

**Заключение.** Таким образом, происходящие глобальные изменения инновационного характера в странах БРИКС, плодотворное сотрудничество, обмен опытом и лучшими практиками в области налогового контроля между налоговыми администрациями этих государств способствуют эффективному сбору налогов, улучшению обслуживания граждан и повышения доверия к системе налогообложения. Кроме того, система международного налогообложения становится более прозрачной, справедливой и определенной, оставляя все меньше места для ухода от налогообложения.

### Список литературы

1. Арзуманова Л. Л. Налоговое взаимодействие государств БРИКС в современных условиях // Актуальные проблемы российского права. 2018. – № 3(88). – С. 69.
2. Беглярова Н. Как происходит налоговое администрирование в Китае [Электронный ресурс]. – URL: <https://companies.rbc.ru/news/REuTgSxpGg/kak-proishodit-nalogovoe-dministrirovanie-v-kitae/>
3. Уплата налога в цифровом юане / block-chain2. 2024. 14 июня [Электронный ресурс]. – URL: <https://www.block-chain24.com/news/novosti-cbdc/gosudarstvennaya-nalogovaya-administraciya-v-kitae-zapuskaet-proekt-po-uplate>
4. Налоговое администрирование в БРИКС / Сайт ФНС России [Электронный ресурс]. – URL: <https://www.nalog.gov.ru/rn77/news/smi/15074409/>
5. Меморандум о сотрудничестве [Электронный ресурс]. – URL: [https://www.nalog.gov.ru/rn77/news/international\\_activities/6950260/](https://www.nalog.gov.ru/rn77/news/international_activities/6950260/)
6. Правовое регулирование применения финансовых технологий. Монография / Под ред. Е. Ю. Грачевой. – М.: Проспект, 2023. С.48–62.
7. О Стратегии развития информационного общества в РФ на 2017–2030 г.: УП РФ от 09.05.2017 № 203 // СПС «КонсультантПлюс». – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_216363/](https://www.consultant.ru/document/cons_doc_LAW_216363/)
8. Golden Tax IV Интеллектуальная налоговая система [Электронный ресурс]. – URL: <https://www.tadviser.ru/index.php>
9. Лютова О.И. Цифровая трансформация принципов налогового права. Journal of Digital Technologies and Law. 2024;2(1):163–180. <https://doi.org/10.21202/jdtl.2024.9>. EDN: zuaihn