

№ 6 (142)
2026

ВЕСТНИК УНИВЕРСИТЕТА

имени О.Е. Кутафина (МГЮА)

Право есть
искусство добра
и справедливости

*Jus est ars
boni et aequi*

В номере

Выпуск ИНФОРМАЦИОННОЕ ПРАВО И ЦИФРОВАЯ РЕАЛЬНОСТЬ

ВЕКТОР ЮРИДИЧЕСКОЙ НАУКИ

- 23** Минбалеев А. В.
Формирование правовых условий
для благоприятного развития
искусственного интеллекта в России
- 31** Добробаба М. Б.
Применение технологий искусственного
интеллекта в контрольно-надзорной
деятельности: проблемы и перспективы
правового регулирования
- 63** Ефремов А. А.
Развитие правового регулирования рынка
данных в России: проблемы и перспективы
- 95** Полякова Т. А., Троян Н. А.
Инструменты инновационной политики
государства в обеспечении национального
суверенитета в условиях цифровой
трансформации в Российской Федерации
- 112** Камалова Г. Г.
Проблемы правового обеспечения
доверия и информационной безопасности
в цифровую эпоху

№ 6 (142)
2026

ВЕСТНИК УНИВЕРСИТЕТА имени О.Е. Кутафина (МГЮА)

Выпуск

**ИНФОРМАЦИОННОЕ ПРАВО
И ЦИФРОВАЯ РЕАЛЬНОСТЬ**

Издается с 2014 года
Выходит один раз в месяц

Председатель редакционного совета:

БЛАЖЕЕВ Виктор Владимирович — ректор Университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук, профессор, г. Москва, Россия

Заместитель председателя редакционного совета:

ГРАЧЕВА Елена Юрьевна — заведующий кафедрой финансового права Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

Главный редактор:

ШПАКОВСКИЙ Юрий Григорьевич — профессор кафедры экологического и природоресурсного права Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

Ответственный секретарь:

БУЛЫЧЕВ Евгений Геннадьевич — начальник отдела научно-издательской политики Научно-исследовательского института Университета имени О.Е. Кутафина (МГЮА), г. Москва, Россия

Редакционный совет:

АФАНАСЬЕВ Сергей Федорович — заведующий кафедрой арбитражного процесса, адвокатуры и нотариата Саратовской государственной юридической академии, доктор юридических наук, профессор, г. Саратов, Россия

БИРЮКОВ Павел Николаевич — заведующий кафедрой международного и евразийского права Воронежского государственного университета, доктор юридических наук, профессор, г. Воронеж, Россия

БУКАЛЕРОВА Людмила Александровна — проректор Российского университета адвокатуры и нотариата имени Г.Б. Мирзоева, доктор юридических наук, профессор, г. Москва, Россия

ВОЛКОВ Геннадий Александрович — профессор кафедры экологического и земельного права юридического факультета Московского государственного университета имени М.В. Ломоносова, доктор юридических наук, г. Москва, Россия

ДЮФЛО Ален — эксперт-практик международного класса в области права, основатель адвокатского бюро «Дюфло и партнеры», преподаватель Университета Лион III имени Жана Мулена, г. Лион, Франция

ЕГОРОВА Мария Александровна — профессор кафедры конкурентного права, помощник проректора по научно-исследовательской деятельности Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

ЕРШОВА Инна Владимировна — первый проректор Университета имени О.Е. Кутафина (МГЮА), заведующий кафедрой предпринимательского и корпоративного права, доктор юридических наук, профессор, г. Москва, Россия

ЕФИМОВА Людмила Георгиевна — заведующий кафедрой банковского права Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

ЖАВОРОНКОВА Наталья Григорьевна — доктор юридических наук, профессор, г. Москва, Россия

ЗРАЖЕВСКАЯ Татьяна Дмитриевна — профессор кафедры конституционного и муниципального права Воронежского государственного университета, Уполномоченный по правам человека в Воронежской области, доктор юридических наук, профессор, г. Воронеж, Россия

ЗУБАРЕВ Сергей Михайлович — заведующий кафедрой административного права и процесса имени Л.Л. Попова Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

ИЩЕНКО Евгений Петрович — профессор кафедры криминалистики Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

ИЩЕНКО Нина Сергеевна — заведующий кафедрой правоведения Гомельского филиала Международного университета «МИТСО», кандидат юридических наук, профессор, г. Гомель, Республика Беларусь

КИСЕЛЕВ Сергей Георгиевич — профессор Института права и национальной безопасности РАНХиГС при Президенте Российской Федерации, профессор Института международных отношений и социально-политических наук Московского государственного лингвистического университета, доктор философских наук, профессор, г. Москва, Россия



Журнал рекомендован Высшей аттестационной комиссией Министерства науки и высшего образования РФ для публикации основных результатов диссертаций на соискание ученой степени доктора и кандидата наук.
Материалы журнала включены в систему Российского индекса научного цитирования.

© Университет имени О.Е. Кутафина (МГЮА), 2026

6/2026

КОМАРОВА Валентина Викторовна — профессор кафедры конституционного и муниципального права Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

ЛАПИНА Марина Афанасьевна — профессор Департамента правового регулирования экономической деятельности Финансового университета при Правительстве Российской Федерации, доктор юридических наук, г. Москва, Россия

МИРОШНИЧЕНКО Владимир Михайлович — ректор Академии безопасности и специальных программ, доктор экономических наук, профессор, г. Москва, Россия

НИКИТИН Сергей Васильевич — заведующий кафедрой гражданского и административного судопроизводства Российского государственного университета правосудия имени В.М. Лебедева, доктор юридических наук, профессор, г. Москва, Россия

НОВОСЕЛОВА Людмила Александровна — заведующий кафедрой интеллектуальных прав Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

ПЛЮЩИКОВ Вадим Геннадьевич — директор Аграрно-технологического института Российского университета дружбы народов, доктор сельскохозяйственных наук, профессор, г. Москва, Россия

РАССОЛОВ Илья Михайлович — профессор кафедры информационного права и цифровых технологий Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, доцент, г. Москва, Россия

РОЗА Фабрис — профессор кафедры трудового права Университета Реймс Шампань-Арденны, Франция

РОССИНСКАЯ Елена Рафаиловна — заведующий кафедрой судебных экспертиз Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

РЫЛЬСКАЯ Марина Александровна — директор Института проблем эффективного государства и гражданского общества Фи-

нансового университета при Правительстве Российской Федерации, доктор юридических наук, доцент, г. Москва, Россия

СИНЮКОВ Владимир Николаевич — проректор по научно-исследовательской деятельности Университета имени О.Е. Кутафина (МГЮА), профессор кафедры теории государства и права, доктор юридических наук, профессор, г. Москва, Россия

СОКОЛОВА Наталья Александровна — заведующий кафедрой международного права, научный руководитель Научно-исследовательского института Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

УСТЮКОВА Валентина Владимировна — и. о. заведующего сектором экологического, земельного и аграрного права Института государства и права РАН, доктор юридических наук, профессор, г. Москва, Россия

ЦАЙ ЦЗЮНЬ — директор Юридического института Хэнаньского университета, доктор юридических наук, профессор, г. Кайфэн, КНР

ЦОПАНОВА Индира Георгиевна — декан юридического факультета Российской таможенной академии, кандидат юридических наук, доцент, г. Москва, Россия

ШИЛЬСТЕЙН Давид — профессор права, заведующий кафедрой уголовного права Университета Париж 1 Пантеон-Сорбонна, г. Париж, Франция

ЩЕГОЛЕВ Виталий Валентинович — проректор Московского гуманитарно-экономического университета по научной работе и международному сотрудничеству, доктор политических наук, г. Москва, Россия

Ответственный редактор выпуска:

МИНБАЛЕЕВ Алексей Владимирович — заведующий кафедрой информационного права и цифровых технологий Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор

В журнале публикуются статьи по научным специальностям группы 5.1 «Право» (юридические науки)	5.1.1. Теоретико-исторические правовые науки. 5.1.2. Публично-правовые (государственно-правовые) науки. 5.1.3. Частно-правовые (цивилистические) науки. 5.1.4. Уголовно-правовые науки. 5.1.5. Международно-правовые науки.
РЕГИСТРАЦИЯ СМИ	Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) ПИ № ФС77-67361 от 5 октября 2016 г.
ISSN	2311-5998 (Print), 2782-6163 (Online)
ПЕРИОДИЧНОСТЬ	12 раз в год
УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ	Федеральное государственное автономное образовательное учреждение высшего образования «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)» Садовая-Кудринская ул., д. 9, стр. 1, вн. тер. г. муниципальный округ Пресненский, г. Москва, Россия, 123242
АДРЕС РЕДАКЦИИ	Садовая-Кудринская ул., д. 9, стр. 2, г. Москва, Россия, 125993 Тел.: 8 (499) 244-88-88 (доб. 687). E-mail: vestnik@msal.ru
ПОДПИСКА И РАСПРОСТРАНЕНИЕ	Свободная цена Журнал распространяется через объединенный каталог «Пресса России» и интернет-каталог агентства «Книга-Сервис» Подписной индекс 40650. Подписка на журнал возможна с любого месяца
ТИПОГРАФИЯ	Отпечатано в Издательском центре Университета имени О.Е. Кутафина (МГЮА) Садовая-Кудринская ул., д. 9, стр. 2, г. Москва, Россия, 125993
ВЫПУСКНЫЕ ДАННЫЕ	Дата выхода в свет: 01.09.2026 Объем 22,79 усл. печ. л. (14,06 а. л.), формат 84×108/16 Тираж 150 экз. Печать цифровая. Бумага офсетная

При использовании опубликованных материалов журнала ссылка на «Вестник Университета имени О.Е. Кутафина (МГЮА)» обязательна. Перепечатка допускается только по согласованию с редакцией. Точка зрения редакции не всегда совпадает с точкой зрения авторов публикаций.

Редактор Л. А. Мункуева

Корректор С. И. Ершова

Компьютерная верстка Д. А. Беляков

**№ 6 (142)
2026**

COURIER

OF THE KUTAFIN MOSCOW STATE LAW UNIVERSITY (MSAL)

Edition
**INFORMATION LAW
AND DIGITAL REALITY**

**Published from the year of 2014
Monthly journal**

Chairperson of the Council of Editors:

BLAZHEEV Victor Vladimirovich — Rector of Kutafin Moscow State Law University (MSAL), Cand. Sci. (Law), Professor, Moscow, Russia

Vice-Chairperson of the Council of Editors:

GRACHEVA Elena Yurievna — Head of the Department of Financial Law of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

Chief Editor:

SHPAKOVSKIY Yuriy Grigorievich — Professor of the Department of Environmental and Natural Resources Law of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

Executive Secretary Editor:

BULYCHEV Evgeniy Gennadievich — Head of the Research and Publishing Policy Department of the Research Institute of Kutafin Moscow State Law University (MSAL), Moscow, Russia

Council of editors:

AFANASIEV Sergey Fedorovich — Head of the Department of Arbitrazh Procedure, Advocacy and Notary of Saratov State Academy of Law, Dr. Sci. (Law), Professor, Saratov, Russia

BIRIUKOV Pavel Nikolaevich — Head of the Department of International and Eurasian Law of Voronezh State University, Doctor of Law, Professor, Voronezh, Russia

BUKALEROVA Ludmila Alexandrovna — Vice-Rector, Russian University of Advocacy and Notary named after G.B. Mirzoev (RUAN), Dr. Sci. (Law), Professor, Moscow, Russia

VOLKOV Gennadiy Aleksandrovich — Professor of the Department of Environmental and Land Law of the Faculty of Law of Lomonosov Moscow State University, Dr. Sci. (Law), Moscow, Russia

DUFLOT Alain — an expert practitioner in the field of law, founder of the law firm «Dufлот & Partners», Lecturer at the Jean Moulin Lyon 3 University, Lyon, France

EGOROVA Maria Alexandrovna — Professor of the Department of Competition Law, Assistant of Vice-Rector for Research of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

ERSHOVA Inna Vladimirovna — First Vice-Rector of Kutafin Moscow State Law University (MSAL), Head of the Department of Business and Corporate Law, Dr. Sci. (Law), Professor, Moscow, Russia

EFIMOVA Lyudmila Georgievna — Head of the Department of Banking Law of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

ZHAVORONKOVA Natalya Grigorevna — Dr. Sci. (Law), Professor, Moscow, Russia

ZRAZHEVSKAYA Tatyana Dmitrievna — Professor of the Department of Constitutional and Municipal Law of Voronezh State University, Commissioner for Human Rights in the Voronezh Region, Dr. Sci. (Law), Professor, Voronezh, Russia

ZUBAREV Sergey Mikhailovich — Head of the Department of Administrative Law and Procedure named after L.L. Popov of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

ISHCHENKO Evgeniy Petrovich — Head of the Department of Criminalistics of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

ISHCHENKO Nina Sergeevna — PhD in Law, Professor, Head of the Department of Jurisprudence of the Gomel Branch of the International University «MITSO», Gomel, Republic of Belarus

KISELEV Sergey Georgievich — Professor, Institute of Law and National Security, RANEPA University; Professor, Institute of International Relations and Socio-Political Sciences, Moscow State Linguistic University, Dr. Sci. (Philosophy), Professor, Moscow, Russia

KOMAROVA Valentina Viktorovna — Professor of the Department of Constitutional and Municipal Law of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

Recommended by the Higher Attestation Commission of the Ministry of Science and Higher Education of the Russian Federation for publication of results of doctoral theses.
Materials included in the journal Russian Science Citation Index.



© Kutafin Moscow State Law University (MSAL), 2026

LAPINA Marina Afanasyeva — Professor of the Department of Legal Regulation of Economic Activity of the Financial University under the Government of the Russia, Dr. Sci. (Law), Moscow, Russia

MIROSHNICHENKO Vladimir Mikhailovich — Rector of the Academy of Security and Special Programs, Dr. Sci. (Economics), Professor, Moscow, Russia

NIKITIN Sergey Vasilyevich — Head of the Department of Civil and Administrative Court Proceedings of the Lebedev Russian State University of Justice, Dr. Sci. (Law), Professor, Moscow, Russia

NOVOSELOVA Lyudmila Alexandrovna — Head of the Department of Intellectual Property Law of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

PLYUSHCHIKOV Vadim Gennadyevich — Director of Agrarian and Technological Institute of the Peoples' Friendship University of Russia, Dr. Sci. (Agr. Sc.), Professor, Moscow, Russia

RASSOLOV Ilya Mikhailovich — Professor of the Department of Information Law and Digital Technologies of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Associate Professor, Moscow, Russia

ROSA Fabrice — Professor of the Department of Labour Law at the University of Reims Champagne-Ardenne, France

ROSSINSKAYA Elena Rafailovna — Head of the Department of Forensic Examination of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

RYLSKAYA Marina Alexandrovna — Director of the Institute of Problems of the Efficient State and Civil Society of the Financial University under the Government of the Russia, Dr. Sci. (Law), Associate Professor, Moscow, Russia

SINYUKOV Vladimir Nikolaevich — Vice-Rector for Research of Kutafin Moscow State Law University (MSAL), Professor of the Department of Theory of the State and Law, Dr. Sci. (Law), Professor, Moscow, Russia

SOKOLOVA Natalya Alexandrovna — Head of the Department of International Law, Academic Director of the Research Institute of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

USTYUKOVA Valentina Vladimirovna — Acting Head of the Sector of Environmental, Land and Agricultural Law of the Institute of the State and Law of the RAS, Dr. Sci. (Law), Professor, Moscow, Russia

TSAY TSZYUN — Director of the Law Institute of Henan University, Dr. Sci. (Law), Professor, Kaifen, the PRC

TSOPANOVA Indira Georgievna — Dean of the Law Faculty of the Russian Customs Academy, Cand. Sci. (Law), Associate Professor, Moscow, Russia

CHILSTEIN David — Professor of Law, Head of the Department of Criminal Law at the University of Paris 1 Pantheon-Sorbonne, Paris, France

SHCHEGOLEV Vitaliy Valentinovich — Vice-Rector for Research and International Cooperation of the Moscow University of Humanities and Economics, Dr. Sci. (Political Sciences), Moscow, Russia

Editor-in-Chief of the issue:

MINBALEEV Alexey Vladimirovich — Head of the Department of Information Law and Digital Technologies of the Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor

The Journal publishes research papers written on scientific specialties of Group 5.1 «Law» (Legal Sciences)	5.1.1. Theory and History of Law. 5.1.2. Public Law and State Law. 5.1.3. Private Law (Civil Law). 5.1.4. Criminal Law. 5.1.5. International Law.
THE CERTIFICATE OF MASS MEDIA REGISTRATION	The journal was registered by the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) on 5 October 2016. The Certificate of Mass Media Registration: PI No. FS77-67361
ISSN	2311-5998 (Print), 2782-6163 (Online)
PUBLICATION FREQUENCY	12 issues per year
FOUNDER AND PUBLISHER	Federal State Autonomous Educational Institution of Higher Education "Kutafin Moscow State Law University (MSAL)" Sadovaya-Kudrinskaya ul., d. 9, str. 1, Presnensky intra-urb. ter. municipal district, Moscow, Russia, 123242
EDITORIAL OFFICE. POSTAL ADDRESS	Sadovaya-Kudrinskaya ul., d. 9, str. 2, Moscow, Russia, 125993 Tel.: +7 (499) 244-88-88 (ext. 687) E-mail: vestnik@msal.ru
SUBSCRIPTION AND DISTRIBUTION	Free price The journal is distributed through "Press of Russia" joint catalogue and the Internet catalogue of "Kniga-Servis" Agency Subscription index: 40650. Journal subscription is possible from any month
PRINTING HOUSE	Printed in Publishing Center of Kutafin Moscow State Law University (MSAL) Sadovaya-Kudrinskaya ul., d. 9, str. 2, Moscow, Russia, 125993
SIGNED FOR PRINTING	01.09.2026 Volume: 22,79 conventional printer's sheets (14,06 author's sheets). Format: 84×108/16. An edition of 150 copies. Digital printing. Offset paper
<i>When using published materials of the journal, reference to "Courier of the Kutafin Moscow State Law University (MSAL)" is obligatory. Full or partial use of materials is allowed only with the written permission of the authors or editors. The point of view of the Editorial Board may not coincide with the point of view of the authors of publications.</i>	
Editor L. A. Munkueva	Proof-reader S. I. Ershova
Computer layout D. A. Belyakov	

СОДЕРЖАНИЕ

СЛОВО К ЧИТАТЕЛЮ	8
УНИВЕРСИТЕТСКАЯ ХРОНИКА	10
ВЕКТОР ЮРИДИЧЕСКОЙ НАУКИ	
Право искусственного интеллекта	
Минбалеев А. В. Формирование правовых условий для благоприятного развития искусственного интеллекта в России	23
Добробаба М. Б. Применение технологий искусственного интеллекта в контрольно-надзорной деятельности: проблемы и перспективы правового регулирования	31
Соловкин С. В. Генеративный искусственный интеллект как инструмент манипуляции: правовые вызовы и пределы регулирования	40
Сушкова О. В. Этические и юридические предпосылки использования искусственного интеллекта субъектами предпринимательской и профессиональной деятельности	47
Титов А. С. Система правовых и иных средств обеспечения применения искусственного интеллекта в сфере воздушного транспорта	55
Правовой режим цифровых данных	
Ефремов А. А. Развитие правового регулирования рынка данных в России: проблемы и перспективы	63
Бундин М. В. Цель обработки персональных данных: теоретические и практические правовые аспекты	70
Ло Имин Развитие правового регулирования применения больших данных в цифровой экономике Китая	78
Химченко А. И. К вопросу о роли данных в обеспечении доверенного функционирования систем искусственного интеллекта	86
Обеспечение суверенитета в киберпространстве	
Полякова Т. А., Троян Н. А. Инструменты инновационной политики государства в обеспечении национального суверенитета в условиях цифровой трансформации в Российской Федерации	95
Гимадрисламова О. Р. Многоуровневая правовая модель доступа к информации в цифровой среде	104

Правовое обеспечение кибербезопасности

Камалова Г. Г.

Проблемы правового обеспечения доверия
и информационной безопасности в цифровую эпоху 112

Золотеева З. Т.

Обеспечение кибербезопасности в государствах
Южного Кавказа: сравнительно-правовой анализ 120

Таран К. К.

Цифровой профиль: правовые проблемы
и вопросы кибербезопасности 128

Лесников П. А.

Административно-правовые аспекты обеспечения
кибербезопасности в цифровой таможенной инфраструктуре 136

Образование и права человека в условиях цифровизации общества

Абдусаламов Р. А.

Публично-правовое обеспечение цифровой трансформации
высшего образования в Российской Федерации 144

Пашнина Т. В.

К вопросу о «новых» правах человека
в контексте цифрового конституционализма 153

НАУЧНЫЙ ПОИСК

Сорокина Е. А.

Моральные императивы в праве ЮАР:
концепция Ubuntu и конституционные вызовы 161

Платицына И. С., Шпаковский Ю. Г.

Искусственный интеллект: экономические и правовые аспекты
инноваций в эпоху цифровой трансформации Большой Евразии 170

Трибуна молодого ученого

Никишина А. В.

Семейные ценности в цифровой среде:
проблемы и гарантии правовой защиты 181

Носова В. А.

Публично-правовое стимулирование развития отрасли
информационных технологий как инструмент
обеспечения технологического суверенитета 190

Рыжков Д. И.

Нормативные подходы к правовому регулированию
городов будущего: от умных счетчиков к умным домам 197

НАУЧНОЕ НАСЛЕДИЕ

Тьюринг А. М.

Вычислительная техника и интеллект (на англ. языке) 206

ПОСТСКРИПТУМ

Шпаковский Ю. Г.

Познавательство о разном 212

CONTENTS

NOTE TO THE READERS	8
UNIVERSITY CHRONICLE	10
VECTOR OF LEGAL SCIENCE	
Artificial Intelligence Law	
Minbaleev A. V. Formation of Legal Conditions for the Favorable Development of Artificial Intelligence in Russia	23
Dobrobaba M. B. The Use of Artificial Intelligence Technologies in Control and Supervision: Challenges and Prospects for Legal Regulation	31
Solovkin S. V. Generative Artificial Intelligence as a Tool of Manipulation: Legal Challenges and the Limits of Regulation	40
Sushkova O. V. Ethical and Legal Prerequisites for the Use of Artificial Intelligence by Business and Professional Entities	47
Titov A. S. System of Legal and other Means of Ensuring the Use of Artificial Intelligence in the Air Transport Sector	55
Legal Regime of Digital Data	
Yefremov A. A. Development of Legal Regulation of the Data Market in Russia: Problems and Prospects	63
Bundin M. V. The Purpose of Processing Personal Data: Theoretical and Practical Legal Aspects	70
Luo Yiming Development of Legal Regulation of the Use of Big Data in China's Digital Economy	78
Khimchenko A. I. On the Issue of Trustworthy Functioning of Artificial Intelligence Systems and the Role of Data	86
Securing Sovereignty in Cyberspace	
Polyakova T. A., Troyan N. A. Instruments of State Innovation Policy to Ensuring National Sovereignty in the Context of Digital Transformation in the Russian Federation	95
Gimadrislamova O. R. Multilevel Legal Model of Access to Information in the Digital Environment	104

Legal Framework for Cybersecurity

Kamalova G. G.

- Problems of Legal Assurance of Trust
and Information Security in the Digital Age 112

Zoloeva Z. T.

- Ensuring Cybersecurity in the South Caucasus States:
a Comparative Legal Analysis 120

Taran K. K.

- Digital Profile, Legal and Cybersecurity Issues 128

Lesnikov P. A.

- Administrative and Legal Aspects of Cybersecurity
in Digital Customs Infrastructure 136

Education and Human Rights in the Context of Digitalization

Abdusalamov R. A.

- Public Legal Support for the Digital Transformation
of Higher Education in the Russian Federation 144

Pashnina T. V.

- On the Issue of «New» Human Rights
in the Context of Digital Constitutionalism 153

SCIENTIFIC RESEARCH

Sorokina E. A.

- Moral Imperatives in South African Law:
The Concept of Ubuntu and Constitutional Challenges 161

Platitsyna I. S., Shpakovskii Yu. G.

- Artificial Intelligence: Economic and Legal Aspects
of Innovation in the Era of Digital Transformation in Greater Eurasia 170

YOUNG RESEARCHERS' PERSPECTIVE

Nikishina A. V.

- Family Values in the Digital Environment:
Problems and Guarantees of Legal Protection 181

Nosova V. A.

- Public Law Incentives for the Development of the Information Technology
Industry as Instrument for Ensuring Technological Sovereignty 190

Ryzhkov D. I.

- The Legal Regulation Approaches for the Cities of Future:
from Smart Meters to Smart Homes 197

SCIENTIFIC HERITAGE

Turing A. M.

- Computing Machinery and Intelligence 206

POSTSCRIPT

Shpakovsky Yu. G.

- Curious Facts & More 212

СЛОВО К ЧИТАТЕЛЮ



Уважаемые читатели!

Перед вами номер, который посвящен активно развивающемуся направлению — киберправу. Большинство исследований представляют собой результаты работы преподавателей кафедры информационного права и цифровых технологий Университета имени О.Е. Кутафина (МГЮА), полученные в рамках различных направлений, реализуемых в Центре компетенций «Киберправо».

Киберправо сегодня активно развивается, поскольку большинство цифровых процессов так или иначе связаны с киберпространством, правовое регулирование использования искусственного интеллекта стремительно развивается как ключевое направление правового обеспечения киберпространства. Искусственный интеллект сегодня становится как помощником, применяемым практически во всех сферах общественной жизни, так и угрозой. В связи с этим весьма актуальным стало принятие специального федерального закона. В марте 2026 г. Правительством РФ был представлен проект федерального закона «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации». В связи с этим сегодня очень важно проанализировать предлагаемые модели регулирования использования данных технологий.

Не менее важными являются и вопросы ответственности за применение искусственного интеллекта, особенностей применения технологий искусственного интеллекта в контрольно-надзорной деятельности; ограничений использования

генеративного искусственного интеллекта как инструмента манипуляции. Эти и другие вопросы поднимаются авторами.

Центр компетенций «Киберправо» сегодня выступает важным экспертным институтом развития правового обеспечения экономики данных. Один из наиболее сложных вопросов в этой части — правовой режим цифровых данных. Здесь важно исследовать развитие правового регулирования рынка данных в России: проблемы и перспективы, особенности развития законодательства о персональных данных, промышленных данных, больших данных, данных для обучения моделей искусственного интеллекта. В настоящем номере также представлены исследования по данным проблемам.

Без внимания не остались и вопросы правового обеспечения кибербезопасности и обеспечения суверенитета в киберпространстве. Как национальный проект «Экономика данных и цифровая трансформация государства», так и национальная технологическая политика ставят данные задачи в качестве приоритетных. Поэтому мы уделили им особое внимание и пригласили известных специалистов информационного права раскрыть проблемы формирования инструментов инновационной политики государства в обеспечении национального суверенитета в условиях цифровой трансформации в Российской Федерации; особенности публично-правового стимулирования развития отрасли информационных технологий как инструмента обеспечения технологического суверенитета; правового обеспечения доверия и информационной безопасности в цифровую эпоху и др.

Надеемся, что все статьи номера будут интересны и станут основой для научных дискуссий по поставленным проблемам киберправа.

А. В. Минбалева,
*заведующий кафедрой информационного
права и цифровых технологий
Университета имени О.Е. Кутафина (МГЮА),
доктор юридических наук, профессор*

Июнь 2026¹

Конференции, круглые столы, семинары

XIV Петербургский международный юридический форум



С 24 по 26 июня 2026 г. в Санкт-Петербурге прошел XIV Петербургский международный юридический форум. В год своего 95-летия Университет имени О.Е. Кутафина (МГЮА) был представлен особенно широко: в состав делегации вошли более 120 преподавателей и работников Университета, которые приняли активное участие в работе секций форума. Эксперты Университета имени О.Е. Кутафина (МГЮА) выступили спикерами и модераторами более чем на 50 площадках по широкому кругу актуальных вопросов: от правового регулирования спортивного арбитража и дипфейков до групповых исков и генетических экспертиз.

Фонд «Росконгресс» и Минюст России представили официальный журнал XIV Петербургского международного юридического форума, где отдельный разворот был посвящен 95-летию Университета имени О.Е. Кутафина (МГЮА).

Впервые в истории Университета имени О.Е. Кутафина (МГЮА) вуз представил свой стенд на площадке Петербургского международного юридического форума. За три дня было проведено 56 мероприятий: презентаций научных трудов,

¹ URL: <https://msal.ru/news/>.

инновационных проектов и лучших практик. Кроме того, на стенде была организована консультационная зона, где гости форума могли узнать больше о реализуемых в Университете образовательных программах, исследованиях и проектах. Гостям были доступны игры на правовую тематику, научные издания и раздаточная продукция.

Стенд Университета имени О.Е. Кутафина (МГЮА) осмотрел министр юстиции Российской Федерации Константин Чуйченко.

Представители Университета также приняли участие в дискуссионных сессиях Петербургского международного юридического форума.

В рамках сессии «Останется ли место естественному интеллекту в юридической науке и образовании?» в качестве спикера выступил профессор кафедры информационного права и цифровых технологий Илья Рассолов.

Сразу три представителя Университета вошли в состав спикеров сессии «Право и биотехнологии: от запретов к архитектуре ответственности»: заведующий кафедрой медицинского права и права биотехнологий, директор Научно-образовательного центра правового обеспечения биоэкономики и генетических технологий Олег Гринь; профессор кафедры конституционного и муниципального права Сергей Кабышев; профессор кафедры интеллектуальных прав Ольга Рузакова.

Вопросы правового регулирования геномных исследований и защиты прав граждан осветила на сессии «Генетические экспертизы и права граждан: правовые вызовы в настоящем и взгляд в будущее» заместитель директора Научно-образовательного центра правового обеспечения биоэкономики и генетических технологий Татьяна Шилюк.

Будущее юридического образования стало темой развернутой дискуссии на сессии «Юридическое образование: обучение длиною в жизнь». Здесь Университет был представлен сразу четырьмя участниками: ректором Виктором Блажеевым, заведующим кафедрой нотариата Константином Корсиком, научным руководителем Научно-образовательного центра по правам человека Татьяной Москальковой и профессором кафедры конституционного и муниципального права Сергеем Кабышевым.

Заведующий кафедрой гражданского права Евгений Вавилин выступил в качестве спикера сессии «Транспортное право: всегда в движении!», где обсуждались актуальные проблемы отрасли в условиях цифровизации.



Правовые вопросы регулирования занятости на цифровых платформах затронул на сессии «Цифровые платформы и рынок труда: новые возможности и новые границы регулирования» директор Центра по обеспечению прав молодежи в цифровом пространстве Дмитрий Гуляев.

Вызовы, стоящие перед антимонопольными органами в условиях трансформации международных рынков, стали предметом выступления заведующего кафедрой конкурентного права, статс-секретаря — заместителя руководителя ФАС России Сергея Пузыревского на сессии «Антимонопольное регулирование в эпоху глобальных перемен: от адаптации к опережению».

Роль права в сохранении культурного суверенитета и защите исторической памяти стала ключевой темой выступления профессора кафедры конституционного и муниципального права Сергея Кабышева на сессии «Право как фактор обеспечения российской национально-культурной идентичности, защиты суверенитета и исторической правды».

Инструменты и перспективы правозащитной дипломатии обсуждались на сессии «Новые возможности юридической дипломатии России», где в качестве спикера выступила научный руководитель Научно-образовательного центра по правам человека Татьяна Москалькова.

26 июня 2026 г., в день рождения Олега Емельяновича Кутафина, на полях XIV Петербургского международного юридического форума на тематическом стенде транслировались видеоролики, посвященные памяти великого ученого и педагога.

В заключительный день форума на стенде Университета имени О.Е. Кутафина (МГЮА) состоялась церемония вручения ведомственных наград Следственного комитета Российской Федерации. Награды вручил советник председателя Следственного комитета Российской Федерации Александр Федоров.



Медалью «За заслуги» награжден ректор Университета имени О.Е. Кутафина (МГЮА) Виктор Блажеев.

Медалью «За высокую гражданственность» награждены первый проректор Инна Ершова и проректор по научно-исследовательской деятельности Владимир Синюков.

Благодарность Председателя Следственного комитета Российской Федерации объявлена проректору по стратегическому и международному развитию Марии Мажориной и директору Института информационной и медиабезопасности, доценту кафедры информационного права и цифровых технологий Владимиру Никишину.

«Это были насыщенные три дня продуктивной работы, важных предложений и смелых мыслей, направленных на процветание нашей страны, развитие правовой системы, укрепление межгосударственного диалога, основанного на принципах права. Для Университета в год, когда мы отмечаем 95-летний юбилей, форум стал особенно знаковым. Мы впервые представили стенд, в рамках которого организовали презентации научных трудов, инновационных проектов и лучших практик. Традиционно Университет принял активное участие в формировании деловой программы форума. Выражаю благодарность Министерству юстиции Российской Федерации, фонду “Росконгресс”, всем коллегам и партнерам за организацию мероприятия!» — сказал ректор Университета имени О.Е. Кутафина (МГЮА) Виктор Блажеев.

XIX сессия Европейско-Азиатского правового конгресса

С 4 по 5 июня 2026 г. в Екатеринбурге прошла XIX сессия Европейско-Азиатского правового конгресса, одного из крупнейших правовых форумов, объединившего свыше 1 000 участников из более чем 20 государств. В этом году мероприятие было посвящено теме «Синтез права и технологий: на пути к технологическому лидерству».

От Университета имени О.Е. Кутафина (МГЮА) в работе конгресса приняла участие представительная делегация во главе с ректором Виктором Блажеевым.

Ректор Университета имени О.Е. Кутафина (МГЮА) выступил на торжественном открытии и пленарной дискуссии конгресса. Он поделился размышлениями о междисциплинарности в юридической сфере, а также подчеркнул необходимость преодоления некоторых межотраслевых границ в праве и рассказал о развитии в рамках программы «Приоритет-2030» правового инжиниринга, который способствует предотвращению юридических рисков и защите интеллектуальной собственности еще на этапе разработки технологического продукта.

В центре внимания деловой программы XIX сессии Европейско-Азиатского правового конгресса оказались вопросы цифровых прав, регулирования автономного транспорта и беспилотной авиации, правового режима данных и цифровой



трансформации профиля гражданина. Деловая программа включала множество тематических площадок, особое место было отведено формированию кадрового потенциала будущего через площадки Европейско-Азиатского молодежного юридического форума.



II Международный научно-практический симпозиум «Право и культура»

В Университете имени О.Е. Кутафина (МГЮА) прошел II Международный научно-практический симпозиум «Право и культура», посвященный правовой охране культурных ценностей народов России.

10 июня состоялось торжественное открытие и пленарное заседание симпозиума. Модератором выступила профессор кафедры интеллектуальных прав Надежда Шебанова.

С приветственным словом к участникам и гостям мероприятия обратился проректор по научно-исследовательской деятельности Владимир Синюков: *«Культура — это обширная сфера деятельности, которая затрагивает право в различных формах. Сегодня в рамках симпозиума мы хотим уделить особое внимание охране уникальных культурных ценностей и исторического достояния народов нашей страны. Уверен, что предстоящая дискуссия поможет нашему научному сообществу под новым углом взглянуть на правовое регулирование объектов культурного наследия».*

В рамках двух дней дискуссий участники обсудили роль гражданского законодательства в сохранении, изучении и развитии культурных ценностей народов России и их взаимосвязь с охраной результатов интеллектуальной деятельности.

XII Летняя школа молодых ученых



В период с 3 по 5 июня 2026 г. на площадке Университета имени О.Е. Кутафина (МГЮА) прошла XII Летняя школа молодых ученых на тему «Морское право: обеспечение государственного суверенитета, безопасности и экономического развития России».

При открытии школы с приветственным словом к участникам обратился ректор Университета Виктор Блажеев: *«Мы создавали проект Летней школы молодых ученых для того, чтобы собрать в одном месте молодых специалистов, интересующихся совершенно разной правовой проблематикой и механизмами ее регулирования. Поэтому преимущество школы заключается в том, что вы знакомитесь с новыми*

людьми и обмениваются научными идеями, которые могут стать фундаментом для ваших исследований. Желаю вам продуктивных дискуссий и увлекательного времяпрепровождения!»

Также перед участниками выступил проректор по научно-исследовательской деятельности Владимир Синюков, отметив, что современная наука — это комплексная коллаборация ведущих экспертов, поэтому перед Летней школой молодых ученых стоит задача по расширению границ правовых исследований из локальных тем в глобальные мировые проблематики.

На протяжении пяти дней перед участниками выступали представители Института океанологии, Центра морского права, Министерства природных ресурсов и экологии, Министерства транспорта, Министерства промышленности и торговли, Общероссийского движения поддержки флота, а также иных научных ведомств и профессорско-преподавательский состав Университета имени О.Е. Кутафина (МГЮА).



В рамках проектной сессии финального дня школы команды участников выступили с презентацией разработанных проектов в области совершенствования законодательного регулирования деятельности моряков, работы судна, а также защиты экологии от загрязнения.

«Став участниками этой школы, вы превратились в уникальных специалистов, способных отвечать на современные вызовы права даже в самых неожиданных и сложных сферах, как морское право. За последние несколько лет данное направление стало особо актуальным в профессиональных кругах, но наблюдается нехватка практиков, способных внести свои предложения для



развития и выведения на новый уровень всех “плавающих” вопросов», — обратился с напутственным словом к участникам проректор по научно-исследовательской деятельности Университета имени О.Е. Кутафина (МГЮА) Владимир Синюков.



Первое сателлитное мероприятие Московского инновационного юридического форума 2027 г.

Во флагманском бутике VASSA&Co прошло первое сателлитное мероприятие Московского инновационного юридического форума 2027 г. Встреча была посвящена роли имиджа в профессиональной коммуникации женщин-руководителей — от дресс-кода в бизнесе и государственных структурах до умения выстраивать открытый и уверенный диалог.

В мероприятии также приняли участие первый проректор Университета имени О.Е. Кутафина (МГЮА) Инна Ершова и проректор по стратегическому и международному развитию Мария Мажорина. Участники обсудили перспективы участия команды VASSA&Co в Московском инновационном юридическом форуме 2027 г.



VII Летняя онлайн-школа зарубежного права «Правовое регулирование инноваций: российская и зарубежная практика»

С 18 по 19 июня 2026 г. в Университете имени О.Е. Кутафина (МГЮА) проходила VII Летняя онлайн-школа зарубежного права «Правовое регулирование инноваций: российская и зарубежная практика».

В рамках торжественного открытия школы с приветственным словом к участникам и организаторам обратился проректор по научно-исследовательской деятельности Университета Владимир Синюков: «*Модель современного юриста должна развиваться не только*

в рамках определенного государства, но и на международном уровне, затрагивая зарубежный опыт и важнейшие аспекты развития правовой системы. Наша школа зарубежного права способствует тесному научному сотрудничеству между представителями правовых сообществ различных государств и взаимному обмену полезными практиками в области инновационных разработок. Призываю вас всех уделять пристальное внимание глобальным правовым новациям и вместе открывать новые горизонты, которые помогут вывести законодательное регулирование наших стран на новый уровень!»

В торжественном открытии приняли участие председатель Ассоциации российских дипломатов Игорь Халевинский, директор Центра международного научного сотрудничества Мария Егорова и доцент кафедры международного частного права Хатиа Пирцхалава.

Летняя школа была посвящена анализу правовых механизмов регулирования инновационной деятельности в России и зарубежных странах. Преподаватели школы представили российский и зарубежный опыт правового регулирования инноваций, провели сравнительный анализ и продемонстрировали эффективные механизмы решения правовых проблем, возникающих в данной сфере.

Международное сотрудничество

В Университете имени О.Е. Кутафина (МГЮА) прошла встреча с делегацией Хэйлунцзянского университета

18 июня 2026 г. в Университете прошла встреча с делегацией Хэйлунцзянского университета.

Участников встречи приветствовали ректор Университета имени О.Е. Кутафина (МГЮА) Виктор Блажеев и проректор по стратегическому и международному развитию Мария Мажорина. Делегацию гостей возглавил секретарь партийного комитета Хэйлунцзянского университета Чи Баосюй. В переговорах также приняли участие представители руководства двух университетов.

Стороны обсудили расширение взаимодействия в сфере фундаментальных и прикладных правовых исследований, а также перспективы реализации совместного проекта по подготовке квалифицированных юридических кадров. Встреча стала еще одним шагом в развитии долгосрочного партнерства Университета имени О.Е. Кутафина (МГЮА) и Хэйлунцзянского университета, направленного на укрепление научных и образовательных связей между Россией и Китаем.



Мероприятия ректората

Завершающее в 2025/2026 учебном году заседание Ученого совета Университета имени О.Е. Кутафина (МГЮА)

29 июня 2026 г. в Университете состоялось заседание Ученого совета, в ходе которого были рассмотрены текущие кадровые вопросы, а также деятельность структурных подразделений.





Встреча началась с церемонии награждения студенческих команд, продемонстрировавших выдающиеся результаты в рамках всероссийских и международных конкурсов. Ректор Университета имени О.Е. Кутафина (МГЮА) Виктор Блажеев вручил командам диплом победителя международного конкурса по криминалистике и судебной экспертизе «Виртуальный криминалист — 2026» в номинации «Специалист в цифровой криминалистике», а также диплом победителя I Межвузовского криминалистического хакатона «Нейрослед» в номинации «Закон и порядок».

Далее на заседании Ученого совета подвели итоги конкурса на соискание стипендии ООО «Газпром энергохолдинг» имени Сергея Сергеевича Филя для обуча-

ющихся Университета имени О.Е. Кутафина (МГЮА) за высокие показатели в образовательной деятельности и научной деятельности в сфере энергетического права. Лауреатам конкурса вручаются дипломы и именные стипендии в размере 60 тысяч рублей. В 2026 г. обладателями стипендии стали восемь обучающихся: Анна Морозова, Елизавета Воробьева, Елена Конохова, Егор Трушин, Эмин Кумбатов, Анастасия Ермоленко, Варвара Глухова и Оксана Копытина.

Заседание продолжилось поздравлением работников, которые отметили свой юбилей в июне 2026 г.



Проректор по молодежной политике Александр Чанышев рассказал о первых результатах деятельности Содружества выпускников Университета имени О.Е. Кутафина (МГЮА) после состоявшейся в мае на Московском инновационном юридическом форуме перезагрузки объединения. Александр Чанышев также представил планируемые проекты Содружества выпускников, среди которых установка памятника Олегу Емельяновичу Кутафину на площади Академика Кутафина в Москве.

В ходе заседания Ученого совета выступила заместитель председателя Ассоциации студентов Анастасия Барбашева, которая рассказала об итогах деятельности органа студенческого самоуправления в

2025/2026 учебном году, а также поделилась планами Ассоциации на предстоящий период. Ректор Университета Виктор Блажеев высоко оценил работу студенческих и молодежных объединений и поблагодарил активистов за реализацию проектов, направленных на развитие вуза.

Проректор по научно-исследовательской деятельности Владимир Синюков представил на утверждение Ученым советом темы диссертаций на соискание степени кандидата и доктора юридических наук. Первый проректор Университета Инна Ершова предложила на утверждение темы магистерских диссертаций. Проректор по стратегическому и международному развитию Мария Мажорина представила на утверждение перечень программ дополнительного профессионального

образования, планируемых к запуску в рамках программы «Приоритет-2030» и в рамках взаимодействия с партнерами.

Ученым советом была утверждена кандидатура директора Института информационной и медиабезопасности Владимира Никишина на соискание премии Президента Российской Федерации в области науки и инноваций для молодых ученых за 2026 год.

В завершение встречи ректор Университета Виктор Блажеев поблагодарил членов Ученого совета за работу.

Совещание по вопросам работы диссертационных советов

В Университете имени О.Е. Кутафина (МГЮА) состоялось совещание по вопросам работы диссертационных советов. Совещание прошло под руководством ректора Виктора Блажеева. Главной темой встречи стало обсуждение результатов работы советов и определение вектора развития системы подготовки научных кадров высшей квалификации в Университете. С докладом об итогах деятельности диссертационных советов за 2025/2026 учебный год выступил проректор по научно-исследовательской деятельности Владимир Синюков.

В ходе заседания особое внимание было уделено актуальным проблемам деятельности диссертационных советов. По данному вопросу выступила председатель экспертного совета по праву и политологии ВАК России, заведующий кафедрой финансового права Университета имени О.Е. Кутафина (МГЮА) Елена Грачева, которая детально остановилась на проблемах повышения качества диссертационных исследований, соблюдения процедурных норм и дальнейшего совершенствования экспертной работы.

В Университете успешно действуют четыре диссертационных совета, охватывающих все научные специальности по праву. Это особенно важно для аспирантов, докторантов и соискателей, поскольку обеспечивает возможность прохождения всех этапов государственной научной аттестации по любой юридической специальности в рамках единой академической среды Университета.



Награждения, премии

Ректор Университета имени О.Е. Кутафина (МГЮА) награжден знаком отличия «За безупречную службу городу Москве»

В преддверии Дня России мэр Москвы Сергей Собянин вручил государственные и столичные награды. За активное участие в общественной жизни города, в ра-





боте по сохранению лучших традиций российского юридического образования и повышению правовой грамотности граждан ректор Университета имени О.Е. Кутафина (МГЮА) Виктор Блажеев награжден знаком отличия «За безупречную службу городу Москве» (30 лет).

«Москва сегодня — это не только сердце нашей страны, но и подлинный интеллектуальный центр мира. И в этом большая заслуга личного внимания мэра Москвы Сергея Семеновича Собянина к науке, образованию, к поддержке академического сообщества, без которого невозможны ни инновации, ни движение вперед. Университет имени О.Е. Кутафина (МГЮА) — моя альма-матер, и я хорошо знаю, что за любым достижением стоит труд большого количества людей. Поэтому столь высокая оценка — признание заслуг всего нашего коллектива. Огромная честь получить эту награду в год, когда мы отмечаем 95-летие Университета. Мы гордимся тем, что работаем в Москве и что вносим свой вклад в развитие России!» — отметил Виктор Блажеев.

Знак отличия «За безупречную службу городу Москве» вручается за многолетнюю плодотворную деятельность, направленную на процветание города и повышение благосостояния москвичей.

Татьяне Москальковой присуждена Государственная премия за выдающиеся достижения в области правозащитной деятельности

В День России в Георгиевском зале Большого Кремлевского дворца состоялась традиционная церемония вручения золотых медалей Героя Труда и Государственных премий в области науки и технологий, литературы и искусства за выдающиеся достижения в правозащитной и благотворительной деятельности за 2025 год.

Лауреатом Государственной премии за выдающиеся достижения в области правозащитной деятельности стала научный руководитель Научно-образовательного центра по правам человека Университета имени О.Е. Кутафина (МГЮА) Татьяна Москалькова.



Университет имени О.Е. Кутафина (МГЮА) удостоен Почетной грамоты Московской городской Думы

19 июня 2026 г. в Московской городской Думе состоялась торжественная церемония вручения наград работникам Университета имени О.Е. Кутафина (МГЮА), приуроченная к 95-летию Университета.

Почетную грамоту Московской городской Думы Университету имени О.Е. Кутафина (МГЮА) за вклад в развитие городского сообщества вручил председатель Московской городской Думы Алексей Шапошников: *«Сегодня в этом зале собрались люди, которые своим ежедневным трудом способствуют развитию столицы и повышению качества жизни москвичей. Особенно рад видеть наших коллег из Университета имени О.Е. Кутафина (МГЮА). За 95 лет своей истории он стал одним из ведущих юридических вузов страны, подготовив тысячи высококвалифицированных специалистов, которые вносят значительный вклад в развитие государства и общества».*

Поблагодарив Московскую городскую Думу за высокую оценку деятельности Университета, Виктор Блажеев подчеркнул: *«Для нас большая честь получить эту награду. Университет и Московскую городскую Думу связывает многолетнее, плодотворное и эффективное взаимодействие. От имени всего коллектива выражаю искреннюю благодарность за столь высокую оценку нашей работы. Это признание достижений многих поколений преподавателей, работников и выпускников Университета».*

Благодарностями Московской городской Думы отмечены также преподаватели и работники Университета за вклад в развитие городского сообщества, большой



вклад в развитие высшей школы и юридической науки, а также подготовку высококвалифицированных кадров на основе инновационных образовательных технологий.

На соискание ученой степени...

В июне 2026 г. в Университете прошли успешные защиты двух докторских диссертаций



Докторант кафедры финансового права Евгений Марьин представил диссертацию на соискание ученой степени доктора юридических наук на тему «Финансово-правовое обеспечение охраны окружающей среды и природопользования в Российской Федерации».

Докторант кафедры финансового права Ирина Сапрыкина защитила диссертацию на соискание ученой степени доктора юридических наук на тему «Юридические факты в налоговом праве».

Поздравляем с успешной защитой и желаем новых научных достижений!

Право искусственного интеллекта

Формирование правовых условий для благоприятного развития искусственного интеллекта в России¹

Аннотация. В статье анализируются особенности и основные направления формирования правовых условий для благоприятного развития искусственного интеллекта в России. Рассмотрены основные факторы и причины, которые препятствовали развитию правового регулирования сферы искусственного интеллекта в последние годы. Выявлено, что развитие правовых условий во многом связано с законодательным опытом, который формирует системный подход, повышает значимость складывающихся правоотношений и детерминирует создание активно развивающейся регуляторной среды в данной сфере. Установлено, что процесс стандартизации в сфере ИИ не должен происходить в отрыве от нормативного правового регулирования, поскольку здесь существует значительное количество рисков и угроз в отношении возможного нарушения прав и свобод человека и гражданина, а также в связи с необходимостью учета особой значимости ИИ при реализации технологической политики Российской Федерации. Главные достоинства этических кодексов в сфере ИИ — формирование в обществе представлений об основных принципах и условиях работы с ИИ, влияние на принятие локальных правовых актов в сфере ИИ, что оказало положительное влияние на формирование правовых условий благоприятного развития ИИ в реальном секторе экономики и социальной сфере. При построении положений базового федерального закона в сфере ИИ ряд норм формулируются на основе норм этики, происходит заимствование принципов.

Выделены ключевые законопроекты в сфере регулирования искусственного интеллекта в России и перспективы принятия базового закона в данной сфере.

Ключевые слова: благоприятное развитие, искусственный интеллект, правовые условия, технологическая политика, правовое обеспечение технологического лидерства, технологии искусственного интеллекта, цифровое право



Алексей Владимирович МИНБАЛЕЕВ,

заведующий кафедрой
информационного
права и цифровых
технологий

Университета имени
О.Е. Кутафина (МГЮА),
доктор юридических наук,
профессор

alexmin@bk.ru

125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2026.142.6.023-030

¹ Статья подготовлена в рамках выполнения работ по государственному заданию на тему «Развитие правовой системы в условиях обеспечения технологического лидерства Российской Федерации: национальные приоритеты и международные вызовы (FSMW-2026-0005)». Регистрационный номер: 126022017763-1.

Alexey V. MINBALEEV,

Head of the Department of information law and digital technologies
of the Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor
alexmin@bk.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Formation of Legal Conditions for the Favorable Development of Artificial Intelligence in Russia

Abstract. *In this article, the authors analyze the characteristics and key areas of development of a legal environment for the favorable development of artificial intelligence in Russia. They examine the key factors and reasons that have hindered the development of legal regulation in the field of artificial intelligence in recent years. It is found that the development of legal conditions is largely linked to the need to develop legislative expertise that fosters a systematic approach, enhances the significance of emerging legal relationships, and determines the creation of a rapidly evolving regulatory environment in this area. It is established that the standardization process in the field of AI should not occur in isolation from legal regulation, as it poses significant risks and threats regarding the potential violation of human and civil rights and freedoms, as well as the need to consider the particular significance of AI in the implementation of the Russian Federation's technology policy.*

The main advantage of ethical codes in the field of AI is that they foster public understanding of the fundamental principles and conditions for working with AI and influence the adoption of local AI legislation. This has had a positive impact on the formation of legal conditions favorable to the development of AI in the real economy and social sphere. Furthermore, when drafting the provisions of the basic federal law on AI today, a number of norms are formulated based on ethical norms, borrowing principles. The article highlights key legislative proposals regulating artificial intelligence in Russia and the prospects for adopting a basic law in this area.

Keywords: *favorable development, artificial intelligence, legal conditions, technology policy, legal support for technological leadership, artificial intelligence technologies, digital law*

Введение. Формирование правовых и иных условий для благоприятного развития искусственного интеллекта сегодня отвечает современной технологической политике Российской Федерации², а также задачам по обеспечению технологического лидерства³. Неслучайно ведущие специалисты в сфере

² Федеральный закон от 28.12.2024 № 523-ФЗ «О технологической политике в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2024. № 53 (ч. I). Ст. 8533.

³ См.: Инновационная юриспруденция : учебник / В. В. Блажеев, М. В. Мажорина, В. Б. Арафонов [и др.]. М. : Проспект, 2025 ; Полякова Т. А., Минбалеев А. В., Кроткова Н. В.

технологического лидерства отмечают, что его обеспечение напрямую зависит от развития «собственной инфраструктуры — серверов, операционных систем, СУБД, средств кибербезопасности... драйверами будет развитие искусственного интеллекта и обеспечивающей инфраструктуры вокруг него — как аппаратной, так и программной»⁴.

Сегодня принципиально важным видится формирование полноценной системы правового регулирования в сфере ИИ. Причем это должны быть не только базовый федеральный закон и система подзаконных нормативных правовых актов, но несколько федеральных законов, направленных на развитие ряда аспектов, связанных с ИИ. Создание правовых условий во многом связано с необходимостью формирования законодательного опыта, который обуславливает системный подход, повышает значимость складывающихся правоотношений и детерминирует формирование активно развивающейся регуляторной среды в данной сфере. Принятие базового законодательства в сфере ИИ, бесспорно, станет отправной точкой и для развития специального регулирования отдельных сфер применения ИИ.

Основная часть. В первую очередь рассмотрим основные факторы и причины, которые препятствовали развитию правового регулирования сферы ИИ в последние годы. Их устранение будет важным условием для более благоприятного развития ИИ.

Основная проблема, которая сегодня должна быть учтена в процессе формирования и развития системы правового регулирования отношений в сфере использования технологий и систем ИИ, а также в сфере непосредственного регулирования самих технологий и систем ИИ, — это отсутствие эффективного взаимодействия различных механизмов регулирования отношений в сфере использования технологий и систем ИИ. Во многом это обусловлено тем, что в России происходит очень серьезная задержка правового регулирования сферы ИИ.

Причины кроются в ряде факторов, среди которых можно выделить следующие:

- инициация и реализация разных механизмов регулирования использования технологий и систем ИИ осуществлялась разными субъектами, без должного взаимодействия;
- в процессе формирования каждого механизма, к сожалению, не всегда учитывался и учитывается опыт формирования и реализации других механизмов;
- не было сформировано единой цели, связанной с возданием единого регуляторного пространства, в котором использование технологий и систем ИИ обеспечивает вклад в технологическое лидерство государства;

Трансформация науки информационного права и информационного законодательства: новый этап в условиях научно-технологического развития России // Государство и право. 2024. № 9. С. 166—179 ; Полякова Т. А., Минбалева А. В., Наумов В. Б. Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве России // Государство и право. 2025. № 1. С. 160—173.

⁴ Попова М. Игра не в классики // Эксперт. 2026. № 4. С. 87.



— в рамках каждого механизма в недостаточной мере встроены инструменты взаимодействия друг с другом.

Базовый закон, посвященный вопросам регулирования сферы ИИ, должен быть целью в сфере регулирования отношений в сфере ИИ. Государство же, во многом под влиянием международных тенденций и рисков создания излишних административных барьеров на пути технологического развития сферы ИИ, выбрало путь приоритизации этического и нормативно-технического регулирования сферы ИИ.

Анализ опыта разработки нормативно-технического регулирования ИИ свидетельствует, что стандартизация сферы ИИ осуществлялась с опорой во многом на международные стандарты ISO и других международных организаций, но они не были главными ориентирами, а только неизбежным этапом развития системы стандартизации и сертификации. За последние 6 лет было принято свыше 400 стандартов в сфере информационных технологий и порядка 100 в сфере ИИ⁵, при этом значительная трансформация предоставила возможности для активного внедрения новых технологий ИИ, повышения производительности и качества производимых товаров и оказываемых услуг, стимулирования новых инновационных процессов. Здесь можно выделить следующие характерные особенности:

- при формировании системы стандартов для сферы ИИ ставилась задача не акцентировать внимание на этических вопросах и формировании системы саморегулирования, что наиболее часто можно встретить в Европейском союзе и ряде государств мира, а создавать эффективные инструменты управления технологическим развитием и обеспечения технологического суверенитета. При этом анализ стандартов, принятых с 2020 по 2026 г., явно свидетельствует, что благодаря их реализации все более усиливается обеспечение технологического суверенитета России;
- тесная интеграция национальных стандартов с национальными программами (сначала с цифровой экономикой, далее — с экономикой данных и цифровой трансформацией государства);
- стремление охватить все ключевые сферы и направления использования ИИ;
- учет национальных интересов и национальных требований в процессе интеграции международных стандартов в сфере ИИ;
- обеспечение всесторонней поддержки российских производителей, разработчиков и вендоров и т.д.

Стандартизация в сфере ИИ стремительно развивается. Уже идут активные разработки новых актов нормативно-технического регулирования, направленных на оценку качества отдельных процессов, связанных с применением технологий ИИ, а также систем ИИ, их безопасности, совместимости и объяснимости. Это влечет за собой внедрение новых стандартов и создание линейки локальных правовых актов в организациях — положений, регламентов, требований, посвященных регулированию тех или иных процессов, связанных с ИИ. При этом отсутствие базового законодательства в сфере ИИ создает массу рисков в данном направлении. Они связаны с приоритетным использованием при создании

⁵ Стандарты для цифрового будущего // URL: <https://www.rgtr.ru/press-tsentr/2797> (дата обращения: 10.04.2026).

локальной правовой базы не нормативных правовых актов, в которых эти аспекты не урегулированы, а стандартов. Это сегодня очень хорошо заметно не только в промышленности, но и на транспорте, в здравоохранении, образовании и других сферах. При этом используются технические термины и их определения, сформулированные в стандартах. Однако их анализ свидетельствует, что часто они отражают особенности тех или иных технических процессов, но оказываются плохо применимыми при правовом регулировании.

В связи с этим важно понимать, что процесс стандартизации не должен происходить в отрыве от нормативного правового регулирования. Это в полной мере распространяется на сферу ИИ, поскольку здесь существует значительное количество рисков и угроз в отношении возможного нарушения прав и свобод человека и гражданина, а также в связи с необходимостью учета особой значимости ИИ при реализации технологической политики Российской Федерации.

Этическое регулирование, в том числе Кодекс этики в сфере искусственного интеллекта, а также последующие специализированные этические кодексы, посвященные отдельным направлениям в сфере ИИ, развивались параллельно с техническим регулированием. Оба механизма, исходя из содержания соответствующих актов, основаны на действующем российском законодательстве, в том числе актах стратегического планирования, учитывают возможность реализации экспериментальных правовых режимов применительно к использованию технологий ИИ. Однако, к сожалению, Кодекс этики в сфере искусственного интеллекта не стал за последние пять лет реальным механизмом, который смог бы существенным образом ограничить нарушения в сфере ИИ.

Однако принижать их роль также нельзя. Главное достоинство таких кодексов состоит в том, что они формируют в обществе представления об основных принципах и условиях (требованиях) работы с ИИ. Благодаря положениям кодексов этики происходит осознание негативных и положительных коннотаций, связанных с ИИ. Они также легли в основу многих локальных правовых актов, тем самым оказав положительное влияние на формирование правовых условий благоприятного развития ИИ в реальном секторе экономики и социальной сфере. Бесспорно, и при построении сегодня положений базового федерального закона в сфере ИИ ряд норм формулируется на основе норм этики, происходит заимствование принципов.

Полагаем, что эффект был бы больше, если бы в Кодексе этики в сфере искусственного интеллекта была не просто отсылка, что он основывается на действующем российском законодательстве (что как раз вызывает вопросы с позиции природы регуляторной модели), а закреплялась возможность применения юридической ответственности за нарушение отдельных этических норм при прямом закреплении в соответствующем нормативном правовом акте, например в базовом федеральном законе, посвященном ИИ. Такой подход смог бы создать необходимые предпосылки для развития надлежащих правовых условий для ограничения возможных злоупотреблений при использовании ИИ, обеспечить более уважительное и ответственное отношение к юридическому факту присоединения к Кодексу этики в сфере искусственного интеллекта или другому этическому кодексу, а также способствовал действенной реализации этических норм на практике.



Теперь обратимся непосредственно к правовому регулированию в сфере ИИ. Сегодня оно развивается через осознание и разработку базового федерального закона. Важно отметить, что к концу 2025 г. сформировалось несколько центров подготовки проекта такого закона. В Университете имени О.Е. Кутафина (МГЮА) работа в данном направлении началась еще в 2021 г., когда в рамках Центра компетенций «Киберправо» была поставлена задача по разработке проекта такого закона. Первоначально был разработан проект модельного закона для государств МПА СНГ «О технологиях искусственного интеллекта» для формирования механизмов доверия к системам искусственного интеллекта путем развития единого комплексного подхода к интеграции правовых и этических норм в государственную политику, использования риск-ориентированного подхода на всех этапах жизненного цикла искусственного интеллекта⁶. 18 апреля 2025 г. Межпарламентская Ассамблея СНГ приняла модельный закон «О технологиях искусственного интеллекта», в который вошли ряд положений из проекта Университета имени О.Е. Кутафина (МГЮА)⁷. В 2025 г. на основе принятого модельного закона был разработан проект модельного закона для государств МПА СНГ «О технологиях (системах) искусственного интеллекта», направленного на развитие принятого акта⁸.

Также в 2025 г. А. В. Минбалеевым и Д. П. Осиповым были подготовлены проект федерального закона «О технологиях искусственного интеллекта»⁹, Концепция развития регулирования отношений в сфере разработки, внедрения и использования технологий искусственного интеллекта в странах БРИКС до 2030 года¹⁰. Это одни из первых публично представленных проектов федерального закона для Российской Федерации и концепции регулирования в сфере ИИ на уровне БРИКС. При этом название закона «О технологиях искусственного интеллекта» обусловлено в первую очередь стремлением придать большее значение в качестве объектов именно технологиям и системам ИИ, нежели самой

⁶ Проект модельного закона «О технологиях искусственного интеллекта» подготовлен в Университете имени О.Е. Кутафина (МГЮА) (URL: <https://www.rgtr.ru/press-tsentr/2797> (дата обращения: 10.04.2026)).

⁷ См.: Модельный закон «О технологиях искусственного интеллекта» // Приложение к постановлению Межпарламентской Ассамблеи СНГ от 18.04.2025 № 58-8. URL: <https://eccis.org/document/7183> (дата обращения: 10.04.2026).

⁸ Обновленный проект модельного закона для государств Межпарламентской Ассамблеи СНГ «О технологиях (системах) искусственного интеллекта» // URL: <https://consortium.msal.ru/wp-content/uploads/2021/11/proekt-modelnogo-zakona-sng-o-tehnologiyah-II.pdf> (дата обращения: 10.04.2026).

⁹ Проект Федерального закона «О технологиях искусственного интеллекта» // URL: <https://consortium.msal.ru/wp-content/uploads/2021/11/proekt-fz-o-tehnologiyah-iskusstvennogo-intellekta.pdf> (дата обращения: 10.04.2026).

¹⁰ Концепция развития регулирования отношений в сфере разработки, внедрения и использования технологий искусственного интеллекта в странах БРИКС до 2030 года // URL: <https://consortium.msal.ru/wp-content/uploads/2021/11/Koncepciya-razvitiya-regulirovaniya-otnoshenij-v-sfere-razrabotki-vnedreniya-i-ispolzovaniya-tehnologij-iskusstvennogo-intellekta-v-stranah-BRIKS-do-2030-goda.pdf> (дата обращения: 10.04.2026).

категории «искусственный интеллект», которая во многом является оценочной и философской.

Кроме того, в ноябре 2024 г. в общероссийской общественной организации «Деловая Россия» также была начата работа над проектом федерального закона «Об искусственном интеллекте», представленного в 2025 г., при подготовке которого нами был дан ряд рекомендаций относительно изменения названия проекта, изменения понятийного аппарата, исключения положений гражданско-правового характера и др.

Первый законопроект, посвященный ИИ, — «Об искусственном интеллекте в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации», разработанный Министерством цифрового развития, связи и массовых коммуникаций РФ, в марте 2025 г. был разослан в профильные федеральные органы исполнительной власти и экспертам.

После анализа экспертных замечаний и предложений были внесены существенные изменения и официально представлен проект федерального закона «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации»¹¹. При этом целью данного федерального закона заявлены «создание правовых условий для ускоренного развития и внедрения технологий искусственного интеллекта, обеспечение безопасности личности, общества и государства, государственного технологического суверенитета при использовании технологий искусственного интеллекта в Российской Федерации».

В ходе публичного обсуждения закон был подвергнут резкой критике, по итогам которой были внесены существенные коррективы. Отдельные эксперты отмечают при этом, что в «процессе доработки законопроекта (март — апрель 2026 г.) произошел переход от формальных ограничений к модели содержательного контроля»¹². Однако остается ряд вопросов относительно приоритетности регулирования самих моделей ИИ. Модель ИИ представляет собой фактически один из начальных результатов в технологическом процессе разработки и внедрения тех или иных технологий и систем ИИ. Для того чтобы устанавливать требования именно к моделям, необходимо создание серьезных административных барьеров при использовании моделей для технологий и систем ИИ.

Также достаточно много вопросов к реализации риск-ориентированного подхода при регулировании ИИ, который фактически закрепляется, в то время как механизм его реализации не определен, много вопросов к субъектам отношений в сфере ИИ, к приоритетности регулирования ИИ как технологии, а не отношений по использованию технологий и систем ИИ, которые и необходимо регулировать.

¹¹ Проект федерального закона «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации» // URL: <https://www.bing.com/search?q=> (дата обращения: 25.03.2026).

¹² Трельский Г. Регулирование ИИ в России 2026—2027: от жестких запретов к профессиональным стандартам // URL: https://zakon.ru/blog/2026/04/28/regulirovanie_ii_v_rossii_20262027_ot_zhestkih_zapretov_k_professionalnym_standartam (дата обращения: 25.03.2026).



Все эти вопросы должны быть закреплены если не в рамках подготавливаемой к первому чтению редакции проекта, то обязательно в рамках рассмотрения законопроекта во втором чтении в Государственной Думе. Однако, несмотря на эти и другие замечания, полагаю, что для благоприятного развития ИИ в России законопроект должен быть принят как можно скорее.

БИБЛИОГРАФИЯ

1. Инновационная юриспруденция : учебник / В. В. Блажеев, М. В. Мажорина, В. Б. Агафонов [и др.]. — М. : Проспект, 2025. — 912 с.
2. Полякова Т. А., Минбалеев А. В., Кроткова Н. В. Трансформация науки информационного права и информационного законодательства: новый этап в условиях научно-технологического развития России // Государство и право. — 2024. — № 9. — С. 166—179.
3. Полякова Т. А., Минбалеев А. В., Наумов В. Б. Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве России // Государство и право. — 2025. — № 1. — С. 160—173.

Применение технологий искусственного интеллекта в контрольно-надзорной деятельности: проблемы и перспективы правового регулирования¹

Аннотация. В статье исследуются правовые и организационные аспекты применения искусственного интеллекта в деятельности органов, осуществляющих государственный контроль (надзор). Показаны особенности и преимущества цифровой трансформации контрольно-надзорной деятельности, одним из направлений которой является применение искусственного интеллекта. Проведен анализ ключевых направлений применения искусственного интеллекта в контрольно-надзорной деятельности, приведены типы операций, осуществляемых искусственным интеллектом. Выявлены проблемы применения технологий искусственного интеллекта в контрольно-надзорной деятельности. Сделан вывод, что особенностью формируемой российской модели развития правового регулирования искусственного интеллекта является акцент на сохранении решающей роли человека при принятии итоговых решений. Показано, что принятие федерального закона «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации», основанного на риск-ориентированном подходе, призвано устранить правовую неопределенность и создать унифицированные основания для контрольно-надзорной деятельности.

Ключевые слова: искусственный интеллект, государственный контроль (надзор), контрольно-надзорная деятельность, контрольно-надзорные мероприятия, риск-ориентированный подход, цифровая трансформация, цифровая платформа, автоматизация, идентификация, прогнозирование, систематизация данных, мониторинг, риски использования искусственного интеллекта



**Марина Борисовна
ДОБРОБАБА,**

профессор кафедры
информационного права
и цифровых технологий
Университета имени
О.Е. Кутафина (МГЮА),
доктор юридических наук,
доцент
mbdobrobaba@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2026.142.6.031-039

¹ Статья подготовлена в рамках выполнения работ по государственному заданию на тему «Развитие правовой системы в условиях обеспечения технологического лидерства Российской Федерации: национальные приоритеты и международные вызовы (FSMW-2026-0005)». Регистрационный номер: 126022017763-1.

Marina B. DOBROBABA,

*Professor of the Department of information law and digital technologies
of the Kutafin Moscow State Law University (MSAL),*

Dr. Sci. (Law), Associate professor

mbdobrobaba@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

The Use of Artificial Intelligence Technologies in Control and Supervision: Challenges and Prospects for Legal Regulation

Abstract. *The article explores the legal and organizational aspects of the application of artificial intelligence in the activities of state control (supervision) bodies. It highlights the features and advantages of the digital transformation of control and supervision activities, one of which is the use of artificial intelligence. The article analyzes the key areas of application of artificial intelligence in control and supervision activities and the types of operations performed by artificial intelligence. It also identifies the challenges of using artificial intelligence technologies in control and supervision activities. The article concludes that the Russian model of developing legal regulation for artificial intelligence emphasizes the importance of human decision-making. It is shown that the adoption of the Federal Law “On the Fundamentals of State Regulation of the Application of Artificial Intelligence Technologies in the Russian Federation”, based on a risk-oriented approach, is intended to eliminate legal uncertainty and create unified grounds for control and supervision activities.*

Keywords: *artificial intelligence, state control (supervision), control and supervision activities, control and supervision measures, risk-based approach, digital transformation, digital platform, automation, identification, forecasting, data systematization, monitoring, risks of using artificial intelligence*

Актуальность проблемы

К началу XXI в. традиционная модель контрольно-надзорной деятельности (далее — КНД), основанная на плановых проверках, исчерпала свой ресурс. Стало очевидным, что государство объективно не способно тотально проверить всех контролируемых субъектов. В свою очередь, в связи с низкой оперативностью традиционного государственного контроля (надзора) по ряду направлений разрыв между моментом совершения правонарушения и моментом его выявления может быть критическим. В сложившихся условиях цифровая трансформация государственного контроля (надзора) стала единственным способом перейти от реагирования на уже случившиеся инциденты к их прогнозированию и предупреждению.

Цифровая трансформация государственного управления, закреплённая в программных документах стратегического планирования, объективно требует внедрения технологий ИИ в КНД. Вместе с тем действующее законодательство

не содержит специальных норм, регламентирующих процессуальный механизм его применения. Особую остроту проблеме придает необходимость соблюдения баланса между эффективностью контроля (надзора) и признанием, соблюдением и защитой прав и свобод контролируемых лиц. Кроме того, пилотные проекты по внедрению ИИ в КНД в России уже выявили правовые коллизии, связанные с юридической силой «решений», вынесенных системами ИИ², и ответственностью за возможные ошибки³. Перечисленные обстоятельства обуславливают необходимость выработки перспективной модели правового регулирования применения технологий ИИ в КНД.

Реформа КНД и его цифровая трансформация

В России реализуется масштабная «регуляторная гильотина» и реформа КНД, целью которых является снижение административной нагрузки на бизнес. Ключевым инструментом этой реформы является *цифровая платформа* «Типовое облачное решение системы автоматизации контрольно-надзорной деятельности»⁴. Осуществляется и трансформация *риск-ориентированного подхода*, законодательно закрепленного гл. 5 Федерального закона от 31.07.2020 № 248-ФЗ (ред. от 29.12.2025) «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»⁵ (далее — Закон № 248-ФЗ).

К числу преимуществ цифровой трансформации КНД относятся⁶:

- 1) *автоматизация контрольно-надзорных процедур*, что способствует точности анализа данных и повышению оперативности проведения контрольно-надзорных мероприятий (далее — КНМ), а следовательно, реализации *принципа оперативности* как ключевого принципа государственного контроля (надзора) (ст. 14 Закона № 248-ФЗ);
- 2) *снижение нагрузки на бизнес*, поскольку автоматизация позволяет проводить проверки дистанционно, без личного присутствия инспектора, что радикально сокращает административные издержки для контролируемых лиц;
- 3) *повышение прозрачности КНД*, осуществляемое за счет публикации данных о работе контрольно-надзорных органов через информационные системы, что

² Судебная практика по вопросам искусственного интеллекта — 2025 // URL: <https://delprof.ru/press-center/experts-pubs/sudebnaya-praktika-po-voprosam-iskusstvennogo-intellekta-2025/> (дата обращения: 15.03.2026).

³ Ковалев С. Д. Ответственность за ошибки искусственного интеллекта // Аграрное и земельное право. 2024. № 8 (236). С. 67—69.

⁴ Постановление Правительства РФ от 21.04.2018 № 482 (ред. от 07.04.2025) «О государственной информационной системе “Типовое облачное решение по автоматизации контрольной (надзорной) деятельности”» // СЗ РФ. 2018. № 18. Ст. 2633 ; 2025. № 15. Ст. 1894.

⁵ СЗ РФ. 2020. № 31 (ч. I). Ст. 5007 ; 2025. № 52 (ч. I). Ст. 8354.

⁶ См.: Иксанов Р. А., Владимиров И. А., Токолов А. В. Правовое регулирование цифровизации контрольно-надзорной деятельности в сфере природопользования // Административное право и процесс. 2025. № 9. С. 37—40.



позволяет воплотить в жизнь *принцип открытости*, который также установлен Законом № 248-ФЗ (ст. 13);

- 4) *предотвращение возможных коррупционных проявлений* в процессе осуществления КНД за счет использования цифровых инструментов, что способствует соблюдению *принципа законности* государственного контроля (надзора) (ст. 7 Закона № 248-ФЗ).

Правовое регулирование государственного контроля (надзора) и применения ИИ в государственном управлении

Основным нормативным актом, регламентирующим отношения по осуществлению государственного контроля (надзора) в России, является Закон № 248-ФЗ. Следует отметить, что в последней редакции он содержит положения, регламентирующие использование цифровых технологий при осуществлении КНД. В то же время предметная область действия Закона № 248-ФЗ сильно сужена — многие виды государственного контроля (надзора), такие как налоговый контроль, валютный контроль, таможенный контроль и т.д. (п. 5 ст. 2), регулируются специальным законодательством.

Что касается ИИ, то в настоящее время его развитие осуществляется в соответствии с Национальной стратегией развития искусственного интеллекта на период до 2030 года⁷. В то же время Минцифры России подготовлен проект федерального закона «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации» (далее — проект закона о госрегулировании ИИ), размещенный в марте 2026 г. на портале проектов нормативных правовых актов⁸. Данный законопроект задает вектор развития правового обеспечения применения технологий ИИ в КНД. В частности, им предусмотрено, что правовое регулирование отношений, возникающих в связи с разработкой, внедрением, использованием ИИ на территории Российской Федерации осуществляется с учетом необходимости оценки, в том числе *вероятности рисков причинения вреда (ущерба) и масштаба причиняемого ущерба* в связи с применением технологий ИИ (п. 2 ст. 5).

Что касается деятельности федеральных органов исполнительной власти, то вопросы применения ими ИИ в КНД затрагиваются только на уровне программных и стратегических документов, в том числе ведомственного характера, с большей или меньшей степенью конкретности⁹. Планируемое принятие и вступление в

⁷ Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года) // СЗ РФ. 2019. № 41. Ст. 5700 ; 2024. № 8. Ст. 1102.

⁸ Проект федерального закона «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации» // URL: <https://regulation.gov.ru/projects/166424/> (дата обращения: 21.03.2026).

⁹ См.: *Добробаба М. Б., Чаннов С. Е., Евсиков К. С.* Правовое обеспечение применения цифровых технологий в государственном управлении. Саратов : Амирит, 2024.

силу закона о госрегулировании ИИ призвано обеспечить формирование нормативной базы, необходимой для полноценного функционирования системы мониторинга и обеспечения безопасного, этичного и подотчетного применения технологий ИИ во всех сферах общественной жизни, в том числе при осуществлении КНД.

Следует отметить, что в научной литературе указывается на необходимость разработки для дальнейшего внедрения в КНД технологии ИИ соответствующей стратегии, в которой должны быть зафиксированы основные направления, формы и методы применения ИИ в КНД, а также временные этапы его внедрения в практику и возможные риски¹⁰.

Ключевые направления применения ИИ в КНД

Основные направления применения ИИ в КНД следующие:

1. Информационно-аналитическое направление

Наиболее масштабным проектом по внедрению ИИ в КНД стали мониторинг и фильтрация интернет-контента. Так, Роскомнадзором создана система цензуры интернет-трафика на базе ИИ. Статистические показатели демонстрируют рост интенсивности КНМ в данной сфере. В 2025 г. количество заблокированных материалов увеличилось почти на 60 %, достигнув 1,29 млн. Столь значительная динамика демонстрирует объективную необходимость автоматизации процессов обнаружения и блокировки, поскольку ручная модерация в таких объемах физически невозможна. С правовой точки зрения внедрение ИИ в деятельность Роскомнадзора обосновывается концепцией цифрового суверенитета, закрепленной в готовящейся новой редакции Доктрины информационной безопасности Российской Федерации¹¹.

2. Контрольно-аналитическое направление

Другим значимым направлением применения ИИ выступает его использование в деятельности контрольно-счетных органов при осуществлении государственного финансового контроля. Так, в соответствии со Стратегией развития Счетной палаты Российской Федерации на 2025—2030 годы¹² осуществляется активная реализация комплексной программы цифровой трансформации, включающей разработку системы на базе ИИ, предназначенной для автоматизации контрольных функций. К формализованным инициативам, планируемым к внедрению на 2026 г. и до 2030 г., относятся *риск-ориентированный аудит* и *цифровой аудит*. Примечательно, что на семинаре контрольных органов БРИКС

¹⁰ Мартынов А. В. Актуальные вопросы применения искусственного интеллекта при осуществлении контрольно-надзорной деятельности органов исполнительной власти // Вестник ННГУ. 2020. № 2. С. 184.

¹¹ В Совбезе раскрыли детали новой доктрины информационной безопасности // URL: <https://www.rbc.ru/politics/28/01/2026/6979d3ef9a79476325e0fcb9> (дата обращения: 11.03.2026).

¹² Стратегия развития Счетной палаты Российской Федерации на 2025—2030 годы // URL: <https://ach.gov.ru/documents/strategy/> (дата обращения: 11.03.2026).



в январе 2026 г. российский опыт в этой области признан соответствующим мировым тенденциям¹³.

3. Обеспечительное направление

Данное направление охватывает применение ИИ для оптимизации вспомогательных процессов в деятельности государственных органов, включая контрольно-надзорные органы. В настоящее время в Аппарате Правительства РФ проводится эксперимент по внедрению ИИ, в рамках которого участники получили возможность: генерировать документы на основе шаблонов; подготавливать проекты презентаций; проводить комплексный анализ данных из различных источников; осуществлять семантический анализ нормативных правовых актов; классифицировать входящую документацию и распределять ее по исполнителям; осуществлять контекстный поиск информации в архивах¹⁴.

Типы операций, осуществляемых ИИ в процессе КНД

В настоящее время можно выделить три основных типа операций, осуществление которых позволяет применять ИИ в КНД: прогнозирование; идентификация объектов; учет и систематизация данных.

Осуществление *прогнозирования* при применении ИИ органами государственного контроля (надзора) обусловлено предиктивными возможностями ИИ, который способен анализировать гигантские массивы данных и вычислять индикаторы риска задолго до того, как нарушение будет совершено или обнаружено. С учетом направленности КНД на предупреждение нарушений прогнозная аналитика является наиболее значимым применением ИИ в КНД, сопровождаемым, как правило, *непрерывным мониторингом*.

Идентификация объектов органами государственного контроля (надзора) может применяться для распознавания текстов документов, обрабатываемых при осуществлении КНМ, а также при наблюдении с беспилотников за объектами контроля. Так, Россельхознадзор применяет беспилотные воздушные суда, что значительно повышает эффективность государственного контроля (надзора)¹⁵.

ИИ может быть использован органами государственного контроля (надзора) для выполнения такой задачи, как *учет и систематизация данных (классификация)*. Так, при работе с обращениями граждан алгоритмы ИИ классифицируют

¹³ Семинар САИ БРИКС по применению искусственного интеллекта // URL: <https://intosairussia.org/news-media/news/brics-sais-seminar-on-artificial-intelligence-use.html> (дата обращения: 11.03.2026).

¹⁴ В Аппарате Правительства внедряют ИИ-сервисы для работы с документами // URL: https://rg.ru/2026/02/12/v-apparate-pravitelstva-vnedriaiut-ii-servisy-dlia-raboty-s-dokumentami.html?utm_referrer=https%3A%2F%2Fyandex.ru%2F (дата обращения: 11.03.2026).

¹⁵ Эффективность проверок бизнеса повысят за счет беспилотников и ИИ // URL: https://rg.ru/2025/11/10/effektivnost-proverok-biznesa-povysiat-za-schet-besplotnikov-i-ii.html?utm_referrer=https%3A%2F%2Fyandex.ru%2F (дата обращения: 03.03.2026).

входящие обращения, определяют тему, степень критичности и даже предлагают возможные ответы или направляют в соответствующий отдел.

Риски и проблемы применения технологий ИИ в КНД

В мире активно развивается регулирование ИИ. Так, в принятом Европейским союзом 13.03.2024 Регламенте об искусственном интеллекте (EU AI Act) ИИ-системы дифференцируются по категориям: неприемлемый, высокий, ограниченный, минимальный риски. При этом использование ИИ в публичном управлении (включая контроль и надзор) относится к группе высокого риска.

В российском законодательстве установление категорий рисков применения ИИ нормативно не закреплено. В то же время предлагается отойти от европейской риск-классификации и передать решения отраслевым регуляторам, которые определяют правила в своих секторах. По мнению Минцифры России, такой подход несет *риски фрагментации и формирования неравных стандартов для участников рынка*¹⁶.

Следует отметить, что в основу проекта закона о госрегулировании ИИ положен *риск-ориентированный подход*, согласно которому требования к системам ИИ дифференцируются в зависимости от степени их потенциального влияния на жизнь человека и общество, что позволяет выстраивать систему мониторинга, адекватную уровню выявленных угроз¹⁷. При этом разработка и обучение моделей ИИ должны осуществляться исключительно на территории Российской Федерации. Особенностью формируемой российской модели развития правового регулирования ИИ является акцент на *сохранении решающей роли человека при принятии итоговых решений*.

Применение цифровых технологий при осуществлении КНД сопряжено с рядом проблем. Так, требует нормативного обеспечения вопрос, связанный с применением процессуальных норм в случае, если *решение вынесено алгоритмом*. В силу отсутствия специального правового регулирования не решен вопрос, связанный с определением *субъекта ответственности* (разработчик, оператор либо инспектор, утвердивший решение) в случае сбоя алгоритма или причинения ущерба неправомерным решением, принятым ИИ. Одной из проблем является *дефицит кадров* сотрудников контрольно-надзорных органов, обладающих профессиональными компетенциями в сфере цифровизации КНД, в том числе связанными с применением технологий ИИ. В связи с этим требуется создание специальных образовательных программ для сотрудников контрольно-надзорных органов.

¹⁶ Минцифры назвало формулу «развитие VS безопасность» основой при внедрении ИИ // URL: https://rapsinews.ru/digital_law_news/20260212/311594824.html (дата обращения: 20.03.2026).

¹⁷ Первый законопроект о регулировании ИИ разработали в России: что изменится для граждан // URL: <https://fedpress.ru/news/77/economy/3429728> (дата обращения: 20.03.2026).



Перспективы применения ИИ в КНД

В настоящее время Аналитический центр при Правительстве РФ совместно с Минцифры и Минэкономразвития изучает перспективы внедрения ИИ в ведомственные информационные системы контрольно-надзорных органов. Сформированы *возможные сценарии применения ИИ* в КНД для отдельных федеральных органов исполнительной власти.

Примечателен пример регионов, где применение ИИ позволяет *выявлять факты нецелевого использования земельных участков*, осуществлять фиксацию нелегальных построек и заброшенных объектов, а также территорий, заросших борщевиком. Данные, собранные ИИ с помощью видеокамер, прикрепляемых на автомобилях инспекторов Министерства имущественных отношений Московской области, аккумулируются в системе, имеющей интеграцию с Росреестром, в автономном режиме проводится их анализ и обозначаются те объекты, где имеется нарушение¹⁸. Полагаем, что положительный региональный опыт применения ИИ при осуществлении КНД может быть внедрен в деятельность органов государственного контроля (надзора) и других субъектов РФ.

Важнейшим направлением развития применения ИИ при осуществлении государственного контроля (надзора) выступает его институализация, сопровождаемая созданием *специализированных координационных органов*. Так, в соответствии с Указом Президента РФ от 26.02.2026 № 116¹⁹ образована *Комиссия по развитию технологий искусственного интеллекта*, призванная обеспечить межведомственную координацию, что критически важно для КНД, осуществляемой множеством ведомств, формировать унифицированные подходы к внедрению ИИ.

Выводы и предложения

Подводя итог, можно сформулировать следующие выводы и предложения, направленные на совершенствование правового регулирования применения технологий ИИ в КНД:

1. Цифровизация КНД является одним из направлений ее совершенствования. Ключевые инструменты реформы КНД — цифровая платформа «Типовое облачное решение системы автоматизации контрольно-надзорной деятельности» и трансформация риск-ориентированного подхода, связанная с динамичным ранжированием рисков.

2. Российская модель правового регулирования ИИ должна, с одной стороны, стимулировать внедрение ИИ, а с другой — устанавливать надежные гарантии защиты прав граждан и бизнеса от возможных рисков алгоритмизации. Принятие

¹⁸ В Подмоскowie появился земельный нейропатруль // URL: <https://rg.ru/2025/09/01/reg-cfo/vkalyvaiut-roboty.html> (дата обращения: 03.03.2026).

¹⁹ Указ Президента РФ от 26.02.2026 № 116 «О Комиссии при Президенте Российской Федерации по вопросам развития технологий искусственного интеллекта» // СЗ РФ. 2026. № 9. Ст. 1023.

федерального закона о госрегулировании ИИ, основанного на риск-ориентированном подходе, призвано устранить правовую неопределенность и создать унифицированные основания для КНД.

3. Основными направлениями применения ИИ в КНД являются: информационно-аналитическое, контрольно-аналитическое и обеспечительное. Основные типы операций, осуществление которых позволяет применять ИИ в КНД, следующие: прогнозирование; идентификация объектов; учет и систематизация данных. Проведен их анализ. С учетом общей направленности приоритета предупреждения нарушений прогнозирование (предиктивная аналитика) является наиболее значимым применением ИИ в КНД и сопровождается, как правило, непрерывным мониторингом.

4. Основными проблемами применения ИИ при осуществлении КНД, требующими системного подхода, являются: проблема защиты информации, в том числе персональных данных субъектов контроля (надзора) при функционировании информационных систем в рамках КНД; проблема определения правового статуса ИИ, в том числе определение субъекта ответственности (разработчик, оператор либо инспектор, утвердивший решение) в случае сбоя алгоритма или причинения ущерба неправомерным решением, принятым ИИ; проблема дефицита кадров сотрудников контрольно-надзорных органов, обладающих профессиональными компетенциями в сфере цифровизации КНД.

БИБЛИОГРАФИЯ

1. *Добробаба М. Б., Чаннов С. Е.* Система управления рисками применения искусственного интеллекта в государственном управлении : монография / под ред. М. Б. Добробабы. — Саратов : Амирит, 2025. — 121 с.
2. *Добробаба М. Б., Чаннов С. Е., Евсиков К. С.* Правовое обеспечение применения цифровых технологий в государственном управлении / под ред. М. Б. Добробабы. — Саратов : Амирит, 2024. — 160 с.
3. *Иксанов Р. А., Владимиров И. А., Токолов А. В.* Правовое регулирование цифровизации контрольно-надзорной деятельности в сфере природопользования // Административное право и процесс. — 2025. — № 9. — С. 37—40.
4. Искусственный интеллект в юридической деятельности : учебник для вузов / под ред. С. Е. Чаннова. — М. : Юрайт, 2026. — 131 с.
5. *Ковалев С. Д.* Ответственность за ошибки искусственного интеллекта // Аграрное и земельное право. — 2024. — № 8 (236). — С. 67—69.
6. *Мартынов А. В.* Актуальные вопросы применения искусственного интеллекта при осуществлении контрольно-надзорной деятельности органов исполнительной власти // Вестник Нижегородского университета имени Н.И. Лобачевского. — 2020. — № 2. — С. 175—186.





**Сергей Васильевич
СОЛОВКИН,**

старший преподаватель
кафедры
информационного права
и цифровых технологий,
научный сотрудник НОЦ
правового регулирования
в сфере высоких
технологий НИИ
Университета имени
О.Е. Кутафина (МГЮА),
кандидат юридических наук
svsolovkin@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

Генеративный искусственный интеллект как инструмент манипуляции: правовые вызовы и пределы регулирования¹

Аннотация. Статья посвящена правовому анализу манипулятивного воздействия на сознание и поведение человека, осуществляемого посредством систем генеративного искусственного интеллекта. На основе психологической и правовой доктрины сформулировано авторское определение манипулятивного воздействия с использованием систем ИИ как самостоятельной правовой категории, охватывающей политическую, коммерческую, межличностную и психоэмоциональную сферы. Выявлены ключевые технологические механизмы такого воздействия (большие языковые модели, технологии синтеза аудиовизуального контента (дипфейки), персонализированные рекомендательные алгоритмы) и приведены случаи их манипулятивного применения. Сформулированы предложения по совершенствованию российского законодательства, включающие введение легального определения манипулятивного воздействия с использованием систем ИИ, прямой запрет на разработку и использование систем ИИ с манипулятивным функционалом, а также институциональные механизмы контроля.

Ключевые слова: цифровая трансформация, информационная безопасность, информационное право, цифровое право, право искусственного интеллекта, персональные данные, искусственный интеллект, генеративный искусственный интеллект, манипуляция сознанием и поведением, угрозы искусственного интеллекта

DOI: 10.17803/2311-5998.2026.142.6.040-046

Sergey V. SOLOVKIN,

Senior Lecturer of the Chair of Information Law and Digital Technologies,
Research Fellow of the Research and Education Centre for Legal Regulation in the
Field of High Technologies of the Research Institute,
Kutafin Moscow State Law University (MSAL), Cand. Sci. (Law)
svsolovkin@msal.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Generative Artificial Intelligence as a Tool of Manipulation: Legal Challenges and the Limits of Regulation

Abstract. This article presents a legal analysis of manipulative influence on human consciousness and behavior carried out by means of generative artificial intelligence (GAI) systems. Drawing on psychological and legal

¹ Исследование выполнено в рамках программы стратегического академического лидерства «Приоритет-2030».

doctrine, the author formulates an original definition of AI-assisted manipulative influence as an independent legal category encompassing the political, commercial, interpersonal and psycho-emotional spheres. The article identifies the principal technological mechanisms of such influence and cases of their manipulative deployment. The article puts forward proposals for the reform of Russian law, including the introduction of a statutory definition of AI-assisted manipulative influence, a direct prohibition on the development and use of AI systems with manipulative functionality, and institutional oversight mechanisms.

Keywords: digital transformation, information security, information law, digital law, artificial intelligence law, personal data, artificial intelligence, generative artificial intelligence, manipulation of consciousness and behavior, artificial intelligence threats

Понятие манипулятивного воздействия с использованием систем генеративного искусственного интеллекта

Стремительное распространение систем генеративного искусственного интеллекта (ГИИ) в последние годы фундаментально изменило информационную среду, в которой существует современный человек. Одним из наиболее острых вызовов, обусловленных применением ГИИ, является их манипулятивный потенциал².

Разработка надлежащего правового инструментария противодействия манипулятивным практикам с применением систем ГИИ предполагает прежде всего последовательное доктринальное конструирование соответствующей категории. Что следует понимать под манипулятивным воздействием применительно к системам ГИИ?

В психологической науке понятие манипуляции разработано достаточно детально. Е. Л. Доценко, чья концепция по праву признается классической в отечественной психологии, определяет манипуляцию как «вид психологического воздействия, искусное исполнение которого ведет к скрытому возбуждению у другого человека намерений, не совпадающих с его актуально существующими желаниями»³. Данное определение фиксирует три сущностных признака манипуляции: во-первых, скрытый (латентный) характер воздействия; во-вторых, направленность на изменение внутренних психических состояний адресата; в-третьих, рассогласование между вносимыми установками и исходными намерениями адресата, т.е. воздействие вопреки его подлинной воле.

Рецепция психологической категории манипуляции в правовую науку сопряжена с рядом концептуальных трудностей. В отличие от таких явлений, как обман (введение в заблуждение относительно фактических обстоятельств) или

² Минбалева А. В. Риски и угрозы агентского искусственного интеллекта (agentic AI) // Информационное право. 2025. № 3 (85). С. 10—13.

³ Психология манипуляции: феномены, механизмы и защита. М. : ЧеРо ; Изд-во МГУ, 1997.



принуждение (прямое давление на волю субъекта), манипуляция не предполагает ни ложного утверждения в строгом смысле, ни применения силы или угрозы. Она действует через формально достоверную или нейтральную информацию, избирательно конструируя информационный контекст таким образом, чтобы направить поведение адресата в заданном направлении при сохранении иллюзии его свободного выбора. Именно эта особенность делает манипуляцию наиболее труднодоступной для правового регулирования и одновременно наиболее опасной с точки зрения прав личности.

Применительно к системам ГИИ указанные трудности многократно возрастают. Как отмечает А. А. Симонян, анализируя угрозы применения систем ГИИ, «опасность такой технологии заключается в психологическом давлении на различные группы лиц с целью манипуляции общественным мнением граждан, шантажа, мошенничества или клеветы»⁴. Вместе с тем представляется, что данный перечень не является исчерпывающим: манипулятивный потенциал ГИИ не сводится к конкретным правонарушениям, но проявляется на более глубоком уровне — уровне систематического подавления когнитивной автономии личности.

В этой связи в настоящей статье предлагается следующая авторская дефиниция: манипулятивное воздействие с использованием систем искусственного интеллекта — это скрытое автоматизированное воздействие, осуществляемое системой ИИ либо лицом посредством системы ИИ, на сознание, эмоциональное состояние и (или) поведение физического лица путем формирования, персонализации и (или) распространения информационного контента с намерением изменить убеждения, решения или действия адресата вопреки его подлинным интересам и (или) без его осознанного согласия на такое воздействие, при этом независимо от того, является ли содержание распространяемой информации ложным.

Технологические механизмы манипулятивного воздействия и актуальные угрозы

Представляется необходимым установить, посредством каких именно инструментов современные системы ГИИ реализуют свой манипулятивный потенциал, и оценить, являются ли соответствующие угрозы лишь теоретическими конструкциями или же они уже нашли документальное подтверждение в общественной практике.

Большие языковые модели представляют собой, пожалуй, наиболее многофункциональный инструмент манипулятивного воздействия. Способность этих систем генерировать связный, стилистически адаптированный текст в режиме реального времени открывает возможность для создания персонализированных убеждающих нарративов в масштабе, ранее технически недостижимом⁵. При

⁴ Симонян А. А. Генеративный искусственный интеллект и DeepFake-технологии как угроза информационной безопасности граждан // Вопросы российского и международного права. 2025. Т. 15. № 2А. С. 166.

⁵ Минбалева А. В. Особенности правовой природы агентского искусственного интеллекта // Аграрное и земельное право. 2025. № 8. С. 75—78.

наличии данных о психологическом профиле конкретного пользователя — его политических взглядах, страхах, ценностях, поведенческих паттернах — система способна автоматически конструировать сообщения, точно эксплуатирующие индивидуальные когнитивные уязвимости. Исследователи по изучению человеко-компьютерного взаимодействия зафиксировали, что гиперперсонализированное воздействие систем ГИИ в режиме реального времени способно формировать устойчивые паттерны компульсивного потребления контента, подрывая когнитивную автономию пользователей, причем в особой зоне риска находятся несовершеннолетние и пожилые люди⁶.

Принципиально важным в контексте правового регулирования является то обстоятельство, что ряд исследователей квалифицирует персонализированные манипулятивные интерфейсы, генерируемые системами ГИИ, как так называемые теневые паттерны (dark patterns) нового поколения, т.е. намеренно вводящие в заблуждение либо психологически эксплуататорские элементы пользовательского взаимодействия⁷. При этом, как установлено в ходе многоуровневого бенчмаркингowego исследования 2025 г., системы ГИИ способны к таким формам психологического вреда, как антропоморфизация ИИ с целью формирования у пользователя эмоциональной зависимости, газлайтинг относительно фактических обстоятельств, а также подрыв самовосприятия и оценки реальности⁸. Следовательно, манипулятивный потенциал больших языковых моделей не ограничивается распространением дезинформации, но проявляется на уровне систематической деструкции когнитивных способностей личности.

Технологии синтеза аудиовизуального контента (диффузионные модели, GAN-архитектуры, модели синтеза речи) — то, что в публичном дискурсе принято обозначать термином «дипфейк-технологии», — образуют второй ключевой вектор манипулятивного воздействия. Возможности этих технологий состоят в создании синтетических аудио- и видеоматериалов, воспроизводящих облик, голос и речевые паттерны реально существующих лиц с качеством, практически неотличимым от подлинных записей. Европейский парламент в аналитическом докладе 2025 г. констатирует, что диффузионные модели значительно упростили создание дипфейков, включая материалы, направленные против несовершеннолетних, что порождает качественно новые угрозы достоинству и безопасности личности⁹.

⁶ *Khraishi R.* [et al.] Real-Time Hyper-Personalized Generative AI Should Be Regulated to Prevent the Rise of “Digital Heroin” // NeurIPS 2025 Position Paper. URL: <https://neurips.cc/virtual/2025/loc/san-diego/poster/121952> (дата обращения: 25.03.2026).

⁷ *Guerrini F.* AI-Driven Dark Patterns: How Artificial Intelligence Is Supercharging Digital Manipulation // Forbes. 17.11.2024. URL: <https://www.forbes.com/sites/federicoguerrini/2024/11/17/ai-driven-dark-patterns-how-artificial-intelligence-is-supercharging-digital-manipulation/> (дата обращения: 25.03.2026).

⁸ *Asif A. et. al.* DarkPatterns-LLM: A Multi-Layer Benchmark for Detecting Manipulative and Harmful AI Behavior. arXiv. 2025 // URL: <https://arxiv.org/pdf/2512.22470.pdf> (дата обращения: 25.03.2026).

⁹ Children and Deepfakes. Briefing. PE 775.855. European Parliament Research Service. March 2025 // URL: [https://www.europarl.europa.eu/regdata/etudes/brie/2025/775855/eprs_bri\(2025\)775855_en.pdf](https://www.europarl.europa.eu/regdata/etudes/brie/2025/775855/eprs_bri(2025)775855_en.pdf) (дата обращения: 25.03.2026).



Документально подтвержденные случаи применения указанных технологий в манипулятивных целях уже исчисляются десятками¹⁰. При этом необходимо особо подчеркнуть, что манипулятивное применение систем ГИИ отнюдь не ограничивается политической сферой.

Рекомендательные алгоритмы и системы микротаргетинга, интегрированные с возможностями ГИИ, образуют третий вектор манипулятивного воздействия, отличающийся наибольшей латентностью. В отличие от дипфейков, создание которых требует целенаправленных усилий, алгоритмическая манипуляция осуществляется в фоновом режиме: система автоматически формирует информационную среду конкретного пользователя таким образом, чтобы максимизировать его вовлеченность или направить его поведение в заданную сторону, при этом сам пользователь, как правило, не осознает факта воздействия. Генеративный ИИ многократно повышает эффективность подобных систем, поскольку позволяет создавать не просто персонализированную, но индивидуально сконструированную информационную реальность для каждого отдельного субъекта¹¹.

Рекомендации по совершенствованию российского законодательства

Действующее российское законодательство не обеспечивает надлежащей правовой защиты физических лиц от манипулятивного воздействия с использованием систем ГИИ.

Необходимым основанием для построения системного регулирования является введение в российское законодательство легального определения манипулятивного воздействия с использованием систем ИИ. По мнению автора, данное определение надлежит закрепить в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в качестве одного из ключевых понятий информационного права, а также отразить в будущих законах в сфере искусственного интеллекта.

Наряду с этим представляется необходимым закрепить понятие «системы ИИ с манипулятивным функционалом», т.е. системы, конструктивные особенности, обучающие данные и (или) алгоритмы которой направлены или систематически приводят к оказанию манипулятивного воздействия в указанном выше смысле. Данная категория необходима для разграничения систем, создающих риск манипуляции в силу своего прямого назначения, и систем, способных быть использованными в манипулятивных целях лишь при определенных условиях

¹⁰ См., например: ВЭФ назвал дипфейки и ИИ главными угрозами для выборов в разных странах // РБК. 11.01.2024. URL: https://www.rbc.ru/technology_and_media/11/01/2024/659fe9ff9a79475f70435f09 (дата обращения: 25.03.2026) ; A fake recording of a candidate saying he'd rigged the election went viral. Experts say it's only the beginning // CNN. 01.02.2024. URL: <https://edition.cnn.com/2024/02/01/politics/election-deepfake-threats-invs> (дата обращения: 25.03.2026) ; Case study: Can we believe what we hear? // URL: <https://www.unesco.org/mil4teachers/en/toolkit-media/indicator-5/activities/ai-disinformation/case-study-2> (дата обращения: 25.03.2026).

¹¹ Asif A. [et. al.] Op. cit.

применения, поскольку правовые последствия для этих двух категорий должны принципиально различаться.

Центральным элементом предлагаемой системы регулирования является нормативный запрет, содержательно аналогичный ст. 5 Регламента ЕС об ИИ, однако адаптированный к российской правовой системе и расширенный с учетом выявленных в настоящей статье пробелов европейского подхода. Предлагается установить следующую систему запретов:

- 1) запрет на разработку и введение в гражданский оборот систем ИИ с манипулятивным функционалом. Лица, осуществляющие разработку систем ИИ на территории Российской Федерации либо предназначенных для использования на территории Российской Федерации, обязаны обеспечить отсутствие в системе функциональных элементов, намеренно направленных на осуществление манипулятивного воздействия в установленном законом смысле. Данный запрет должен подкрепляться обязательной оценкой соответствия системы ИИ на этапе ее сертификации или регистрации;
- 2) запрет на использование систем ИИ с манипулятивным функционалом. Ни один оператор или пользователь системы ИИ не вправе применять ее в целях оказания манипулятивного воздействия на физических лиц; нарушение данного запрета влечет административную или уголовную ответственность в зависимости от степени причиненного вреда и наличия умысла. При этом, следуя логике Регламента ЕС об ИИ, запрет надлежит сформулировать альтернативно — по критерию цели или эффекта, что позволит охватить случаи «непреднамеренной» манипуляции, возникающей вследствие недостаточной осмотрительности разработчика при проектировании системы;
- 3) запрет на использование техник сублиминального воздействия. С учетом стремительного развития нейроинтерфейсных технологий и систем биометрического профилирования представляется целесообразным отдельно запретить применение систем ИИ, воздействующих на сознание человека методами, выходящими за пределы его осознанного восприятия, в том числе посредством встраивания скрытых побудительных стимулов в аудиовизуальный контент;
- 4) в части Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» предлагается расширить действие ст. 15, распространив запрет автоматизированного принятия значимых решений на все случаи использования персональных данных субъекта в целях построения его психологического профиля для нужд манипулятивного таргетирования, независимо от того, имеют ли результаты такого воздействия формально юридически значимый характер.

Эффективность запретительных норм определяется не только их содержанием, но и наличием надлежащего механизма реализации и контроля. В этой связи предлагается следующее:

1. Создание реестра запрещенных систем ИИ с манипулятивным функционалом. Включение системы в реестр должно влечь обязательный запрет ее распространения и использования на территории Российской Федерации; иностранные системы, внесенные в реестр, подлежат блокировке.

2. Введение обязательной оценки манипулятивного риска как самостоятельной процедуры в рамках сертификации систем ИИ высокого риска. Данная процедура



должна предшествовать выводу системы на рынок и включать проверку обучающих данных, алгоритмической архитектуры и функциональных возможностей системы на предмет наличия признаков манипулятивного функционала.

3. Формирование многоуровневой системы ответственности, охватывающей все звенья жизненного цикла системы ИИ: разработчика — за создание системы с манипулятивным функционалом; оператора — за введение в оборот и применение такой системы; пользователя — за намеренное использование систем ИИ общего назначения в манипулятивных целях. При этом разработчик и оператор должны нести повышенную ответственность, основанную на принципе строгой ответственности (без необходимости доказывания вины), аналогично ответственности за вред, причиненный источником повышенной опасности (ст. 1079 ГК РФ), тогда как ответственность пользователя строится на общих началах виновной ответственности.

4. Наделение Роскомнадзора дополнительными полномочиями по расследованию фактов манипулятивного воздействия с использованием систем ИИ, включая право на запрос алгоритмического аудита у разработчиков и операторов.

Таким образом, предлагаемая система мер образует взаимосвязанный нормативный комплекс, обеспечивающий правовую защиту физических лиц от манипулятивного воздействия систем ГИИ.

БИБЛИОГРАФИЯ

1. *Минбалеев А. В.* Особенности правовой природы агентского искусственного интеллекта // Аграрное и земельное право. — 2025. — № 8. — С. 75—78.
2. *Минбалеев А. В.* Риски и угрозы агентского искусственного интеллекта (agentic AI) // Информационное право. — 2025. — № 3 (85). — С. 10—13.
3. Психология манипуляции: феномены, механизмы и защита. — М. : ЧеРо ; Изд-во МГУ, 1997. — 344 с.
4. *Симонян А. А.* Генеративный искусственный интеллект и DeepFake-технологии как угроза информационной безопасности граждан // Вопросы российского и международного права. — 2025. — Т. 15. — № 2А. — С. 165—172.
5. *Asif A.* [et. al.] DarkPatterns-LLM: A Multi-Layer Benchmark for Detecting Manipulative and Harmful AI Behavior. arXiv. 2025 // URL: <https://arxiv.org/pdf/2512.22470.pdf> (дата обращения: 25.03.2026).
6. *Guerrini F.* AI-Driven Dark Patterns: How Artificial Intelligence Is Supercharging Digital Manipulation // Forbes. 17.11.2024. URL: <https://www.forbes.com/sites/federicoguerrini/2024/11/17/ai-driven-dark-patterns-how-artificial-intelligence-is-supercharging-digital-manipulation/> (дата обращения: 25.03.2026).
7. *Khraishi R.* [et al.] Real-Time Hyper-Personalized Generative AI Should Be Regulated to Prevent the Rise of «Digital Heroin». NeurIPS 2025 Position Paper // URL: <https://neurips.cc/virtual/2025/loc/san-diego/poster/121952> (дата обращения: 25.03.2026).

Этические и юридические предпосылки использования искусственного интеллекта субъектами предпринимательской и профессиональной деятельности¹

Аннотация. В настоящее время субъекты предпринимательской и профессиональной деятельности в своей практике все больше внедряют технологии искусственного интеллекта. Алгоритмы и различные языковые модели широко используются для принятия как корпоративных решений, так и решений, направленных на выбор контрагента, на заключение различного рода сделок, включая государственные контракты. Все эти предпосылки оказывают серьезное влияние на юридические условия принятия решений, поднимают ряд этических вопросов. В определенной степени такое положение вещей приводит к социальной и юридической дискриминации, алгоритмической предвзятости и другим отрицательным правовым последствиям (манипуляции или даже монополизации). Существующий Кодекс этики в сфере искусственного интеллекта² в России, а также законопроект об искусственном интеллекте³ лишь отчасти решают те проблемные вопросы, которые возникают как в юридической науке, так и в правоприменительной практике. Хотя, с другой стороны, наоборот, вызывает опасения порядок применения тех положений, которые в нем (законопроекте) отражены. В связи с чем, на наш взгляд, разработанная система правовых средств и принципов, а также создание отраслевых саморегулируемых организаций станет дополняющим механизмом использования искусственного интеллекта как «помощника» для решения рутинных вопросов субъектами предпринимательской и профессиональной деятельности.

Ключевые слова: искусственный интеллект, предпринимательская деятельность, инновационная деятельность, этические принципы, саморегулируемые организации, субъекты профессиональной деятельности, юридические предпосылки, система правовых средств



**Ольга Викторовна
СУШКОВА,**

доцент кафедры
информационного права
и цифровых технологий
Университета имени
О.Е. Кутафина (МГЮА),
кандидат юридических
наук, доцент
ovsushkova@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2026.142.6.047-054

¹ Исследование выполнено в рамках программы стратегического академического лидерства «Приоритет-2030» (Центр компетенций «Киберправо»).

² Кодекс этики в сфере искусственного интеллекта // СПС «КонсультантПлюс» (дата обращения: 17.04.2026).

³ Проект Федерального закона «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации» (подготовлен Минцифры России, ID проекта 02/04/03-26/00166424) (не внесен в ГД ФС РФ, текст по состоянию на 18.03.2026) // СПС «КонсультантПлюс». Текст документа приведен в соответствии с публикацией на сайте <https://regulation.gov.ru/> по состоянию на 18.03.2026.

Olga V. SUSHKOVA,

*Associate Professor of the Department of Information Law and Digital Technologies
of the Kutafin Moscow State Law University (MSAL),
Cand. Sci. (Law), Associate Professor
ovsushkova@msal.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993*

Ethical and Legal Prerequisites for the Use of Artificial Intelligence by Business and Professional Entities

Abstract. *Currently, business and professional entities are increasingly implementing artificial intelligence technologies in their practice. Algorithms and various language models are widely used to make both corporate and decisions aimed at choosing a counterparty and concluding various types of transactions, including government contracts. All these prerequisites have a serious impact on both the legal conditions for decision-making and raise a number of ethical issues. To a certain extent, this state of affairs leads to social and legal discrimination, algorithmic bias, and other negative legal consequences such as manipulation or even monopoly. The existing Codes of Ethics in the field of artificial intelligence in Russia, as well as the draft law on artificial intelligence, only partially address these challenging issues, which are developing both in legal scholarship and in law enforcement practice. However, on the other hand, concerns have arisen regarding the application of the provisions reflected in the draft law. Although, on the other hand, on the contrary, there are concerns about the application of those provisions that are reflected in it (the draft law). In this regard, in our opinion, the developed system of legal means and principles, as well as the creation of industry self-regulatory organizations, will complement the mechanism for using artificial intelligence as an «assistant» to solve routine issues by business and professional entities.*

Keywords: *artificial intelligence, entrepreneurial activity, innovative activity, ethical principles, self-regulating organizations, subjects of professional activity, legal prerequisites, system of legal means*

Введение

В настоящее время цифровизация охватывает все сферы общественных отношений путем реализации прорывных технологических инноваций. Однако такая ситуация задает больше вопросов, чем предлагает ответов. Фрагментарное правовое регулирование общественных отношений в сфере предпринимательской и профессиональной деятельности, осложненных применяемыми цифровыми технологиями, заставляет научное сообщество и органы законодательной власти принять решение, которое не только позволило бы объективно, в реальном вре-

мени использовать существующие прорывные технологии и программное обеспечение, но и сформировало правовые критерии применения искусственного интеллекта (ИИ). Однако есть опасения, что будущее регулирование ИИ, вероятно, останется фрагментированным из-за отсутствия коллективного видения общих целей и расходящихся интересов в реализации политики, стратегий и практик в области ИИ. Поэтому основой эффективной модели ИИ должны стать этические нормы и принципы, а именно *прозрачность, объяснимость и подотчетность*.

Прозрачность означает, что системы ИИ разрабатываются и используются таким образом, чтобы обеспечить надлежащую отслеживаемость и объяснимость, одновременно информируя людей о том, что они взаимодействуют с системой ИИ, а также должным образом информируя пользователей о возможностях и ограничениях этой системы ИИ в отношении прав отдельных субъектов (п. 1.2 Кодекса этики в сфере ИИ об уважении автономии и свободы воли человека).

Объяснимость означает возможность аргументированно доказывать на уровне отдельных пользователей и на коллективном уровне, если система ИИ затрагивает интересы как отдельного физического или юридического лица, так и группы лиц (п. 1.5 Кодекса этики в сфере ИИ).

Подотчетность тесно связана с *принципом справедливости* и требует создания механизмов, обеспечивающих ответственность за системы ИИ и результаты их использования как до, так и после их разработки, внедрения и применения. В этой части следует указывать, что при наступлении неблагоприятных последствий ответственность за вред, причиненный ИИ (как источником повышенной опасности), будет нести разработчик или правообладатель программы (разд. 2, п. 2.1 Кодекса этики в сфере ИИ).

Кроме того, следует назвать и иные принципы, обозначенные в Кодексе этики в сфере ИИ: недискриминация (п. 1.4), соответствие закону (п. 1.3).

Следует отметить, что вышеуказанные этические принципы ИИ неразрывно связаны с принципами, которые отражены в гражданском законодательстве (например, в ст. 1 ГК РФ), и указывают на тот факт, что правовые категории, которые отражены в нормах Гражданского кодекса РФ (например, в ст. 128)⁴, являются основополагающими для регулирования общественных отношений в сфере предпринимательской и профессиональной деятельности.

Помимо этих этических принципов, будущее регулирование ИИ должно учитывать этические темы и связанные с ними вопросы.

Теоретическая основа: этические предпосылки

Исследования, проводимые учеными в области ИИ, достигли достаточного уровня обоснованности понимания текущей ситуации благодаря изучению структуры предметной области и необходимости использования эвристических методов с помощью все более интеллектуальных технологий, таких как экспертные системы, машинное обучение, глубокое обучение и сегодня — большие языковые модели.

⁴ Гражданский кодекс РФ (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 31.07.2025, с изм. от 25.03.2026; с изм. и доп., вступ. в силу с 01.08.2025) // СЗ РФ. 1994. № 32. Ст. 3301.



Так, например, в работе⁵ Ю. С. Харитоновой и В. С. Савиной отмечается, что в современном промышленном производстве наблюдается тенденция комбинирования аппаратного и программного обеспечения (hardware и software); это необходимо для того, чтобы технологии искусственного интеллекта приобрели большую практическую значимость. Неслучайно исследователи отмечают, что «для прикладных систем потребность в комбинации различных методов искусственного интеллекта с функциональными приложениями становится все более серьезной»⁶.

Е. А. Суханов предостерегает, что «можно констатировать отсутствие сколько-нибудь серьезных оснований для кардинального пересмотра или полного отказа от сложившихся традиционных цивилистических подходов, которые пока не только не препятствуют развитию процесса цифровизации, но и позволяют в необходимой мере осуществлять его юридическое оформление в сфере имущественного оборота»⁷.

Тем не менее можно утверждать, что взаимосвязь между технологией и правом многогранна и динамична. На практике существуют два способа повышения с помощью технологии эффективности права: *первый* — когда научное развитие применяется к праву (этот подход получил название «вычислительные юридические исследования»); *второй* — когда изменение рыночных условий приводит к дальнейшему развитию технологий, улучшающих предоставление юридических услуг (этот подход назван LegalTech⁸). Иногда эти два подхода можно комбинировать, например, при принятии корпоративных или иных решений⁹ в сфере предпринимательской и профессиональной деятельности.

Внедрение новых технологий в законодательство обычно влечет за собой необходимость разработки новых правил; при разработке и применении новых правил регулирующие органы учитывают социальные, этические и правовые аспекты. По сути, разработка регулирования зависит от содержания технологии, которая может применяться в различных областях. В своем фундаментальном смысле технология относится к методам, улучшающим выполнение существующей задачи. Поэтому в более широком смысле регулирование технологий законом можно рассматривать как область права и технологий.

⁵ Харитонова Ю. С., Савина В. С. Технология искусственного интеллекта и право: вызовы современности // Вестник Пермского университета. Юридические науки. 2020. № 3. С. 526.

⁶ WIPO Technology Trends 2019 Artificial Intelligence. WIPO, 2019. P. 33.

⁷ Суханов Е. А. О гражданско-правовых проблемах цифровизации // Вестник гражданского процесса. 2025. № 1. С. 37—52.

⁸ Минбалева А. В. Основные проблемы и перспективы развития LegalTech в России в условиях цифровизации // Юрист. 2022. № 9. С. 43—48.

⁹ См.: LegalTech в сфере предпринимательской деятельности : монография / Р. Н. Адельшин, Е. И. Андреева, Л. В. Андреева [и др.] ; отв. ред. И. В. Ершова, О. В. Сушкова. М. : Проспект, 2023.

Теоретическая основа: юридические предпосылки

В настоящее время дефиниция ИИ, предлагаемая законодателем, сформулирована следующим образом: ИИ — «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений»¹⁰. Данное определение не совсем точно выражает суть алгоритма, поскольку ИИ, являясь языковой моделью, направлен на создание именно алгоритмической конструкции (модели) с определенным набором функций для решения четких задач.

Внедрение ИИ в сферу бизнеса и профессиональной деятельности в настоящее время вызывает ряд опасений. Ситуация осложняется тем, что все больше различные системы ИИ, сложные программные продукты не только отражают в своем содержании решение рутинных задач, но и затрагивают область права. Последнее, на мой взгляд, ведет к необоснованным рискам и возможным потерям при реализации бизнес-идей¹¹.

С другой стороны, алгоритмы машинного обучения могут обрабатывать огромные объемы судебной практики и доказательств гораздо быстрее, чем любой человек, выявляя соответствующие авторитетные источники или закономерности в данных. Юридические фирмы и суды уже используют инструменты на основе ИИ для электронного поиска доказательств, анализа документов и анализа договоров, что значительно сокращает время и затраты, необходимые для выполнения этих трудоемких задач¹².

Важно отметить, что генеративный ИИ позволяет исследователям и практикам переосмыслить традиционные юридические задачи обработки естественного языка, такие как суммирование, поиск информации или классификация предложений, как задачи генерации текста. Это привело к более унифицированному методологическому подходу по использованию субъектами предпринимательского и профессионального сообществ ИИ для решения текущих внутренних и

¹⁰ Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года) // СЗ РФ. 2019. № 41. Ст. 5700.

¹¹ Например, Anthropic разработана новая ИИ-модель Claude Mythos. Она настолько мощная, что ее якобы боялся выпускать в широкий доступ (см. об этом: URL: <https://www.mn.ru/smart/anthropic.razrabotala-novuyu-ii-model-claude-mythos-ona-nastolko-moshhnaya-cto-ee-yakoby-boyatsya-vypuskat-v-shirokij-dostup> (дата доступа 17.04.2026)).

¹² См., например, ПНСТ 840-2023 (ISO/IEC TR 24368:2022). Предварительный национальный стандарт Российской Федерации. Искусственный интеллект. Обзор этических и общественных аспектов (утв. и введен в действие приказом Росстандарта от 16.11.2023 № 60-пнст; введен в действие с 01.01.2024 на период до 01.01.2027 (см.: М. : Институт стандартизации, 2023)).



внешних задач (включая и обмен данными при подготовке условий договора как крупной сделки).

Все эти предпосылки указывают на то, что наступила эра ИИ в правовой сфере. Хотя это мощный инструмент, его использование в правовой системе влечет за собой ответственность за сохранение целостности верховенства права. Значительная часть инфраструктуры ИИ, лежащей в основе юридических технологий, по своей сути ориентирована на англоязычные тексты и принципы общего права, что не совсем подходит для российской правовой системы. Как верно указывает Е. А. Суханов, «в англо-американском Common Law... исторически сложилась иная система правовых режимов в виде real property, personal property, intellectual property и др., причем объектами каждого из них являются и вещи, и имущественные права (ибо здесь в рамках категории “имущество” (property) отсутствует юридическое разделение вещных и обязательственных прав, присущее континентально-европейскому праву)»¹³.

В связи с этим любая будущая система, направленная на совершенствование предпринимательского оборота, должна прозрачно устранять негативные последствия и создавать механизмы для обеспечения соответствия существующим требованиям.

Основные проблемы и пробелы

Анализ и разработка этических и юридических предпосылок по использованию ИИ в практической деятельности субъектами бизнеса направлена не только на возможность повседневной практики, но и на минимизацию рисков в хозяйственном обороте. Существующие модели ИИ не всегда могут определить степень риска субъекта предпринимательской деятельности при его вступлении, например, в те или иные договорные правоотношения. При этом немаловажными остаются риски, связанные с внутренними проблемами организации. Сюда входят проблемы частых увольнений, утечки информации, неэффективной коммуникации в больших коллективах, низкой мотивации работников, выполняющих рутинную работу.

Среди внешних рисков выделяются ярче всего риски экономических потерь в связи с изменениями на рынке (падением курса валют, изменением конъюнктуры рынка, снижением стоимости активов и различных ресурсов). Кроме того, важным и наиболее актуальным риском остается неверный подбор контрагентов. Поэтому предприниматели используют ИИ, который может такие риски снизить путем анализа соответствующего рынка или области человеческого взаимодействия, в результате которого могут выявиться конкретные проблемы.

Тем не менее решение указанных проблем возможно при помощи обращения к форме саморегулируемых организаций¹⁴.

¹³ Суханов Е. А. О гражданско-правовых проблемах цифровизации // Вестник гражданского процесса. 2025. № 1. С. 45.

¹⁴ Сушкова О. В. Гражданско-правовые проблемы саморегулирования субъектов на рынке цифровых финансовых активов // Гражданское право. 2021. № 4. С. 21—26.

Представляется, что ключевым фактором среди таких мер может стать создание саморегулируемых организаций (СРО) в области ИИ. Существующие в России организации и объединения в этой сфере, такие как «Альянс», могут считаться СРО только в широком смысле¹⁵ и не подпадают под действие законодательства о СРО¹⁶.

Выводы и предложения

В настоящее время прогнозировать какие-либо юридические модели тотального применения ИИ в сфере предпринимательской и профессиональной деятельности не приходится. Однако ввиду того, что бизнес, юридическое сопровождение предпринимательской деятельности и технологии всегда находятся в тесной взаимосвязи, вероятно, это будет происходить по нескольким взаимосвязанным направлениям.

Во-первых, можно ожидать, что субъекты предпринимательской деятельности для сопровождения большинства бизнес-процессов остановятся на гибридных подходах, сочетающих в себе сильные стороны как классических методов и форм реализации юридической практики и этики, так и автоматизированных. Сочетание этих двух подходов может устранить такие ограничения, как фактические искажения, и повысить надежность моделей ИИ для решения важных правовых задач.

Во-вторых, что немаловажно, нормативно-правовые и этические принципы будут определять пути развития ИИ в праве, чтобы обеспечить конфиденциальность и не только соответствовать законодательству с формальной точки зрения, но и отражать суть ее правовой природы.

БИБЛИОГРАФИЯ

1. *Ершова И. В.* Саморегулирование предпринимательской и профессиональной деятельности: вопросы теории и законодательства // Актуальные проблемы российского права. — 2014. — № 10 (47).
2. *Медведев А. И.* Саморегулирование как инструмент обеспечения прозрачности искусственного интеллекта // Предпринимательское право. — 2025. — № 3. — С. 40—43.
3. *Минбалеев А. В.* Основные проблемы и перспективы развития LegalTech в России в условиях цифровизации // Юрист. — 2022. — № 9. — С. 43—48.
4. *Суханов Е. А.* О гражданско-правовых проблемах цифровизации // Вестник гражданского процесса. — 2025. — № 1. — С. 37—52.

¹⁵ *Ершова И. В.* Саморегулирование предпринимательской и профессиональной деятельности: вопросы теории и законодательства // Актуальные проблемы российского права. 2014. № 10 (47). С. 2144.

¹⁶ *Медведев А. И.* Саморегулирование как инструмент обеспечения прозрачности искусственного интеллекта // Предпринимательское право. 2025. № 3. С. 40—43.



5. Сушкова О. В. Гражданско-правовые проблемы саморегулирования субъектов на рынке цифровых финансовых активов // Гражданское право. — 2021. — № 4. — С. 21—26.
6. Харитонова Ю. С., Савина В. С. Технология искусственного интеллекта и право: вызовы современности // Вестник Пермского университета. — Юридические науки. — 2020. — № 3.
7. LegalTech в сфере предпринимательской деятельности : монография / Р. Н. Адельшин, Е. И. Андреева, Л. В. Андреева [и др.] ; отв. ред. И. В. Ершова, О. В. Сушкова. — М. : Проспект, 2023. — 200 с.

Система правовых и иных средств обеспечения применения искусственного интеллекта в сфере воздушного транспорта

Аннотация. Интеграция искусственного интеллекта в воздушный транспорт требует создания комплексной системы мер, обеспечивающих безопасное и эффективное применение указанных технологий в сфере авиации. Настоящая статья посвящена комплексному анализу системы правовых и иных средств обеспечения применения искусственного интеллекта в сфере воздушного транспорта. Автором классифицированы правовые средства, а также выделено несколько иных средств, способствующих гармоничному и законному применению передовых авиационных технологий. В статье обосновывается вывод о том, что средства обеспечения использования искусственного интеллекта в сфере авиации представляют собой многоуровневую сложную структуру, элементы которой тесно взаимосвязаны и зависят друг от друга. Делается вывод о том, что единственным возможным путем совершенствования и стимулирования применения искусственного интеллекта в воздушном транспорте является междисциплинарный подход, обеспечивающий комплексный характер совершенствования правового регулирования.

Ключевые слова: искусственный интеллект, беспилотное воздушное судно, система правовых средств, технические стандарты искусственного интеллекта, этика, воздушный транспорт



**Алексей Сергеевич
ТИТОВ,**

эксперт по
взаимодействию
с госорганами
Акционерного общества
«Международный аэропорт
Шереметьево»
sled.titov@mail.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2026.142.6.055-062

Aleksey S. TITOV,

Expert on interaction with government agencies
JSC "Sheremetyevo International Airport"
sled.titov@mail.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

System of Legal and other Means of Ensuring the Use of Artificial Intelligence in the Air Transport Sector

Abstract. The integration of artificial intelligence into air transport requires the creation of a comprehensive system of measures that ensure the safe and effective use of these technologies in the aviation sector. This article provides a comprehensive analysis of the legal and other means of ensuring the use of artificial intelligence in the aviation sector. The author classifies the legal means and identifies several other means that contribute to the harmonious and legal use of advanced aviation technologies. The article concludes that the means of ensuring the use of artificial intelligence in the

© Титов А. С., 2026

aviation sector are a multi-level and complex structure, with elements that are closely interconnected and dependent on each other. It is concluded that the only possible way to improve and promote the use of artificial intelligence in air transport is through an interdisciplinary approach that ensures a comprehensive improvement of legal regulation.

Keywords: *artificial intelligence, unmanned aerial vehicle, legal framework, technical standards for artificial intelligence, ethics, air transport*

В настоящее время вопрос необходимости использования технологий искусственного интеллекта особенно актуален в связи с глобальной цифровизацией авиационной отрасли и внедрением элементов автономности в системы управления воздушных судов, что, безусловно, положительным образом влияет на обеспечение безопасности полетов, экономическую и экологическую выгоду для эксплуатанта и государства.

Воздушные судна являются источником повышенной опасности, в связи с чем законодатели разных государств справедливо уделяют особое внимание вопросам правового регулирования данного вида транспорта. Его трансграничный характер обуславливает необходимость единого подхода к нормативному регулированию в сфере авиации.

В работе самолета используется колоссальное количество электронных систем, что делает его одним из наиболее высокотехнологичных транспортных средств на сегодняшний день, однако по мере развития информационных технологий и самолетостроения усложняется и их программно-аппаратная составляющая¹.

Вместе с тем использование новых технологий, в частности искусственного интеллекта, подразумевает определенную степень риска, что, в свою очередь, требует серьезной проработки вопроса безопасности практического применения таких технологических решений.

В данном случае целесообразно рассматривать вопрос с точки зрения системы правовых и организационных средств обеспечения применения искусственного интеллекта в сфере воздушного транспорта, которые позволяют использовать ИИ в авиации, способствуют его гармоничному развитию с обязательным соблюдением баланса эффективности и безопасности.

Целесообразно выделить три элемента системы правовых средств: международно-правовое регулирование, национальное регулирование и договорные средства.

Юридическая сила международно-правового регулирования продиктована частью 4 ст. 15 Конституции РФ², согласно которой нормы международного права являются составной частью правовой системы Российской Федерации и имеют приоритет перед национальными законами. Статья 3 Воздушного кодекса РФ³

¹ Матюха С. В. Развитие применения искусственного интеллекта в беспилотных авиационных системах // Транспортное дело России. 2024. № 3. С. 252—256.

² Конституция Российской Федерации (принята всенародным голосованием 12.12.1993, с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).

³ Воздушный кодекс РФ от 19.03.1997 № 60-ФЗ // СЗ РФ. 1997. № 12. Ст. 1383.

определяет, что в случае установления международным договором иных правил, чем те, которые предусмотрены Воздушным кодексом РФ, применяются правила международного договора. Таким образом, международно-правовое регулирование как самостоятельный элемент системы правовых средств, с учетом трансграничности следования авиарейсов, имеет важное значение в формировании и функционировании права в сфере авиации.

Имеется множество международно-правовых актов, регламентирующих вопросы в сфере воздушного транспорта, однако основополагающим актом является Конвенция о международной гражданской авиации 1944 г. (Чикагская конвенция), положившая начало деятельности Международной организации гражданской авиации (International Civil Aviation Organization, ICAO — ИКАО). Согласно ст. 37 данной Конвенции все государства-участники, которых на сегодняшний день 193, обязуются обеспечить максимальное единообразие правил, стандартов, процедур, касающихся воздушных судов и аэронавигации⁴. На данном базисном принципе основывается и единый уровень авиационной безопасности для воздушных судов разных стран, в число которых входит и Российская Федерация. Такие факторы, как разный уровень экономического и технологического развития, в данном случае нивелируются едиными общепризнанными и обязательными стандартами. Таким образом, воздушное судно будет в одинаковой степени проходить предполетную подготовку в разных странах.

Также следует обратить внимание на нормативные документы ИКАО, которые оказывают значительное влияние на развитие национальных нормативных документов в сфере воздушного транспорта и учитываются Министерством транспорта РФ при разработке Федеральных авиационных правил, являющихся императивными актами.

В рамках правового регулирования искусственного интеллекта в сфере авиационного транспорта следует обратить внимание на один из крупных нормативных правовых актов — Закон об искусственном интеллекте, принятый Европейским парламентом 13.03.2024 и одобренный Советом Евросоюза 21.05.2024. Помимо основных положений об искусственном интеллекте, данный акт определяет риск-ориентированный подход к регулированию вопросов применения искусственного интеллекта и относит беспилотные авиационные системы к высокорисковому классу.

Каждая страна в национальном законодательстве в той или иной степени закрепляет нормы права, регулирующие отношения, возникающие при использовании искусственного интеллекта. Если говорить о нормативных правовых актах Российской Федерации, то следует отметить ряд законов и подзаконных нормативных правовых актов, регламентирующих в той или иной степени применение искусственного интеллекта в сфере воздушного транспорта:

- 1) Воздушный кодекс РФ, содержащий основные нормы права, регламентирующие порядок использования воздушного пространства, основные вопросы деятельности в сфере авиации, включая использование беспилотных авиационных систем;

⁴ Конвенция о международной гражданской авиации (заключена в г. Чикаго 07.12.1944).



- 2) Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»⁵. Именно данный акт создал правовую возможность использования регуляторных (цифровых) песочниц для проведения испытаний инновационных технологий, в том числе беспилотных авиационных систем, снимая административные ограничения, установленные действующим законодательством в сфере воздушного транспорта;
- 3) постановление Правительства РФ от 23.05.2024 № 641 как пример введения экспериментального правового режима для беспилотных летательных аппаратов, использующих алгоритмы искусственного интеллекта. Полученные результаты имеют важное значение для дальнейшего формирования и изменения правовых норм в данной части с целью безопасного и наиболее эффективного использования автономных авиационных систем;
- 4) Федеральные авиационные правила «Сертификация авиационной техники, организаций разработчиков и изготовителей. Часть 21»⁶, определяющие процедуру сертификации беспилотных авиационных систем, которые в том числе используют автоматизацию и алгоритмы искусственного интеллекта. Несоблюдение данных правил влечет привлечение к ответственности, в связи с чем минимальные требования к указанным системам должны быть соблюдены в обязательном порядке.

Перечисленные выше нормативные правовые акты не образуют закрытый перечень. Также параллельно существует регулирование вопросов оборота информации ограниченного доступа (включая персональные данные, коммерческую тайну и т.д.), обеспечения информационной безопасности и безопасности критической информационной инфраструктуры и других не менее важных аспектов, возникающих при использовании искусственного интеллекта.

Тем не менее система правовых средств образует стройную систему норм, которая наглядно показывает многогранность правового регулирования беспилотной авиации, в управлении которой также применяются технологии искусственного интеллекта.

Говоря о договорных средствах, следует отметить, что в настоящее время коммерческие организации, использующие искусственный интеллект в своей деятельности, нередко относят все сведения, связанные с ИИ, к информации ограниченного доступа, к коммерческой тайне. Такой подход к защите информации о технологиях искусственного интеллекта обусловлен высокой степенью их эффективности в производстве и способствует доминированию на рынке товаров и услуг. Вместе с тем часть сведений в общих чертах о применяемых технологиях искусственного интеллекта периодически публикуется в СМИ с целью

⁵ Федеральный закон от 31.07.2020 № 258-ФЗ (в ред. от 31.05.2025) «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации» // СЗ РФ. 2020. № 31 (ч. I). Ст. 5017.

⁶ Приказ Минтранса России от 17.06.2019 № 184 «Об утверждении Федеральных авиационных правил «Сертификация авиационной техники, организаций разработчиков и изготовителей. Часть 21»» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 09.09.2019.

ознакомления общества с новыми технологиями, увеличения доверия к искусственному интеллекту, а также привлечения инвестиций.

К договорным средствам следует отнести договоры на разработку программного обеспечения и аппаратной составляющей с искусственным интеллектом, его обслуживание, пользовательские и лицензионные соглашения. В рамках частного правового регулирования происходит установление прав и обязанностей сторон при реализации продукта на основе искусственного интеллекта.

Тем не менее вопрос распределения ответственности между разработчиком систем искусственного интеллекта, эксплуатантом воздушного судна и поставщиком программно-аппаратной составляющей остается открытым. В настоящее время ответственность за вред, причиненный в результате деятельности искусственного интеллекта в сфере авиации несет владелец воздушного транспорта как источника повышенной опасности, что предусмотрено ст. 1079 ГК РФ.

Помимо правовых средств обеспечения применения искусственного интеллекта, содержание которых фактически сводится к нормам права, следует также выделить организационные и технические средства.

Организационные средства оказывают важное влияние на обеспечение применения искусственного интеллекта, так как представляют собой совокупность административных механизмов, допускающих интеграцию систем искусственного интеллекта в сферу воздушного транспорта без рисков снижения безопасности, эффективности и надежности.

В первую очередь это выражается в масштабном подходе к технологии как таковой со стороны органов публичной власти⁷. Здесь следует отметить роль документов стратегического планирования, которые задают вектор дальнейшего развития права и на принципах и результатах апробации которых с большой долей вероятности будут приниматься или изменяться нормативные правовые акты, чем обуславливается возможность отнесения документов стратегического планирования в том числе и к правовым средствам обеспечения применения искусственного интеллекта.

Одним из основных документов в вопросе применения искусственного интеллекта в сфере транспорта является Национальная стратегия развития искусственного интеллекта на период до 2030 года⁸. Данные меры направлены, в частности, на снятие административных барьеров и создание пилотных зон для тестирования беспилотного транспорта, в том числе воздушного. С учетом вышеуказанной Стратегии разрабатывался ряд других документов стратегического планирования и национальных программ, в рамках которых может реализовываться экономическое стимулирование организаций, внедряющих и развивающих технологии искусственного интеллекта.

⁷ *Добробаба М. Б., Чаннов С. Е.* Система управления рисками применения искусственного интеллекта в государственном управлении : монография / под ред. М. Б. Добробабы. Саратов : Амирит, 2025.

⁸ Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года) // СЗ РФ. 2019. № 41. Ст. 5700.



В связи с трансграничностью и стремлением к унификации законодательства в области обеспечения безопасности полетов значение имеют рекомендации ИКАО, которые определяют мировые ориентиры развития гражданской авиации, в том числе в вопросе применения автономных воздушных судов и автоматизации управления⁹. Стандартизация процессов использования и обслуживания искусственного интеллекта будет способствовать наиболее эффективному его внедрению и совершенствованию. Все результаты тестирования указанной технологии должны быть исследованы центрами компетенций по искусственному интеллекту. Внутренние регламенты по вопросам работы с искусственным интеллектом авиапредприятий также будут способствовать упорядоченной работе в данном направлении. Указанные сведения должны накапливаться и использоваться для дальнейшего совершенствования алгоритмов работы с искусственным интеллектом¹⁰.

Также к организационным средствам относится необходимость подготовки квалифицированных кадров для работы с искусственным интеллектом в области воздушного транспорта. Разработка стандартов и программного обеспечения, производство технического обслуживания требуют специальных познаний в области информационного права и цифровых технологий. Сегодня с учетом развития и цифровизации самого образования появляются программы обучения, связанные с искусственным интеллектом и беспилотными транспортными средствами.

Конечно, когда сфера регулирования касается не только частных, но и публичных интересов, требуется высокий уровень взаимодействия между государственными органами, авиационными предприятиями, разработчиками и поставщиками программно-аппаратной составляющей. Как показывает имеющаяся практика, авиация является сложной экосистемой, законодательство которой носит в большей степени императивный и разрешительный характер. Интеграция, развитие и приведение к единообразию компонентов авиационных систем на международном уровне представляются одной из приоритетных задач для достижения высокого баланса безопасности и эффективности гражданской авиации.

Отдельно в рамках организационных средств необходимо отметить вопросы реализации локальных актов, где применяется искусственный интеллект. Сюда нужно отнести политику использования искусственного интеллекта, которая будет определять пределы применения указанной технологии, регламенты создания интеллектуальных систем, определяющие этапы и контроль разработки систем, реестры.

Следует также обозначить, что в организационные средства входят и вопросы этического характера. Принятый в 2021 г. Кодекс этики в сфере ИИ¹¹ обозначил ключевые принципы, на которых должен основываться искусственный интеллект, в числе которых человекоцентричность, безопасность, ответственность человека, прозрачность и объяснимость, справедливость, защита данных, контроль

⁹ Ананенко А. О. Административно-правовое регулирование применения беспилотных транспортных средств : дис. ... канд. юрид. наук. М., 2024.

¹⁰ Камалов К. Ф., Соколов О. А. Анализ применения искусственного интеллекта в гражданской авиации // Вестник науки. 2023. Т. 3. № 11 (68). С. 896—901.

¹¹ Кодекс этики в сфере ИИ / URL: <https://ethics.a.ai.ru/> (дата обращения: 23.03.2026).

со стороны человека. Указанный Кодекс, выступая в роли мягкого права, также оказывает влияние на формирование стандартов искусственного интеллекта, требований к нему и дальнейшему нормотворчеству.

Использование систем искусственного интеллекта было бы невозможно, а правовое регулирование бессмысленно без технических средств¹².

Именно инженерно-технологическая составляющая лежит в основе функционирования не только самой авиации, но и всей системы искусственного интеллекта в целом.

Технические средства обеспечения применения искусственного интеллекта в сфере воздушного транспорта представляют собой программно-аппаратную единицу, результат цифрового вычисления которой в настоящее время является одним из острых вопросов правового регулирования.

В данную категорию попадают не только автономные авиационные системы, но и электронные помощники, использующие анализ больших данных и машинное зрение в качестве одних из основных инструментов.

Как уже упоминалось выше, вопросы сертификации беспилотных воздушных систем и пилотов в настоящее время относятся к категории разрешительных, при которых проверяется соответствие конструкции воздушного судна программного обеспечения, средств и каналов связи и управления. Однако, если применяются технологии искусственного интеллекта, это требование распространяется на все компоненты, обеспечивающие функционирование искусственного интеллекта, включая вычислительные модули и сенсорные системы.

Также следует отметить необходимость сертификации наземной и облачной инфраструктуры, куда входят центры обучения моделей искусственного интеллекта, аэродромы/вертодромы/станции, центры обработки данных.

В качестве примера можно привести международный стандарт ISO 21384-3-2023 Unmanned aircraft systems — Part 3: Operational procedures¹³, определяющий стандарты эксплуатации беспилотных авиационных систем, включая требования к операторам, осуществляющим полеты в беспилотном воздушном судне, наземным и воздушным операциям, специфике защиты данных и др. Необходимо отметить отечественные стандарты, в частности, в области беспилотной авиации — ГОСТ Р 59519-2021¹⁴, который определяет состав беспилотных авиационных систем и общие технические требования к компонентам систем.

Весьма важным вопросом с точки зрения технической стороны применения искусственного интеллекта является необходимость обеспечения кибербезопасности

¹² Право искусственного интеллекта : учебник / под ред. А. В. Минбалева. 2-е изд., доп. и перераб. Саратов : Амирит, 2025.

¹³ ISO 21384-3-2023 Unmanned aircraft systems — Part 3: Operational procedures. Беспилотные авиационные системы. Часть 3. Правила эксплуатации от 01.10.2026 // URL: <https://cdn.standards.iteh.ai/samples/80124/74015427f9cc492aa692ffa60a962961/ISO-21384-3-2023.pdf> (дата обращения: 24.03.2026).

¹⁴ ГОСТ Р 59519-2021 «Национальный стандарт Российской Федерации. Беспилотные авиационные системы. Компоненты беспилотных авиационных систем. Спецификация и общие технические требования», утв. приказом Росстандарта от 27.05.2021 № 474-ст. М. : Стандартинформ, 2021.



беспилотных авиационных систем¹⁵, использования современных средств защиты информационных каналов связи, недопущения несанкционированного доступа к управлению или смены задачи автономному воздушному судну.

Учитывая, что именно технические средства являются предметом правового регулирования, в том числе в части обязательного соблюдения сертификационных требований, можно сделать вывод о том, что данная категория средств является одной из центральных, так как определяет пределы допустимого использования возможностей искусственного интеллекта.

В заключение следует отметить, что авиационная отрасль представляет собой весьма сложную экосистему. Вопрос обеспечения безопасности полетов и повышения эффективности авиации в большей степени может быть решен с внедрением искусственного интеллекта, однако до настоящего времени имеется ряд вопросов как правового, так и неправового характера, решение которых возможно при системном подходе.

Как было указано, система правовых средств представлена в виде многоуровневой структуры. Обеспечение применения искусственного интеллекта в сфере воздушного транспорта достигается также путем организационных и технических средств. Указанные средства имеют значительное количество пересечений, что позволяет сделать вывод о междисциплинарном подходе к вопросу использования искусственного интеллекта в авиации.

Трансграничный и унифицированный характер регулирования воздушного законодательства требует использования всех инструментов по обеспечению применения новых технологий — от локального до международного уровня. Именно такой подход позволит обеспечить максимально эффективный и безопасный уровень применения искусственного интеллекта в сфере воздушного транспорта.

БИБЛИОГРАФИЯ

1. *Авамчиков В. М., Тимохович А. С., Рожнов И. П.* Цифровая трансформация в авиационной отрасли: возможности и перспективы // Вестник евразийской науки. — 2024. — Т. 16. — № 3.
2. *Ананенко А. О.* Административно-правовое регулирование применения беспилотных транспортных средств : дис. ... канд. юрид. наук. — М., 2024. — 159 с.
3. *Добробаба М. Б., Чаннов С. Е.* Система управления рисками применения искусственного интеллекта в государственном управлении : монография / под ред. М. Б. Добробабы. — Саратов : Амирит, 2025. — 122 с.
4. *Камалов К. Ф., Соколов О. А.* Анализ применения искусственного интеллекта в гражданской авиации // Вестник науки. — 2023. — Т. 3. — № 11 (68). — С. 896—901.
5. *Матюха С. В.* Развитие применения искусственного интеллекта в беспилотных авиационных системах // Транспортное дело России. — 2024. — № 3. — С. 252—256.
6. *Право искусственного интеллекта : учебник / под ред. А. В. Минбалеева.* — 2-е изд., доп. и перераб. — Саратов : Амирит, 2025. — 460 с.

¹⁵ *Авамчиков В. М., Тимохович А. С., Рожнов И. П.* Цифровая трансформация в авиационной отрасли: возможности и перспективы // Вестник евразийской науки. 2024. Т. 16. № 3.

Правовой режим цифровых данных

Развитие правового регулирования рынка данных в России: проблемы и перспективы¹

Аннотация. Статья посвящена анализу современного состояния правового регулирования рынка данных в России как одной из задач ряда национальных целей развития и возможных перспектив его совершенствования. С помощью сравнительно-правового анализа международного и зарубежного опыта обоснована необходимость разработки комплексной концепции правового регулирования рынка данных. На основе методов правового моделирования и институционального проектирования разработаны ключевые элементы содержания данной концепции.

Ключевые слова: концепция, национальные цели развития, правовое регулирование, рынок данных, экономика данных

DOI: 10.17803/2311-5998.2026.142.6.063-069

Aleksey A. YEFREMOV,

Professor of the Information Law and Digital Technologies Department
of the Kutafin Moscow State Law University (MSAL),
Dr. Sci. (Law), Associate Professor
aaefremov@msal.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Development of Legal Regulation of the Data Market in Russia: Problems and Prospects

Abstract. This article analyzes the current state of legal regulation of the data market in Russia as one of the objectives of several national development goals and potential prospects for its improvement. Using a comparative legal analysis of international and foreign experience, the need to develop a comprehensive concept for legal regulation of the data market is substantiated. Based on legal modeling and institutional design methods, key elements of this concept's content are developed.

Keywords: concept, national development goals, legal regulation, data market, data economy



**Алексей
Александрович
ЕФРЕМОВ,**

профессор кафедры
информационного права
и цифровых технологий
Университета имени
О.Е. Кутафина (МГЮА),
доктор юридических наук,
доцент
aaefremov@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

¹ Исследование выполнено в рамках программы стратегического академического лидерства «Приоритет-2030».

Формирование и развитие рынка является необходимым условием достижения национальных целей России, и в первую очередь такой цели, как цифровая трансформация государственного и муниципального управления, экономики и социальной сферы.

Решение данной задачи требует соответствующего правового обеспечения, которое носит межотраслевой характер в силу комплексного характера отношений, возникающих в рамках формирования и развития указанного рынка, а также особенностей публично-правовых и частноправовых статусов его участников.

Анализ повесток и документов международных организаций свидетельствует о том, что единого международно-правового подхода к регулированию рынка данных в настоящее время не сложилось. Государства приоритетно развивают внутренние рынки данных для обеспечения своей конкурентоспособности, стремятся ограничить трансграничные потоки данных (прежде всего персональных данных своих граждан).

В зарубежных странах, как правило, отсутствуют отдельные законодательные акты, регулирующие именно рынок данных, а отдельные вопросы его регулирования рассматриваются в нормативных правовых актах, определяющих правовое регулирование доступа к информации и данных публичного сектора, в том числе государственных информационных систем, порталов и платформ, включая возможности и ограничения повторного использования указанных данных, оказания услуг на основе обработки данных, «маркетплейсов» данных.

В отдельных странах (Южная Корея, Япония) формируются подходы к определению содержания правовых форм организации оборота данных, в том числе соответствующих договоров в данной сфере.

Для России является актуальным определение как общего публично-правового механизма достижения национальных целей развития России на основе определения их правовой природы², так и целевых задач и показателей, направленных на их достижение.

В современной российской юридической научной литературе практически отсутствуют комплексные системные исследования, посвященные формированию и развитию рынка данных и правового обеспечения такого формирования и развития. При этом следует отметить, что такие исследования проводятся, например, в отношении энергетического рынка³.

В отношении правового регулирования рынка данных можно выделить исследования, связанные с определением объекта отношений на данном рынке, в том числе рассмотрение данных как товара⁴, с регулированием оборота данных в

² Ефремов А. А. Адаптация экспериментального правового регулирования для достижения национальных целей развития Российской Федерации // Вестник Воронежского государственного университета. Серия : Право. 2025. № 3 (62). С. 164—172.

³ Энергетические рынки: проблемы и задачи правового регулирования : монография / под ред. В. В. Романовой. М. : Юрист, 2018.

⁴ Христова С. М. Данные как товар: анализ противоречий теоретического и прагматического подхода // Вестник Московского университета имени С.Ю. Витте. Серия 1 : Экономика и управление. 2025. № 1 (52). С. 77—86.

рамках цифровых платформ⁵, с проблемами регулирования больших данных⁶, с оборотом цифровых данных⁷ и данных в целом⁸, с проблемами конкуренции⁹.

Таким образом, нерешенными до настоящего времени в доктрине публичного права и частного права остаются вопросы:

- определения понятия рынка данных и содержания отношений на указанном рынке;
- определение правового статуса участников рынка данных;
- определение правового режима объектов оборота на рынке данных.

В этой связи формирование и развитие правового регулирования рынка данных должно быть основано на единой концепции, использование которой нормотворческими органами позволит обеспечить системность такого регулирования. Разработанная в рамках программы стратегического академического лидерства «Приоритет-2030» Концепция правового регулирования рынка данных (далее — Концепция) включает следующие ключевые положения.

Предметом Концепции являются принципы правового регулирования рынка данных в Российской Федерации, основы правового статуса участников рынка данных в России, основы правового режима данных как объекта оборота в России, а также принципы трансграничного оборота данных.

Основными задачами правового регулирования рынка данных в Российской Федерации на данном этапе его формирования являются:

- определение основных направлений правового регулирования новой сферы общественных отношений — формируемого рынка данных — для обеспечения стимулирования его развития и достижения мирового лидерства;
- выявление и устранение правовых и организационных барьеров, препятствующих формированию и развитию рынка данных на федеральном и региональном уровне, а также определение правовых стимулов развития данного рынка;
- гармонизация интересов непосредственных субъектов (участников) рынка данных, а также государственных и общественных интересов в сфере развития экономики данных;
- обеспечение информационной безопасности личности, общества и государства при формировании и развитии оборота данных;
- создание условий для взаимодействия внутреннего российского рынка данных с рынками данных дружественных стран и интеграционных объединений

⁵ Болобонова М. О., Хрупалов В. А. Правовое регулирование оборота данных в деятельности цифровых платформ: спорные вопросы теории и практики // Бизнес, менеджмент и право. 2020. № 2. С. 42—46.

⁶ Минбалева А. В. Правовая природа больших данных // Вестник Южно-Уральского государственного университета. Серия : Право. 2024. Т. 24. № 3. С. 88—93.

⁷ Мефодьева К. А. Некоторые проблемы правового регулирования оборота цифровых данных в эпоху больших данных // Евразийский юридический журнал. 2018. № 10. С. 73—75.

⁸ Афанасьев С. Д., Чихладзе Л. Т. Правовое регулирование оборота данных: современные проблемы в контексте формирования экономики данных // Закон и право. 2024. № 2. С. 37—42.

⁹ Ючинсон К. С. Большие данные и законодательство о конкуренции // Право. Журнал высшей школы экономики. 2017. № 1. С. 216—245.



(ЕАЭС, СНГ, ШОС, БРИКС) с учетом необходимости обеспечения государственного суверенитета Российской Федерации в информационном пространстве, а также ее экономического, финансового и технологического суверенитета.

Для обеспечения формирования и развития рынка данных в Российской Федерации, обеспечения его мирового лидерства в рамках законодательного и подзаконного нормативного правового регулирования, а также практики применения соответствующих правовых норм должны быть системно реализованы следующие *принципы*:

- обеспечение государственного суверенитета Российской Федерации в информационном пространстве, а также экономического, финансового и технологического суверенитета Российской Федерации при формировании и развитии рынка данных, его взаимодействии с зарубежными и международными рынками данных;
- стимулирование развития рынка данных на основе вовлечения данных в гражданский оборот, определения правового режима и правовых форм оборота данных, обеспечения прав и законных интересов всех субъектов (участников) рынка данных;
- оценка рисков развития оборота данных для интересов личности, общества и государства;
- обеспечение информационной безопасности всех участников рынка данных, а также защиты данных;
- поддержка конкуренции, развития малого и среднего предпринимательства, технологических стартапов в сфере оборота данных;
- развитие международного сотрудничества в сфере оборота данных, ориентированного на обеспечение мирового лидерства российского рынка данных;
- участие представителей рынка данных в формировании правового регулирования и анализа практики его применения;
- развитие институтов и инструментов саморегулирования рынка данных при условии обеспечения прав и законных интересов всех субъектов (участников) рынка данных.

Реализация указанных принципов при разработке проектов нормативных правовых актов в сфере регулирования рынка данных, их реализации и последующего мониторинга и оценки фактического воздействия указанных нормативных правовых актов должна осуществляться согласованно и комплексно.

Направления и механизмы реализации Концепции следующие.

Определение состава и правового статуса субъектов (участников) рынка данных. Общий состав субъектов (участников) рынка данных определяется на основе их функций в рамках производства (генерации) и дальнейшего оборота данных. Это:

- производитель данных — субъект (участник) рынка данных, производящий (генерирующий) данные, в том числе с помощью автоматизированных средств или измерительного оборудования и иных технических средств;
- субъект данных — субъект (участник) рынка данных, к которому относятся данные, будь то юридическое или физическое лицо, орган государственной власти или местного самоуправления;

- поставщик данных — субъект (участник) рынка данных, который предоставляет данные другому субъекту (участнику) рынка данных; при этом поставщик данных может также являться производителем данных или субъектом данных;
- получатель данных — субъект (участник) рынка данных, который получает данные от другого субъекта (участника) рынка данных, в частности путем получения доступа к данным, размещенным на соответствующей цифровой платформе; при этом получатель данных может также являться обработчиком данных;
- обработчик данных — субъект (участник) рынка данных, осуществляющий операции по обработке данных, в том числе оператор соответствующей цифровой платформы.

Правовой статус субъектов (участников) рынка данных должен определяться как общими нормами федерального законодательства, так и специальными нормами, определяющими их права, обязанности и ответственность с учетом принципов правового регулирования рынка данных в Российской Федерации.

Определение правового режима данных как объекта оборота на рынке данных. При определении правового режима данных, наборов данных и отдельных видов данных важно обеспечить как стимулирование их вовлечения в оборот, в том числе на основе определения правовых форм такого оборота, так и защиту прав личности, общества и государства, прежде всего в сфере защиты прав субъектов персональных данных и прав обладателей информации (данных), составляющих различные виды тайн, т.е. баланс интересов всех участников рынка данных. Такой баланс может быть обеспечен, например, как стимулированием возможностей оборота обезличенных данных, так и одновременным ужесточением ответственности за их деанонимизацию.

Определение механизмов для обеспечения государственного суверенитета Российской Федерации в информационном пространстве, а также экономического, финансового и технологического суверенитета Российской Федерации при формировании и развитии рынка данных, его взаимодействии с зарубежными и международными рынками данных. Данное направление реализуется посредством выявления возможных угроз государственному суверенитету, в том числе при заимствовании международного и зарубежного опыта регулирования рынка данных, принятии Российской Федерацией международных обязательств в рамках международных договоров и документов международных организаций. Особое внимание должно быть уделено реализации положений документов международных организаций в национальном законодательстве, предварительной оценке последствий такой реализации с точки зрения национальных интересов Российской Федерации и защиты ее внутреннего рынка данных.

Определение инструментов и мер стимулирования развития рынка данных на основе вовлечения данных в гражданский оборот и определения правовых форм оборота данных. В рамках развития гражданского законодательства целесообразны систематизация и определение новых форм договоров в сфере оборота данных, их ключевых условий, разработка типовых форм таких договоров. В рамках развития информационного законодательства должны быть скорректированы правовые нормы, регламентирующие создание и применение



государственных и муниципальных информационных систем и платформ с точки зрения ориентации на возможное использование содержащихся в них данных не только для реализации соответствующих государственных функций и оказания государственных услуг, но и для дальнейшего использования этих данных в разных отраслях экономики, с учетом требований об информационной безопасности и защите отдельных видов тайн.

Обеспечение конкуренции и поддержки малого и среднего предпринимательства, технологических стартапов. Данное направление реализуется посредством совершенствования положений антимонопольного законодательства в отношении формируемого рынка данных, а также требований к его участникам. Особое значение имеет обеспечение конкуренции на этапе вовлечения данных, и в первую очередь государственных данных, в гражданский оборот, исключение монополизации со стороны крупных технологических компаний в сфере как оборота данных, так и их обработки. Следует определить специальные меры, обеспечивающие равный и недискриминационный доступ к данным в рамках проводимых экспериментов в государственном управлении в сфере его цифровой трансформации и внедрения цифровых технологий, в том числе технологий искусственного интеллекта. Указанные механизмы могут быть обеспечены в том числе определением обязательности участия в таких проектах субъектов малого и среднего предпринимательства и технологических стартапов, а не только крупных технологических компаний.

Внедрение инструментов оценки рисков развития оборота данных и совершенствование механизмов обеспечения информационной безопасности. Данное направление реализуется посредством внедрения в практику нормотворчества в сфере оборота данных и развития рынка специализированной оценки рисков развития такого оборота с точки зрения обеспечения прав и законных интересов личности, общества и государства. Прогнозный характер такой оценки позволит минимизировать потенциальный вред от таких рисков в рамках нормотворчества. Развитие рынка данных формирует новые вызовы и для существующего правового регулирования информационной безопасности, в настоящее время в большей мере ориентированной на обеспечение безопасности объектов критической информационной инфраструктуры и информационных систем, а не данных в рамках их оборота, в том числе при передаче от одного субъекта (участника) рынка другому. Особое значение имеют совершенствование и развитие правового регулирования хранения данных, поскольку в настоящее время правовые нормы, в том числе архивного законодательства, в большей мере определяют порядок хранения информации и электронных документов, а не данных и наборов данных.

Определение направлений и форм международного сотрудничества в сфере развития рынка данных. Для Российской Федерации важно обеспечить взаимовыгодное сотрудничество с дружественными государствами и интеграционными объединениями (ЕАЭС, СНГ, ШОС, БРИКС) в сфере развития рынка данных на основе технологической кооперации и совместного использования данных, предоставления доступа к рынкам данных друг друга на основе принципа взаимности, а также обеспечения прав и законных интересов всех участников рынка при осуществлении трансграничной передачи данных. При этом усилия Российской Федерации должны быть ориентированы на обеспечение мирового лидерства в сфере рынка данных, в том числе и на основе «экспорта» российских подходов к регулированию

рынка данных, определению правового статуса его участников и правового режима объектов оборота, которые должны стать основой для соответствующих двусторонних и многосторонних соглашений в сфере оборота данных, а также решений органов международных организаций, в том числе их цифровых повесток.

Обеспечение участия представителей рынка данных в формировании правового регулирования и анализе практики его применения. Это направление реализуется посредством обязательного проведения оценки регулирующего воздействия в отношении вводимых обязательных требований в сфере регулирования рынка данных, а также регулярного мониторинга правоприменения и оценки применения обязательных требований, включая оценку фактического воздействия устанавливающих обязательные требования нормативных правовых актов. При этом важно обеспечить максимальное вовлечение участников рынка в формирование правового регулирования в указанных формах, в том числе на основе взаимодействия регулирующих органов, уполномоченных по защите прав предпринимателей в Российской Федерации и субъектах РФ, объединений участников рынка данных.

Реализация указанных направлений, по нашему мнению, будет способствовать формированию комплексного и системного правового регулирования рынка данных в России.

БИБЛИОГРАФИЯ

1. *Афанасьев С. Д., Чихладзе Л. Т.* Правовое регулирование оборота данных: современные проблемы в контексте формирования экономики данных // Закон и право. — 2024. — № 2. — С. 37—42.
2. *Болобонова М. О., Хрупалов В. А.* Правовое регулирование оборота данных в деятельности цифровых платформ: спорные вопросы теории и практики // Бизнес, менеджмент и право. — 2020. — № 2. — С. 42—46.
3. *Ефремов А. А.* Адаптация экспериментального правового регулирования для достижения национальных целей развития Российской Федерации // Вестник Воронежского государственного университета. — Серия : Право. — 2025. — № 3 (62). — С. 164—172.
4. *Мефодьева К. А.* Некоторые проблемы правового регулирования оборота цифровых данных в эпоху больших данных // Евразийский юридический журнал. — 2018. — № 10. — С. 73—75.
5. *Минбалеев А. В.* Правовая природа больших данных // Вестник Южно-Уральского государственного университета. — Серия : Право. — 2024. — Т. 24. — № 3. — С. 88—93.
6. *Христова С. М.* Данные как товар: анализ противоречий теоретического и прагматического подхода // Вестник Московского университета имени С. Ю. Витте. — Серия 1 : Экономика и управление. — 2025. — № 1 (52). — С. 77—86.
7. Энергетические рынки: проблемы и задачи правового регулирования : монография / под ред. В. В. Романовой. — М. : Юрист, 2018. — 240 с.
8. *Ючинсон К. С.* Большие данные и законодательство о конкуренции // Право. Журнал высшей школы экономики. — 2017. — № 1. — С. 216—245.





**Михаил Вячеславович
БУНДИН,**

доцент кафедры
административного
и финансового права
юридического факультета
Национального
исследовательского
Нижегородского
государственного
университета
имени Н.И. Лобачевского,
кандидат юридических наук
mbundin@jur.unn.ru
603022, Россия, г. Нижний
Новгород, просп. Гагарина,
д. 23

Цель обработки персональных данных: теоретические и практические правовые аспекты

Аннотация. Статья посвящена изучению важной категории «цель обработки персональных данных», а также вопросам ее использования при применении принципов обработки персональных данных и их защите. Показано особое значение этой категории применительно к процессу выбора конкретного правового основания для обработки, а также для выявления особенностей правового режима отдельных персональных данных (на примере биометрических). Кроме того, в статье исследуются особенности формулирования целей обработки персональных данных в уведомлении о начале обработки, политики оператора в отношении обработки и защиты данных, а также конкретных и контекстных согласий на обработку данных. Делаются выводы о необходимости более гибкого подхода к формулированию цели обработки в каждом из указанных случаев в интересах защиты прав и интересов индивида.

Ключевые слова: персональные данные, принципы и условия обработки, цель обработки данных, политика конфиденциальности, правовые основания обработки персональных данных

DOI: 10.17803/2311-5998.2026.142.6.070-077

Michail V. BUNDIN,

Associate Professor of the Department
of Administrative and Financial Law
of the Faculty of Law of the National Research Lobachevsky State University
of Nizhny Novgorod, Cand. Sci. (Law)
mbundin@jur.unn.ru

23, prosp. Gagarina, Nizhny Novgorod, Russia, 603022

The Purpose of Processing Personal Data: Theoretical and Practical Legal Aspects

Abstract. The article is devoted to the study of the important category 'purpose of personal data processing,' as well as issues of its use in applying the principles of personal data processing and their protection. The special significance of this category is shown in relation to the process of choosing a specific legal basis for processing, as well as for identifying the features of the legal regime of certain personal data (using the example of biometric data). The author also examines the specifics of formulating the purpose of processing personal data in the notification of the beginning of processing, the operator's policy regarding data processing and protection, as well as specific and contextual consent to data processing. The article concludes that it is necessary to take a more flexible approach to formulating the purpose

of processing in each of these cases in order to protect the rights and interests of individuals.

Keywords: *personal data, principles and conditions of processing, purpose of data processing, privacy policy, legal basis for processing personal data*

Проблематика защиты персональных данных уже давно занимает одно из ведущих мест в обсуждениях о влиянии цифровизации современного общества на права личности. Действительно, проблема накопления значительных объемов данных о физических лицах крупными ИТ-гигантами, государством и его органами все больше вызывает определенное беспокойство в обществе. В этом ключе институт защиты персональных данных становится все более значимым для индивида в части предоставления возможности контроля за использованием данных о себе и защиты своих прав и законных интересов.

Обозначенная проблематика в современном информационном праве активно исследуется учеными, но широкое развитие правоприменительной практики делает проблему весьма актуальной. Вопросы вызывает даже само определение понятия «цель обработки персональных данных» и ее роли в общей системе обеспечения безопасности персональных данных.

Так, важно отметить, что соответствие параметров обработки персональных данных ее цели можно рассматривать как краеугольный камень в формировании системы принципов, на которых строится их защита, причем этот принцип был обозначен изначально, когда правовой институт защиты персональных данных еще формировался. В частности, указанный принцип был включен в часть 1 «Общие положения» Основных положений о защите неприкосновенности частной жизни и международных обменов персональными данными (Приложение к Рекомендациям Совета ОЭСР от 23.09.1980)¹, где говорится, что персональные данные должны соответствовать целям, в которых они будут использоваться (принцип качества данных). Цели эти должны быть конкретизированы не позднее чем в момент их использования (принцип конкретизации целей). Данные не должны использоваться в иных целях, помимо обозначенных (принцип ограничений на использование данных), и такое обозначение должно быть открытым/публичным (принцип открытости).

Необходимость ограничения использования данных определенными и законными целями, включая требование об их относимости заявленным целям, как и сроков их хранения, предусмотрены в ст. 5 достаточно известной Конвенции о защите физических лиц при автоматизированной обработке персональных данных Совета Европы². Последнее особенно актуально в том числе и для России,

¹ The Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58/FINAL] / OECD // URL: <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0188> (дата обращения: 30.04.2026).

² Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28.01.1981) // СЗ РФ. 2014. № 5. Ст. 419.



поскольку она ратифицировала³ и имплементировала ее положения через принятие специального Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ⁴ (далее — Закон о персональных данных).

Еще одним документом, который стоит упомянуть в ретроспективном плане, является Директива 95/46/ЕС⁵, содержащая в целом аналогичные положения, касающиеся ограничения параметров обработки соответствующими конкретными, явно выраженными законными целями. Описание этого принципа можно дать следующими основными тезисами:

- обработка должна ограничиваться достижением конкретных, заранее определенных и законных целей;
- недопустима обработка персональных данных, не совместимая с целями их сбора;
- недопустимо объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой;
- содержание, объем и сроки обработки персональных данных должны соответствовать целям обработки персональных данных.

Аналогичные положения можно встретить практически во всех законодательных актах многих государств Европейского союза, Совета Европы и СНГ, в основе формирования содержания которых использовались вышеуказанные документы. Отсюда напрашивается главный и очевидный вывод о том, что цель обработки является важнейшим параметром оценки ее законности, т.е. определением того, насколько обработка персональных данных является справедливой, законной, соответствующей интересам субъекта персональных данных.

В юридических исследованиях данный принцип именуется принципом «ограничения обработки конкретной целью (purpose limitation)»⁶, что означает прозрачность и предсказуемость процессов обработки для индивида, а также его возможность реализовать права по управлению данными. В связи с этим выделяются ряд составляющих принципа: «...конкретность цели и обязательность ее доведения до сведения субъекта данных на момент сбора; законность цели; соответствие последующих действий по обработке целям, заявленным при сборе»⁷.

Продолжением данного принципа можно считать принцип недопустимости объединения баз данных, созданных для различных и, прежде всего, несовместимых между собой целей; принцип минимизации данных; принцип точности и

³ Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» // СЗ РФ. 2005. № 52 (ч. I). Ст. 5573.

⁴ СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.

⁵ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // URL: <https://eur-lex.europa.eu/legal-content/en/txt/html/?uri=celex:31995L0046> (дата обращения: 30.04.2026).

⁶ Савельев А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». 2-е изд., перераб. и доп. М. : Статут, 2021.

⁷ Савельев А. И. Научно-практический постатейный комментарий...

достаточности данных для целей обработки; принцип ограниченности хранения данных достижением цели или утраты необходимости в ее достижении⁸.

Все эти принципы и их описание в значительной степени известны и тут, скорее, можно говорить о единой и вполне понятной идее-принципе, которая указывает на необходимость выстраивания всех процессов по обработке персональных данных в соответствии с определенной целью.

Однако то, как изложенное реализуется на практике, стоит рассмотреть более подробно. В частности, тут можно говорить о следующих аспектах:

- 1) определение цели в документе, определяющем политику оператора в отношении обработки и защиты персональных данных;
- 2) определение цели при формировании и получении согласия физического лица на обработку персональных данных;
- 3) при выборе правового основания;
- 4) при определении категории/режима персональных данных.

В первом случае важно понимать в совокупности, какие цели преследует оператор при обработке персональных данных. Действующая форма уведомления о начале обработки персональных данных, предусмотренная приказом Роскомнадзора от 28.10.2022 № 180⁹, ориентируется именно на описание основных процессов обработки применительно к определенным целям, в отличие от предыдущей формы, которая ориентировалась на описание информационных систем обработки персональных данных, с учетом того, что уведомление преимущественно затрагивало автоматизированную обработку. При этом описание цели с учетом пояснений и разъяснений Роскомнадзора носит крайне обобщенный характер¹⁰. Примерами таких формулировок могут быть: ведение кадрового и бухгалтерского учета; подача отчетности в федеральные органы исполнительной власти¹¹. Ведомство также поясняет, что цель в таком случае должна совпадать с уставной деятельностью и видами деятельности ОКВЭД, закрепленными при регистрации организации или индивидуального предпринимателя.

При кажущейся простоте на практике ситуация не настолько очевидна с учетом того, что оператор вправе достаточно свободно формулировать параметры обработки для каждой цели. Часто, например, операторы пытаются провести

⁸ Савельев А. И. Научно-практический постатейный комментарий...

⁹ Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных» // Официальный интернет-портал правовой информации. URL: <http://publication.pravo.gov.ru/document/view/0001202212150022> (дата обращения: 30.04.2026).

¹⁰ Информация Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 25.12.2022 «Примеры заполнения документов об обработке персональных данных» // СПС «Гарант».

¹¹ Автор приводит примеры из доступной части реестра операторов персональных данных. См. для справки: URL: <https://pd.rkn.gov.ru/operators-registry/operators-list/> (дата обращения: 30.04.2026).



очень широкие обобщения и указывают в качестве цели «соблюдение требований применимого законодательства...» или «оказание услуг...», «защита прав и интересов оператора», «организация и проведение мероприятий...». Роскомнадзор также в целом в определенной степени поддерживает такую позицию (например, одно из территориальных подразделений рекомендовало для организаций указывать в обязательном порядке «ведение кадрового и бухгалтерского учета»¹²). Также ведомство подчеркивало необходимость совпадения целей, указанных в уведомлении, а значит, и в публичной части реестра, с указанными в документах, определяющих политику оператора в отношении обработки и защиты персональных данных, которые согласно закону подлежат обязательному опубликованию, в том числе на сайте оператора, если он осуществляет сбор и обработку с его использованием¹³.

Однако применительно ко второму рассматриваемому аспекту (определение цели при формировании и получении согласия физического лица на обработку персональных данных) законодательство, наоборот, требует иного подхода в определении цели обработки персональных данных¹⁴. В частности, ч. 1 ст. 9 Закона о персональных данных требует, чтобы согласие, помимо прочего, было информированным и предметным. Несмотря на то что сам Закон не дает трактовки «предметности» и «информированности», все же здесь следует предположить определенный контекст отношений между оператором и субъектом персональных данных с учетом того, что этот контекст определяет необходимость сообщения и доведения до сведения субъекта информации об обработке и суть того, в связи с чем, т.е. с какой, собственно, целью дается¹⁵ согласие на обработку персональных данных.

Следует предположить, что для субъекта персональных данных это не может быть чем-то абстрактным и непонятным из ситуации, в которой дается согласие. Учитывая это, такие формулировки цели, как «осуществление уставной деятельности оператора», «ведение бухгалтерского учета», «выполнение требований применимого законодательства...», «проведение маркетинговых исследований», вряд ли будут в достаточной степени предметными и понятными для физического лица, которое предоставляет согласие. Индивид дает его с конкретной целью, в своем интересе и применительно к конкретной ситуации. Следовательно, цель для него должна быть понятна и соответствовать ситуации и его интересам, чтобы индивид мог свое согласие предоставить и оценить последствия своих действий.

Видится логичным, что при формулировании целей в согласии оператор вполне может описать ее в более понятной и «приземленной» форме. Например, при предоставлении конкретного сервиса нет смысла писать, что оператор просит дать согласие на обработку для предоставления не всех своих гипотетических

¹² См. также: Примеры и частые ошибки при заполнении уведомления об обработке персональных данных, информационного письма о внесении изменений в сведения в реестре операторов персональных данных // Роскомнадзор. URL: <https://32.rkn.gov.ru/directions/p39115/p39085/p19001/p13324/> (дата обращения: 30.04.2026).

¹³ Комментарий к Федеральному закону «О персональных данных» // СПС «Гарант».

¹⁴ Комментарий к Федеральному закону «О персональных данных».

¹⁵ Комментарий к Федеральному закону «О персональных данных».

цифровых сервисов, которые у него есть, а одного или нескольких, в которых заинтересован пользователь. Аналогичная ситуация складывается с мероприятиями, конкурсами и т.п. Это никак не нарушает общей логики в части определения оператором целей для политики в отношении обработки и защиты данных или уведомления об обработке, предусмотренного ст. 21 Закона о персональных данных.

В третьем случае (при выборе правового основания) разумно предположить, что цель обработки напрямую связана с определением правового основания для обработки персональных данных. Собственно, соотнесение обработки с конкретной целью и позволяет часто его определить. Анализ содержания ч. 1 ст. 6 Закона о персональных данных это в полной мере подтверждает. Из 12 правовых оснований, указанных там, 10 непосредственно связаны с целью:

- исполнение оператором обязанностей, предусмотренных законом;
- в связи с участием лица в судопроизводстве;
- для исполнения судебного акта или иного подлежащего исполнению акта;
- для предоставления государственных и муниципальных услуг;
- для исполнения договора с участием индивида;
- для защиты жизни и здоровья в экстренных ситуациях;
- для осуществления законных прав и интересов оператора;
- для деятельности журналиста, СМИ, научной, литературной или иной творческой деятельности;
- для статистических и исследовательских целей;
- обработка обезличенных данных в целях повышения эффективности государственного или муниципального управления или в иных целях, предусмотренных законодательством об экспериментальных правовых режимах.

Исключение составляет обработка на основании согласия и обработка общедоступных персональных данных, где цель в той или иной мере определяется оператором или субъектом¹⁶. Возможно даже иное утверждение, что обработка персональных данных, за исключением вышеуказанных 10 оснований-целей, должна осуществляться на основании согласия или в режиме общедоступной информации. Несмотря на то что определение правового основания для обработки в некоторых случаях остается нетривиальной задачей, тем не менее общая логика тут вполне усматривается.

Наконец, четвертый аспект в определении цели обработки (при определении категории/режима персональных данных) является одним из самых интересных с точки зрения как практики, так и теории. Условно в самом общем приближении правовой режим конфиденциальности персональных данных имеет три основные составляющие: правовой режим специальных категорий персональных данных; правовой режим биометрических персональных данных; правовой режим иных категорий персональных данных¹⁷. Однако, если в отношении двух из них принципиальное значение имеют только категория и содержание персональных

¹⁶ Комментарий к Федеральному закону «О персональных данных».

¹⁷ *Минина А. А., Атаян Г. Ю., Богатырева А. Т.* Отдельные особенности правового режима и защиты персональных данных // *Право и государство: теория и практика.* 2023. № 8 (224).



данных, то в отношении биометрических персональных данных принципиальное значение имеет именно цель обработки персональных данных¹⁸.

В определении биометрических персональных данных в ст. 11 Закона о персональных данных явно указано, что это «физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются для установления его личности...». Следовательно, цель их обработки связана с необходимостью «установления личности субъекта» и становится обязательным критерием их определения¹⁹. Это в той или иной степени соответствует и практике. Например, фотоизображение физического лица, его голос, походка или иные физиологические особенности²⁰, если они не используются, т.е. обрабатываются с целью установления его личности, не являются, по сути, биометрическими персональными данными и становятся таковыми, если мы начинаем преследовать такую цель. Полагаем, что фотоизображение, полученное в первую очередь в семейных или личных целях, может вполне стать эталоном для поиска соответствий в сети Интернет с помощью технологий, позволяющих установить соответствие, т.е. распознать человека по его уникальным физиологическим параметрам.

Такая позиция подтверждается и судебной практикой, например, Савеловский районный суд в деле № 02а-0577/2019 указал, что запись с городских камер видеонаблюдения даже с применением технологии распознавания лиц не является сама по себе биометрическими персональными данными, поскольку она не используется для установления личности²¹. Несмотря на то что такая позиция суда выглядит спорной²² как минимум в части того, что алгоритм распознавания собственно и призван определять человека или иной объект, критерий наличия связи между целью обработки и необходимостью «установления личности» для определения биометрических данных является ключевым в контексте текущей редакции ст. 11 Закона о персональных данных.

Как видим, цель обработки данных в действительности является важнейшим ее параметром, который не только определяет ее законность, но также влияет одновременно на определение правового основания обработки и, в определенных случаях, правового режима конфиденциальности персональных данных.

Также стоит иметь в виду, что цель обработки персональных данных может носить крайне общий характер при формулировании документов, определяющих политику оператора в отношении обработки и защиты персональных данных, но

¹⁸ Комментарий к Федеральному закону «О персональных данных».

¹⁹ Комментарий к Федеральному закону «О персональных данных».

²⁰ *Кривогин М. С.* Правовой режим биометрических персональных данных // Проблемы науки. 2015. № 10 (40).

²¹ Информация по делу № 02а-0577/2019 // Официальный портал судов общей юрисдикции города Москвы. URL: <https://www.mos-gorsud.ru/rs/savelovskij/services/cases/kas/details/988f386e-be51-47b0-b48f-e871043ef1fc> (дата обращения: 30.04.2026).

²² *Геращенко А. И.* На факультете права обсудили развитие правового регулирования биометрии в России и за рубежом // Официальный сайт факультета права Высшей школы экономики // URL: <https://pravo.hse.ru/techlaw/news/1038235820.html> (дата обращения: 30.04.2026).

в конкретных ситуациях, например при сборе персональных данных на основе согласий, требует часто определенной конкретизации, связанной с контекстом, в рамках которого это согласие предоставляется. Последнее в значительной степени важно для того, чтобы гарантировать права субъекта персональных данных и его информированность о цели, для которой это согласие предоставляется.

С другой стороны, это никак не влияет на возможность «обобщения» целей для формирования уведомления о начале обработки персональных данных и внесения изменений в реестр операторов персональных данных. Наоборот, в данном случае излишняя конкретизация только усложнила бы общее понимание бизнес-процессов оператора, связанных с обработкой данных о физических лицах.

В данном контексте вполне логичным как раз видится идея об отказе от практики излишнего сбора согласий на обработку персональных данных за счет определения отраслевых стандартов, содержащих типовые бизнес-процессы по их обработке, большая часть которых имеет иные правовые основания. Видится вполне логичным проработка Роскомнадзором с участием представителей отраслей более четкой позиции в отношении так называемого законного интереса оператора и методик его оценки²³.

БИБЛИОГРАФИЯ

1. *Кривогин М. С.* Правовой режим биометрических персональных данных // Проблемы науки. — 2015. — № 10 (40).
2. *Минина А. А., Атаян Г. Ю., Богатырева А. Т.* Отдельные особенности правового режима и защиты персональных данных // Право и государство: теория и практика. — 2023. — № 8 (224).
3. *Савельев А. И.* Законный интерес как универсальное основание для обработки персональных данных без согласия субъекта: проблемы правоприменительной практики // Закон. — 2025. — № 9. — С. 16—32.
4. *Савельев А. И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». — 2-е изд., перераб. и доп. — М. : Статут, 2021.

²³ *Савельев А. И.* Законный интерес как универсальное основание для обработки персональных данных без согласия субъекта: проблемы правоприменительной практики // Закон. 2025. № 9. С. 16—32.



**ЛО Имин,**

аспирант кафедры
информационного права
и цифровых технологий
Университета имени
О.Е. Кутафина (МГЮА)
lym001008@gmail.com
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

Развитие правового регулирования применения больших данных в цифровой экономике Китая

Аннотация. В статье рассматривается эволюция правового регулирования применения технологий больших данных в условиях цифровой экономики Китая. Автором выделяются три этапа становления соответствующей нормативной базы: начальный этап (до 2020 г.), характеризующийся фрагментарностью регулирования; этап формирования системной структуры (2020—2022 гг.), связанный с принятием ключевых законов в сфере данных, и современный этап (с 2022 г. по настоящее время), ориентированный на стимулирование оборота данных и их использование в качестве фактора производства. Особое внимание уделяется анализу «Двадцати положений о данных», закрепивших разделение правомочий в отношении данных и переход от охранительной модели к модели, ориентированной на использование. В заключении обосновывается институционализация больших данных в стратегическом планировании Китая и трансформация правового подхода от управления рисками к управлению развитием.

Ключевые слова: большие данные, цифровая экономика, Китай, правовое регулирование, защита данных, оборот данных, элементы данных, цифровая трансформация

DOI: 10.17803/2311-5998.2026.142.6.078-085

LUO Yiming,

graduate student of the Department of information law and digital technologies
of the Kutafin Moscow State Law University (MSAL)

lym001008@gmail.com

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Development of Legal Regulation of the Use of Big Data in China's Digital Economy

Abstract. The article traces the evolution of the legal regulation of big data applications within the context of China's digital economy. The author identifies three distinct stages in the formation of the regulatory framework: the initial stage (before 2020), marked by fragmented normative provisions; the stage of systematic structuring (2020—2022), defined by the adoption of foundational data legislation; and the current stage (since 2022), focused on promoting data circulation and utilization as a factor of production. Special attention is given to the “Twenty Provisions on Data”, which introduced a differentiated system of data rights and signaled a shift from a protection-oriented to an utilization-oriented regulatory model. The conclusion highlights the institutionalization of big data in China's strategic planning and the

broader transformation of legal governance from risk prevention to development facilitation.

Keywords: *big data, digital economy, China, legal regulation, data protection, data circulation, data elements, digital transformation*

Цифровая трансформация — это глобальное революционное изменение эпохи, влияние которого охватывает способы производства, образ жизни и формы управления¹. Цифровая экономика является важным продуктом этой трансформации и основной экономической формой, следующей за аграрной и промышленной². Если основным ресурсом аграрной экономики являются семена, а индустриальной — нефть, то основным ресурсом цифровой экономики являются данные.

Впервые на государственном уровне в Китае концепция цифровой экономики была официально представлена и продвинута в сентябре 2016 г. на саммите «Группы двадцати» (G20) в Ханчжоу. Китай, выступая в качестве страны-председателя, включил цифровую экономику в основную повестку дня, способствовал разработке Инициативы «Группы двадцати» по развитию и сотрудничеству в области цифровой экономики³ (далее — Инициатива «Группы двадцати») и положил начало стратегическому планированию развития цифровой экономики в Китае.

На основании Инициативы «Группы двадцати»⁴ по развитию и сотрудничеству в области цифровой экономики, представленной на саммите «Группы двадцати», а также таких программных документов, как «中华人民共和国国民经济和社会发展第十四个五年规划和二〇三五年远景目标纲要»⁵ («Наброски четырнадцатого пятилетнего плана национального экономического и социального развития Китайской Народной Республики и перспективные цели на 2035 год») и «国家信息化发展战略纲要»⁶ («Наброски национальной стратегии развития информатизации»), Государственное статистическое управление Китая в мае 2021 г. официально опубликовало «数字经济及其核心产业统计分类 (2021)»⁷ («Статистическую классификацию цифровой экономики и ее ключевых отраслей (2021)») (далее — Классификация цифровой экономики), определив основную сферу цифровой экономики: ряд

¹ 新华社北京11月9日电 11月9日·国家主席习近平向2022年世界互联网大会乌镇峰会致贺信 [Поздравительное письмо Президента Председателя Си Цзиньпина участникам Всемирной интернет-конференции 2022 года в Учжэне].

² 国务院关于印发“十四五”数字经济发展规划的通知 国发〔2021〕29号 // URL: https://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm (дата обращения: 17.03.2026).

³ Инициатива «Группы двадцати» по развитию и сотрудничеству в области цифровой экономики // URL: <http://kremlin.ru/supplement/5111> (дата обращения: 17.03.2026).

⁴ Инициатива «Группы двадцати»...

⁵ 中华人民共和国国民经济和社会发展第十四个五年规划和二〇三五年远景目标纲要 // URL: <https://www.ndrc.gov.cn/xxgk/zcfb/ghwb/202103/P020210313315693279320.pdf> (дата обращения: 17.03.2026).

⁶ 国家信息化发展战略纲要 // URL: https://www.xinhuanet.com/politics/2016-07/27/c_1119291902.htm (дата обращения: 17.03.2026).

⁷ 《数字经济及其核心产业统计分类 (2021)》(国家统计局令第33号)。



экономических видов деятельности, в которых данные являются ключевым фактором производства, современные информационные сети — важным носителем, а эффективное использование информационных технологий — важной движущей силой повышения эффективности и оптимизации экономической структуры.

В октябре 2019 г. данные впервые были включены правительством Китая в число факторов производства в «*中共中央关于坚持和完善中国特色社会主义制度推进国家治理体系和治理能力现代化若干重大问题的决定*»⁸.

В 14-м пятилетнем плане Китая неоднократно упоминается целый ряд информационных технологий, включая большие данные, искусственный интеллект и квантовые информационные технологии. В контексте цифровой экономики применение больших данных, направленное на максимальное извлечение и использование ценности данных, выделяется в связи с их основополагающим характером и важностью, обусловленными особым статусом данных как фундаментального ресурса.

План «14-я пятилетка» был разработан в 2021 г., и к настоящему времени отрасль цифровой экономики Китая значительно развилась: доля добавленной стоимости ключевых отраслей цифровой экономики превысила 10,5 %, а повсеместное применение больших данных стало технологической реальностью. Развитие технологий неизбежно ведет к изменению социальных отношений. С юридической точки зрения системное воздействие применения больших данных проявляется главным образом в трех аспектах: конфликт между циркуляцией данных и защитой прав, конфликт между использованием данных и их безопасностью, а также конфликт между стимулированием инноваций и нормативным регулированием.

Правовое регулирование применения больших данных в Китае

Рассмотрим развитие правовых норм, регулирующих применение больших данных в Китае, в хронологическом порядке. Правовое регулирование применения больших данных в Китае в основном делится на три этапа.

Первый этап (до 2020 г.): начальный этап

Первое упоминание термина «большие данные» в официальных документах Китая появилось в «*2014年政府工作报告*»⁹ (Отчете о работе правительства за 2014 год) в марте 2014 г. На данном этапе большие данные в основном рассматривались как «технология будущего, которую следует активно развивать», а в программных документах и местных нормативных актах были закреплены соответствующие положения, поощряющие их развитие. Например, в провинции Гуйчжоу, которая является пионером в области применения больших данных в Китае,

⁸ «*中共中央关于坚持和完善中国特色社会主义制度推进国家治理体系和治理能力现代化若干重大问题的决定*» // URL: https://www.xinhuanet.com/politics/2019-11/05/c_1125195786.htm (дата обращения: 17.03.2026).

⁹ *政府工作报告 (2014)* Пекин, 14 марта (Синьхуа) // URL: https://www.gov.cn/guowuyuan/2014-03/14/content_2638989.htm (дата обращения: 17.03.2026).

был принят «贵州省大数据发展应用促进条例»¹⁰ (Регламент о содействии развитию и применению больших данных в провинции Гуйчжоу), в котором подчеркивается, как различные субъекты провинции, включая правительство, предприятия и население, должны способствовать развитию применения больших данных.

Как в сфере применения, так и в области правового регулирования большие данные все еще находятся в зачаточном состоянии, существуют лишь отдельные нормы законов, в которых упоминаются большие данные: в «网络安全法»¹¹ (Законе «О кибербезопасности»), «中华人民共和国反垄断法»¹² (Законе «Об анти-монопольном регулировании») и в других законодательных актах. Вместе с тем правовое регулирование больших данных находится в хаотичном и неопределенном состоянии.

На государственном уровне критически важные объекты инфраструктуры, такие как центры обработки данных, находятся под защитой законов о кибербезопасности и национальной безопасности, и, как правило, принципы безопасности данных и технические стандарты устанавливаются еще на этапе их создания.

Однако из-за отсутствия закона о защите персональных данных, а также соответствующих положений, касающихся технологий больших данных и автоматизированного принятия решений, применение больших данных на данном этапе привело к массовым нарушениям прав потребителей и ущемлению прав на неприкосновенность частной жизни. Личные данные массово утекают в Интернете, особенно в социальных сетях и мобильных приложениях, где они беззастенчиво похищаются платформами и компаниями с целью извлечения прибыли.

Наиболее типичным примером являются кроссплатформенное профилирование поведения и алгоритмическое ценообразование: различные приложения в рамках одной платформы или приложения разных платформ содержат бэкдоры, через которые происходит обмен пользовательскими данными с целью их агрегирования для прогнозирования спроса и внедрения динамического ценообразования. Эксперимент по дифференцированному ценообразованию, проведенный в 2000 г. на американской платформе Amazon, уже раскрыл общественности факт «дискриминационного ценообразования на основе больших данных». В процессе массового внедрения приложений на основе больших данных в Китае такие ОТА-платформы, как Didi Chuxing и Ctrip, а также другие платформы электронной коммерции постоянно подвергаются критике со стороны потребителей за различия в ценообразовании.

Однако в рамках традиционной правовой системы из-за пробелов в законодательстве и сложностей с получением доказательств, обусловленных неравноправным положением потребителей по отношению к платформам, подобные проблемы нередко не находят справедливого правового решения. При поиске

¹⁰ 贵州省大数据发展应用促进条例 // URL: https://zrzy.guizhou.gov.cn/wzgb/zwgk/zfxxgk/fdzdgknrlztcwj/zcfg/202201/t20220121_72373768.html (дата обращения: 17.03.2026).

¹¹ 中华人民共和国网络安全法 (2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过) 新华社北京11月7日电 // URL: https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm (дата обращения: 17.03.2026).

¹² «中华人民共和国反垄断法» // URL: <https://www.gjxfj.gov.cn/gjxfj/xxgk/fgwj/flfg/webinfo/2016/03/1460585589884490.htm> (дата обращения: 17.03.2026).



по ключевым словам «большие данные» на сайте судебных документов и в юридической базе данных Wolters Kluwer Xianxing и других ресурсах результаты до 2020 г. включали лишь два дела: «Дело о споре по поводу ответственности за правонарушение между Чжэн Югао и ответчиком — компанией Shanghai Ctrip Business Co., Ltd.» [(2020) Hu 0105 Min Chu 9010] и «Дело о споре по поводу ответственности за правонарушение между Лю Цюанем и компанией Beijing SanKuai Technology Co., Ltd.» [(2019) Сян 01 Мин Цзун 9501], причем оба дела завершились отклонением судом всех исковых требований истцов.

Второй этап (2020—2022 гг.):

создание систематизированной структуры

На данном этапе применение больших данных в Китае достигает зрелости, а правовая система вступает в фазу системного развития. В период с 2021 по 2022 г. в Китае были последовательно приняты два важных закона в цифровой сфере: Закон «О защите персональных данных»¹³ и Закон «О безопасности данных»¹⁴, которые ввели такие ключевые механизмы, как классификация и ранжирование данных, оценка безопасности, а также трансграничная передача данных. Эти два Закона, наряду с ранее принятым Законом «О кибербезопасности», составляют правовую основу цифровой сферы Китая и обеспечивают базовую правовую защиту для развития экономики данных.

После совершенствования законодательства вышеупомянутое явление «кроссплатформенного профилирования поведения и алгоритмического ценообразования» было незамедлительно эффективно пресечено на территории Китая.

7 июля 2021 г. Народный суд района Кэцяо города Шаосин провинции Чжэцзян рассмотрел дело о правонарушении, возбужденное г-жой Ху против компании «Shanghai Ctrip Business Co., Ltd.» (далее — «дело Ctrip»). Г-жа Ху обратилась в суд с иском, мотивируя его тем, что Ctrip собирает ее личную информацию, не являющуюся необходимой для оказания услуг, с целью «дискриминации постоянных клиентов на основе больших данных», и потребовала возмещения ущерба в размере трехкратной стоимости, а также добавления в приложение Ctrip опции, позволяющей продолжать пользоваться приложением даже в случае несогласия с Соглашением об оказании услуг и Политикой конфиденциальности. По итогам рассмотрения дела Народный суд района Кэцяо вынес решение в зале суда. В итоге истица выиграла дело, и платформа была обязана выплатить г-же Ху компенсацию и добавить в свои правила необходимые пункты, касающиеся использования персональной информации и автоматизированного принятия решений¹⁵.

После правового урегулирования вопросов, касающихся прав пользователей и безопасности данных, в связи с развитием цифровой экономики и прогрессом

¹³ 中华人民共和国个人信息保护法 (2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过) // URL: https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm.

¹⁴ 中华人民共和国数据安全法 (2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过) // URL: https://www.gov.cn/xinwen/2021-06/11/content_5616919.htm.

¹⁵ Суд Кецяо говорит «нет» практике приложений, требующих «полного доступа» для работы // Официальный WeChat-аккаунт суда Кецяо «Защита персональных данных». URL: <https://mp.weixin.qq.com/s/dz7rckcd6sbsqka26gfrkw> (дата обращения: 17.03.2026).

в области цифровых технологий, таких как искусственный интеллект, взаимодействие больших данных с другими цифровыми технологиями, возник ряд новых вопросов, касающихся прав, связанных с данными, например в области обращения с данными и их обработки. К примеру, это касается потребности в обучающих наборах данных при обучении искусственного интеллекта методами глубокого обучения. В связи с такими правовыми действиями, как торговля данными и их обнародование, где данные выступают в качестве нового объекта права, появилась необходимость в принятии новых законодательных актов.

А. В. Минбалева отмечает, что формула Натана Ротшильда «Кто владеет информацией, тот правит миром» постепенно превращается в «Кто обладает данными, тот управляет миром»¹⁶. Это свидетельствует о том, какое важное место занимают данные в современной экономике данных. А для экономики данных и стран, стремящихся к ее развитию, тот, «кто сможет обеспечить свободный обмен данными, сможет занять лидирующие позиции в процессе развития».

Третий этап (с 2022 г. по настоящее время): стимулирование использования и обращения

В целях содействия обмену и использованию данных, изменения традиционного правового подхода, в основе которого лежит «защита», и перехода к ориентированному на «использование» подходу, вызванному новой парадигмой экономики данных, правительство Китая приняло «中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见»¹⁷ («Мнение о создании базовой системы регулирования данных для более эффективного использования данных в качестве производственного фактора») (далее — «Двадцать положений о данных»).

Анализ «Двадцати положений о данных» позволяет выделить четыре основных модуля: «Система прав владения», «Оборот и торговля», «Распределение доходов» и «Безопасность и управление».

«Двадцать положений о данных» предлагают инновационный подход к системе прав владения, предусматривающий их разделение на право владения ресурсами данных, права на обработку и использование данных, а также права на управление продуктами данных, при этом делая акцент на ослаблении роли права владения и усиливая внимание к обороту прав пользования. В сфере обращения и торговли предлагается создать эффективную и соответствующую нормативным требованиям систему, сочетающую биржевые и внебиржевые механизмы, с целью регулирования торговли данными, развития деятельности операторов данных и формирования рынка данных как производственного фактора. Распределение доходов осуществляется в соответствии с принципом «кто вкладывает, кто вносит вклад, тот и получает выгоду», что способствует перераспределению доходов от данных в пользу создателей данных и разумной регулировке доходов всех сторон. Кроме того, предусматриваются создание безопасной, контролируемой,

¹⁶ Адаптация и развитие информационного права в условиях цифровой трансформации / под ред. А. В. Минбалева. Саратов, 2024. С. 18.

¹⁷ 中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见_中央有关文件_中国政府网 // URL: https://www.gov.cn/zhengce/2022-12/19/content_5732695.htm (дата обращения: 17.03.2026).



гибкой и инклюзивной системы управления, внедрение классификации и многоуровневой защиты данных, а также предотвращение рисков, связанных с безопасностью данных.

«Двадцать положений о данных» создают правовую основу для решения таких проблем, как отсутствие четкого определения прав владения данными и отсутствие правил их обращения, что в значительной степени способствует применению больших данных, а также интеграции технологий больших данных с другими цифровыми технологиями, тем самым содействуя развитию экономики данных в Китае.

После принятия «Двадцати положений о данных» провинции Китая постепенно приняли собственные положения о данных, такие как «深圳经济特区数据条例»¹⁸ (Положение о данных Шэньчжэня) и «上海市数据条例»¹⁹ (Положение о данных Шанхая). Кроме того, Государственное управление по данным Китая продвигает новые меры, направленные на разработку политики в области регистрации элементов данных и сертификации данных как активов, с целью обеспечения дополнительных гарантий для обращения данных. Одновременно с этим в разных регионах появляются биржи данных и компании, основной деятельностью которых является обработка данных, включая их добычу, очистку и анализ.

Заключение

С 2016 г., когда термин «большие данные» впервые был упомянут в государственных планах развития Китая, и по настоящее время — 2026 год — за два пятилетних плана применение больших данных в Китае значительно развилось, а правовое регулирование постоянно совершенствуется и адаптируется к изменениям. От первоначального пассивного «предотвращения рисков» к активному «управлению развитием» сегодня правовое регулирование применения больших данных в Китае стало более конкретным: произошли классификация и дифференцированный надзор за данными, при котором к публичным, корпоративным и личным данным применяются разные правила. Права и обязанности определяются в зависимости от конкретных сценариев применения. Кроме того, поощряется использование данных в качестве производственного фактора при распределении результатов труда.

В 15-м пятилетнем плане Китая²⁰, принятом в марте 2026 г., в третьей части, посвященной в основном будущему развитию науки и технологий, термин

¹⁸ 深圳经济特区数据条例 (2021年6月29日深圳市第七届人民代表大会常务委员会第二次会议通过) // URL: https://sf.sz.gov.cn/ztzl/yhyshj/yhyshjzcwj/content/post_10596788.html (дата обращения: 17.03.2026).

¹⁹ 上海市数据条例 (2021年11月25日上海市第十五届人民代表大会常务委员会第三十七次会议通过) // URL: <https://www.shanghai.gov.cn/nw12344/20211129/a1a38c3dfe8b4f8f8fcb5e79f9be9251.html> (дата обращения: 17.03.2026).

²⁰ 中华人民共和国国民经济和社会发展第十五个五年规划纲要 // URL: <https://www.news.cn/politics/20260313/085af5de5a4b4268aa7d87d90817df2f/c.html> (дата обращения: 17.03.2026).

«большие данные» исчез, уступив место таким новым технологиям, как искусственный интеллект, квантовые технологии и интерфейсы «мозг-машина». Однако это не означает исчезновение больших данных в Китае. Напротив, производные термины больших данных, такие как «инфраструктура данных», «элементы данных» и «ресурсы данных», встречаются во всех разделах плана, особенно в четвертой главе «Построение цифрового Китая», где значительное внимание уделяется «разработке и использованию ресурсов данных» и «совершенствованию базовой системы элементов данных». В разделах, посвященных государственному управлению в таких сферах, как метеорология и транспорт, по-прежнему неоднократно упоминается «мониторинг данных». Это свидетельствует о том, что применение больших данных в условиях цифровой экономики Китая достигло зрелости и охватывает все сферы экономики и государственного управления.

В дальнейшем в Китае основное внимание в правовом регулировании больших данных будет уделяться совершенствованию и детализации конкретных систем управления данными в различных сферах на основе Закона о кибербезопасности, Закона о защите персональных данных, Закона о безопасности данных, а также «Двадцати положений о данных».

БИБЛИОГРАФИЯ

1. Адаптация и развитие информационного права в условиях цифровой трансформации : монография / под ред. А. В. Минбалева. — Саратов : Амирит, 2024. — 190 с.
2. Минбалева А. В. Правовая природа больших данных // Вестник Южно-Уральского государственного университета. — Серия : Право. — 2024. — № 3. — С. 88—93.
3. Полякова Т. А., Минбалева А. В., Кроткова Н. В. Развитие доктрины российского информационного права в условиях перехода к экономике данных // Государство и право. — 2023. — № 9. — С. 158—171.
4. Правовое обеспечение применения цифровых технологий в государственном управлении : монография / под ред. М. Б. Добробабы. — Саратов : Амирит, 2024. — 156 с.
5. Цифровая трансформация государства и права в условиях экономики данных : монография / под ред. А. В. Минбалева. — Саратов : Амирит, 2025. — 258 с.





**Алексей Игоревич
ХИМЧЕНКО,**

доцент кафедры
информационного права
и цифровых технологий
Университета имени
О.Е. Кутафина (МГЮА),
кандидат юридических наук
aihimchenko@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

К вопросу о роли данных в обеспечении доверенного функционирования систем искусственного интеллекта

Аннотация. Статья посвящена исследованию проблематики доверенного функционирования систем искусственного интеллекта. При проведении исследования использовались различные методы, в том числе общенаучный, системный метод, методы обобщения и правового анализа. Активное развитие решений в сфере искусственного интеллекта оказывает значительное влияние на структуру общественных отношений, происходит фундаментальная перестройка механики функционирования многих общественных и деловых процессов. В указанных условиях, с учетом потенциальных рисков использования, актуализируется вопрос доверенного функционирования систем искусственного интеллекта как важнейшего условия, определяющего возможность применения этих систем при решении задач обработки данных.

Исследуются риски и вопросы безопасности функционирования систем ИИ. Анализируются ключевые структурные элементы, образующие систему доверия к системам ИИ, способы обеспечения доверия, характеристики систем ИИ. Анализируется роль данных в механике функционирования систем ИИ. Выделяются и структурируются направления внедрения доверенных технологий ИИ, рассматриваются вопросы поиска практических решений по повышению безопасного и доверенного функционирования систем ИИ.

Ключевые слова: искусственный интеллект, системы искусственного интеллекта, доверие, цифровая среда, стандарт, безопасность, надежность, данные, оборот данных, жизненный цикл, доверенные технологии, нейросети

DOI: 10.17803/2311-5998.2026.142.6.086-094

Aleksey I. KHIMCHENKO,

Associate Professor of the Department of Information Law and Digital Technologies
of the Kutafin Moscow State Law University (MSAL), Cand. Sci. (Law)
aihimchenko@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

On the Issue of Trustworthy Functioning of Artificial Intelligence Systems and the Role of Data

Abstract. The article is devoted to the study of the problems of trusted functioning of artificial intelligence systems. Methods: analysis, system method, idealization, legal modeling, hypothesis building, generalization and system

analysis. Results. The active development of artificial intelligence is redirecting key technological approaches from digital transformation to AI transformation.

In these conditions, taking into account the potential risks of use, the issue of trusted operation of artificial intelligence systems becomes relevant, as it is a crucial condition that determines the possibility of using these systems for data processing tasks.

The article explores the risks and security issues associated with the operation of AI systems. It analyzes the key structural elements that form the system of trust in AI systems, the methods of ensuring trust, and the characteristics of AI systems. The article also examines the role of data in the operation of AI systems. The article highlights and structures the areas of implementation of trusted AI technologies, and discusses the search for practical solutions to improve the secure and trusted operation of AI systems.

Keywords: artificial intelligence, artificial intelligence systems, trust, digital environment, standard, security, reliability, data, lifecycle, trusted technologies, neural networks

Введение

На современном этапе технологического развития существенное внимание отводится тематике искусственного интеллекта (ИИ), что преломляет отраслевой фокус внимания от цифровой трансформации к ИИ-трансформации. Использование ИИ для поиска и генерации информации, обработки данных и аналитики значительно влияет на эффективность и трудозатратность большинства существующих процессов — расширяет доступность цифровых услуг, сокращает большинство географических ограничений, способствует решению экологических, социальных и управленческих задач.

Внедрение ИИ в экономику, социальную сферу и государственное управление уже сегодня приносит определенный эффект¹ и, по экспертным оценкам, может достичь показателя в 4 % ВВП к 2028 г.² При этом ожидаемый экономический эффект к 2030 г. оценивается в 7,9—12,8 трлн руб. в год³. Например, только в здравоохранении прогнозируется эффект в 65 млрд руб. к 2030 г. посредством развития различных групп продуктов, таких как цифровые ассистенты, клиническая сводка, помощник врача, экспертный контроль⁴.

Помимо прямых экономических эффектов, к позитивным факторам относят также повышение качества обработки и аналитики информации, рост динамики и эффективности технологических процессов, расширение географии оказания

¹ URL: <http://government.ru/news/55306/> (дата обращения: 01.03.2026).

² URL: https://yakov.partners/upload/iblock/c5e/c8t1wrkdne5y9a4nqlcderalwny7xh4/20231218_AI_future.pdf?ysclid=lvj59xugqn182161365 (дата обращения: 01.03.2026).

³ URL: <https://yakovpartners.ru/publications/ai-2025/> (дата обращения: 01.03.2026).

⁴ URL: <https://yakovpartners.ru/publications/ai-healthcare/> (дата обращения: 01.03.2026).



услуг, улучшение ключевых метрик в процессах поддержки принятия решений, персонализацию и адресность, повышение безопасности и качества жизни, снижение издержек в ключевых отраслях экономики.

В то же время, формируя значительные предпосылки для фундаментальных преобразований в различных сферах общественных отношений, ИИ-решения вызывают и определенные опасения в части влияния на общественные процессы, культуру⁵, возможного нанесения вреда при обучении⁶, качества образования⁷.

Рассматривая вопросы изменения роли человека и права в информационных правоотношениях, В. Б. Наумов отмечает, что «несмотря на мизерный в исторических масштабах период проникновения ИИ в нашу жизнь, некоторые проводимые исследования дают основания для подтверждения гипотез обширного негативного воздействия ИИ», поднимая при этом проблематику критического мышления человеческого общества, изменения соответствующих навыков и воли⁸.

Отчасти подтверждая наметившиеся изменения в конфигурации человеческих навыков, исследование РОМИР фиксирует нисходящую тенденцию использования офисных программ (Word, Excel, PowerPoint и аналогов) и языков программирования (Python, SQL, C++ и др.) при увеличении динамики использования ИИ и нейросетей⁹.

Вместе с тем в отраслевых исследованиях¹⁰ экспертами также выявляются и другие риски применения ИИ-решений:

- рост количества некачественного контента в Интернете;
- принятие решений на основе недостоверных ответов сервиса;
- видоизменение рынка труда;
- стимулирование цифрового мошенничества;
- нарушение принятых в обществе норм.

Рассматривая роль и влияние ИИ на общественные отношения, следует отметить, что важным элементом цивилизованного развития технологий (и одновременно сдерживающим потенциальные негативные эффекты развития) традиционно выступает правовое регулирование. Однако и в этой плоскости отмечаются скудная и требующая ревизии система правового регулирования¹¹, необходимость поиска правовых конструкций регулирования¹², а вопросы, связанные с

⁵ Василевская Л. Ю. Кодекс этики для искусственного интеллекта: юридический миф и реальность // Гражданское право. 2023. № 2. С. 20.

⁶ Архипов В. В., Наумов В. Б., Старостенко В. А., Нестеров А. А. Использование искусственного интеллекта в высшем образовании: опыт СПбГУ // Труды по интеллектуальной собственности (Works on Intellectual Property). 2025. Т. 52. № 1. С. 128.

⁷ URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/iskusstvennyi-intellekt-v-shkole-dobro-ili-zlo> (дата обращения: 01.03.2026).

⁸ Наумов В. Б. Право и «Батлерианский джихад»: размышления об угрозах использования искусственного интеллекта // Информационное общество. 2025. № 2. С. 140.

⁹ Отчет «Информационные технологии в восприятии россиян — 2025». М., 2026. С. 64.

¹⁰ URL: <https://yakovpartners.ru/publications/gen-ai-regulation/> (дата обращения: 01.03.2026).

¹¹ Наумов В. Б. Указ. соч. С. 136.

¹² Батурич Ю. М., Полубинская С. В. Искусственный интеллект: правовой статус или правовой режим? // Государство и право. 2022. № 10. С. 152.

правовым статусом ИИ, рассматриваются в контексте защиты человека от неконтролируемого влияния ИИ и неизменности гарантий конституционных прав и свобод человека¹³.

В этой связи нельзя не отметить создание Центра развития искусственного интеллекта¹⁴, в задачи которого входят «нормативно-правовое регулирование обеспечения безопасности технологий ИИ, а также тиражирование лучших практик, к которым отнесены решения, доказавшие свою эффективность и безопасность». Очевидно, что выделение для тиражирования безопасных практик подчеркивает значимую роль аспекта безопасности в функционировании систем ИИ.

Значимость проблематики безопасности обусловлена в том числе большим набором возможностей для атак на системы искусственного интеллекта, среди которых отравление данных, атака инверсии модели, атака градиентного спуска и подмена модели, подмена данных и др.¹⁵ Не углубляясь в специфику защиты систем ИИ, стоит отметить, что столь широкий спектр потенциальных атак предопределяет необходимость классификации атак на системы ИИ.

Таким образом, лишь поверхностный анализ специфики функционирования ИИ-систем в контексте их влияния на общественные отношения позволяет отметить наличие комплексного рискового потенциала, что, в свою очередь, говорит о необходимости структурирования и систематизации соответствующих рисков.

Вместе с тем, помимо рисков результирующего воздействия ИИ-решений на общественные отношения, стоит выделить также значимую технологическую роль данных в механике функционирования систем ИИ и специфику их использования.

Поскольку технологически модели машинного обучения выполняют аппроксимацию требуемой функции по таблице ее значений, построенной на основе заданного обучающего набора наблюдений, очевидно, что именно данные, их наборы и структура являются ключевым элементом ИИ-систем и залогом их качественного и продуктивного функционирования.

И здесь важную роль играют такие свойства данных, как качество, адекватность данных запросу (алгоритм может быть обучен на данных, ориентированных на другие задачи) и их достоверность (не зря в рамках работы над национальным проектом «Экономика данных» предусматривалась проработка мероприятий по выявлению недостоверных данных, в том числе генерируемых с использованием ИИ¹⁶).

Другой важной составляющей механики использования данных является правомерность их использования, поскольку определенные категории данных, необходимые для обучения нейронных сетей, не могут передаваться сторонним сервисам в силу обязательств по конфиденциальности (например коммерческой, адвокатской тайне и др.).

¹³ Карцхия А. А. Правовая охрана достижений искусственного интеллекта // ИС. Авторское право и смежные права. 2024. № 4. С. 4.

¹⁴ Дмитрий Григоренко: Правительство создает Центр развития искусственного интеллекта // URL: <http://government.ru/news/55306/> (дата обращения: 01.03.2026).

¹⁵ (Не)доверенный ИИ: обучать нельзя запретить // URL: <https://kryptonite.ru> <https://kryptonite.ru/articles/expert-discussion-of-trusted-ai/> (дата обращения: 01.03.2026).

¹⁶ URL: <http://government.ru/news/50469/> (дата обращения: 01.03.2026).



Нередко возникает и такая уникальная особенность технологий ИИ, как «проблема соблюдения баланса между требованиями по защите персональных данных и необходимостью их использования для обучения систем ИИ»¹⁷.

Доверенное функционирование

Любое взаимодействие, в том числе в коммуникационной и цифровой среде, в целом возможно лишь при выполнении определенного набора фундаментальных принципов, одним из которых является доверие. Не является исключением и отрасль ИИ, конструктивное развитие и совершенствование которой в условиях все более глубокой интеграции алгоритмов в общественные отношения, равно как и любых других прорывных технологий, возможно лишь в состоянии доверия, при доверенном «сотрудничестве» с пользователями и потребителями.

Вместе с тем стремительность и интенсивность процессов цифровой трансформации оказывают значительное влияние на степень доверия, «подрывая доверие людей к цифровым технологиям и к информационным коммуникациям»¹⁸. Более того, ситуация развивается в период, когда одновременно фиксируется тенденция снижения доверия и к праву, как к основному социальному регулятору¹⁹.

В указанных условиях формирования тенденции к снижению доверия ключевые документы по тематике ИИ предполагают доверенный вектор развития соответствующих технологий. Так, Кодекс этики в сфере искусственного интеллекта²⁰ рекомендует акторам ИИ проводить мероприятия, направленные на повышение уровня доверия и осведомленности пользователей и общества в целом.

В то же время Стратегия развития искусственного интеллекта²¹ (далее — Стратегия) фиксирует, что отсутствие понимания того, как искусственный интеллект достигает результатов, является одной из причин низкого уровня доверия к соответствующим технологиям и может стать препятствием для их развития, а к основным задачам развития отнесено обязательное внедрение доверенных технологий искусственного интеллекта в областях его использования, где может быть нанесен ущерб безопасности Российской Федерации.

При этом к показателям, характеризующим достижение целей Стратегии, отнесено достижение роста показателя уровня доверия граждан к соответствующим технологиям в 2030 г. до 80 %.

Не ставя целью на данном этапе исследование гносеологической стороны понятия доверия и его сущности в целом, попробуем понять, что лежит в основе

¹⁷ Наумов В. Б., Тютюк Е. В. Правовые проблемы машинного обучения // Образование и право. 2020. № 6. С. 220.

¹⁸ Наумов В. Б. Указ. соч. С. 135.

¹⁹ Polyakova T. A., Naumov V. B., Minbaleev A. V. (2022). Trust in the law during the digital transformation // Государство и право. 2022. № 11. С. 140.

²⁰ URL: <https://a-ai.ru> по состоянию на 10.01.2022 (дата обращения: 01.03.2026).

²¹ Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // СЗ РФ. 2019. № 41. Ст. 5700.

категории доверия применительно к системам ИИ, каковы подходы к обеспечению доверенного функционирования систем ИИ и роли данных при этом.

Несмотря на всю ширину спектра общественных отношений, к которым применяется категория доверия, и частоту такого применения, смысл, как правило, определяется текущим контекстом. При этом в условиях критического влияния на правоотношения единого правового подхода в действующем законодательстве нет²².

В технологическом контексте доверие в исследованиях рассматривается как сочетание нескольких факторов: техническое доверие к непосредственному решению (т.е. способность выполнять заявленную задачу), *доверие к данным*, лежащим в основе алгоритма, и готовность к принятию результата²³. В то же время при оценке надежности систем ИИ выделяют факторы доверия: теоретическое обоснование моделей, доказанную эффективность алгоритмов решения оптимизационных задач, *доверенный датасет*, использование доверенного ПО и аппаратных платформ²⁴.

Как видим, доверие к данным в экспертных подходах выделяется среди ключевых элементов, формирующих структуру доверия к ИИ. При этом непосредственный вопрос дает немало поводов для размышления, поскольку классическая наука обеспечивает доверие к результатам, основываясь на математических вычислениях и законах физики, в том числе времени. Большинство же алгоритмов основаны лишь на эмпирических данных и могут не иметь причинно-следственной структуры.

Основные направления внедрения доверенных технологий

Возвращаясь к вопросу обеспечения доверия к системам ИИ, обратимся к положениям Стратегии, согласно которым к основным направлениям внедрения доверенных технологий ИИ отнесены:

- внедрение доверенных технологий ИИ в программы цифровой трансформации;
- формирование компетенций, позволяющих использовать доверенные технологии ИИ и большие фундаментальные модели;
- методическое и нормативно-правовое обеспечение внедрения доверенных технологий ИИ в государственном управлении;
- определение единого критерия для координации деятельности по внедрению доверенных технологий ИИ;

²² Химченко А. И. Актуальные информационно-правовые вопросы формирования цифровой среды доверия // Правовое государство: теория и практика. 2023. № 4. С. 84.

²³ Профессор Центра ИИ «Сколтеха», заведующий лабораторией в области доверенного искусственного интеллекта Иван Тюкин рассказал «Ъ-Науке», что такое доверенный искусственный интеллект // URL: <https://www.kommersant.ru/doc/7639406> (дата обращения: 11.04.2026).

²⁴ (Не)доверенный ИИ: обучать нельзя запретить.



- формирование реестра апробированных доверенных технологий ИИ, проверенных на угрозы информационной безопасности;
- подготовка проектов по разработке и внедрению доверенных технологий ИИ в отраслях экономики и социальной сферы;
- создание инфраструктуры, необходимой для использования доверенных технологий ИИ;
- внедрение сертифицированных решений;
- обеспечение внедрения и использования доверенных технологий ИИ для выполнения текущих задач и другие мероприятия.

В основе подхода к созданию комплексной системы нормативно-правового регулирования общественных отношений, связанных с развитием и использованием технологий ИИ, определены следующие принципы:

- разработка, создание и использование технологий ИИ для тех областей их применения, в которых может быть нанесен ущерб безопасности Российской Федерации, в соответствии с требованиями информационной безопасности доверенных технологий;
- создание доверенного программного обеспечения для разработки безопасных и функционально эффективных решений в области ИИ по единым открытым стандартам.

К числу задач развития отнесено и формирование «единого пространства» доверенных технологий ИИ, продвижение отечественных доверенных технологий ИИ.

Вместе с тем в положениях Стратегии определяется, что доверенные технологии искусственного интеллекта — это технологии, отвечающие стандартам безопасности, разработанные с учетом принципов объективности, недискриминации, этичности, исключающие при их использовании возможность причинения вреда человеку и нарушения его основополагающих прав и свобод, нанесения ущерба интересам общества и государства, технологическое решение, соответствующее стандартам безопасности, разработанное с учетом объективности, непредвзятости, этичности и исключения применения для нанесения угрозы гражданам и государству. При этом выделить среди всего массива технологий ИИ доверенные не представляется возможным, так как по этим составляющим не разработаны требования и методики подтверждения требований.

Поскольку согласно Стратегии технологически ИИ состоит из информационно-коммуникационной инфраструктуры, ПО и сервисов обработки данных и принятия решений, то для обеспечения доверия ИИ к указанным сущностям необходимо сформировать и предъявить стандарты безопасности, критерии «доверенности».

Помимо этого, имеет смысл обратиться также к техническому регулированию. Так, проблематика доверия находит отражение в Национальном стандарте РФ ГОСТ Р 59276-2020 (Стандарт)²⁵, где доверие определяется как важнейшее условие при решении ответственных задач обработки данных.

²⁵ ГОСТ Р 59276-2020 «Национальный стандарт Российской Федерации. Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения» (утв. и введен в действие приказом Росстандарта от 23.12.2020 № 1371-ст).

Вопросы обеспечения доверия к системам ИИ рассматриваются на основе подтверждения их качества. В соответствии со Стандартом систему подтверждения образуют существенные характеристики систем ИИ, а также факторы, приводящие к снижению качества систем ИИ. Кроме того, на обеспечение доверия оказывают влияние особенности, возникающие на различных стадиях жизненного цикла, а также уровнях архитектуры систем ИИ.

Проверка доверия к системе ИИ реализуется посредством установления подтверждения соответствия характеристик системы ИИ установленным требованиям. В связи с тем, что способность системы ИИ вызывать доверие может изменяться во времени, Стандартом рекомендуется использовать контрольные точки проверки доверия на протяжении жизненного цикла системы. В зависимости от фактора снижения качества системы ИИ Стандартом определяются способы обеспечения доверия к ней. При определении доверия систем ИИ выделяются три уровня архитектуры (физический, инфраструктурный и прикладной), для каждого из которых формируются свои существенные характеристики, к которым отнесены выполнение проверочных мероприятий, выполнение требований безопасности ИТ-инфраструктуры, подтверждения надежности и безопасности ПО.

В условиях фактического отсутствия правового регулирования ИИ следует отметить и то, что проблематика регулирования ИИ находится в фокусе внимания профильных институтов. Так, Минцифры России опубликовало для общественного обсуждения законопроект «Об основах госрегулирования сфер применения технологий искусственного интеллекта»²⁶, призванный на законодательном уровне закрепить правила разработки и использования ИИ.

Несмотря на начальную стадию проработки, нельзя не отметить внимание законодателя к проблематике обеспечения доверенного функционирования. Законопроект предусматривает разделение моделей ИИ на категории в зависимости от их происхождения и уровня доверия, при этом выделяются доверенные модели, подлежащие использованию в государственных информационных системах и на объектах критической информационной инфраструктуры.

Заключение

Тематика развития ИИ в настоящее время находится в активном фокусе внимания государства и различных институтов развития, приобретая ключевое значение в реализации и достижении стратегических целей развития, развитии отдельных секторов экономики и формировании новых технологических подходов.

Отсутствие правового регулирования на определенном этапе способствовало как динамичному развитию соответствующих технологий, так и формированию определенного рискованного потенциала от использования. Одновременно стратегический подход к развитию и применению технологий ИИ подразумевает их доверенное и безопасное использование.

Вместе с тем подходы к обеспечению доверия к системам ИИ в настоящее время находят отражение лишь на стратегическом уровне и уровне стандартизации,

²⁶ URL: <http://regulation.gov.ru/Eutities/Npa/view/166424> (дата обращения: 19.03.2026).



в то время как такие структурные составляющие, как требования, методики их подтверждения, стандарты безопасности к системам ИИ (и их составляющим), не сформированы.

Одним из ключевых (с точки зрения как технологической реализации, так и достижения указанных состояний) структурных элементов механики ИИ являются данные. И в вопросе обеспечения доверенного функционирования систем ИИ приоритетной задачей является формирование стандартов безопасности и критериев «доверенности» данных.

БИБЛИОГРАФИЯ

1. *Архипов В. В., Наумов В. Б., Старостенко В. А., Нестеров А. А.* Использование искусственного интеллекта в высшем образовании: опыт СПбГУ // Труды по интеллектуальной собственности (Works on Intellectual Property). — 2025. — Т. 52. — № 1.
2. *Батулин Ю. М., Полубинская С. В.* Искусственный интеллект: правовой статус или правовой режим? // Государство и право. — 2022. — № 10. — С. 141—154.
3. *Василевская Л. Ю.* Кодекс этики для искусственного интеллекта: юридический миф и реальность // Гражданское право. — 2023. — № 2. — С. 19—22.
4. *Карцхия А. А.* Правовая охрана достижений искусственного интеллекта // ИС. Авторское право и смежные права. — 2024. — № 4. — С. 4—16.
5. *Наумов В. Б.* Право и «Батлерианский джихад»: размышления об угрозах использования искусственного интеллекта // Информационное общество. — 2025. — № 2. — С. 131—144.
6. *Наумов В. Б., Тютюк Е. В.* Правовые проблемы машинного обучения // Образование и право. — 2020. — № 6.
7. *Химченко А. И.* Актуальные информационно-правовые вопросы формирования цифровой среды доверия // Правовое государство: теория и практика. — 2023. — № 4. — С. 78—86.
8. *Polyakova T. A., Naumov V. B., Minbaleev A. V.* Trust in the law during the digital transformation // Государство и право. — 2022. — № 11.

Обеспечение суверенитета в киберпространстве

Инструменты инновационной политики государства в обеспечении национального суверенитета в условиях цифровой трансформации в Российской Федерации¹

Аннотация. Статья посвящена исследованию актуальных информационно-правовых вопросов, связанных со значением и возрастающей ценностью государственного суверенитета под влиянием современных технологий в условиях цифровой трансформации. В фокусе внимания находятся вопросы о приоритетах развития информационного права и укрепления национального суверенитета в цифровую эпоху. Авторы акцентируют внимание на особенностях и проблемах правового обеспечения информационного суверенитета и информационной безопасности Российской Федерации, а также правового регулирования безопасности искусственного интеллекта.

Ключевые слова: национальный суверенитет, информационная безопасность, информационное законодательство, информационное право, искусственный интеллект, цифровая трансформация, цифровые технологии

DOI: 10.17803/2311-5998.2026.142.6.095-103



**Татьяна Анатольевна
ПОЛЯКОВА,**

главный научный сотрудник,
и.о. зав. сектором
информационного
права и международной
информационной безопасности
Института государства
и права Российской академии
наук, доктор юридических наук,
профессор,
заслуженный юрист РФ
polyakova_ta@mail.ru
119019, Россия, г. Москва,
ул. Знаменка, д. 10



**Наталья Анатольевна
ТРОЯН,**

старший научный сотрудник
сектора информационного
права и международной
информационной безопасности
Института государства
и права Российской академии
наук, кандидат юридических
наук
n-troyan66@yandex.ru
119019, Россия, г. Москва,
ул. Знаменка, д. 10

¹ Статья написана в рамках Государственного задания FMUZ-2024-0035 «Обеспечение цифрового суверенитета и информационной безопасности правовыми средствами».

© Полякова Т. А.,
Троян Н. А., 2026

Tatiana A. POLYAKOVA,

*Chief Researcher, Acting Head of the Information Law and International
Information Security Sector at the Institute of State and Law
of the Russian Academy of Sciences,
Dr. Sci. (Law), Professor, Honored Lawyer of the Russian Federation*
polyakova_ta@mail.ru

10, ul. Znamenka, Moscow, Russia, 119019

Natalia A. TROYAN,

*Senior Researcher, Information Law and
International Information Security Sector,
Institute of State and Law, Russian Academy of Sciences,
Cand. Sci. (Law)*

n-troyan66@yandex.ru

10, ul. Znamenka, Moscow, Russia, 119019

Instruments of State Innovation Policy to Ensuring National Sovereignty in the Context of Digital Transformation in the Russian Federation

Abstract. *This article is devoted to the study of topical information and legal issues related to the significance and increasing value of state sovereignty under the influence of modern technologies in the context of digital transformation. The focus is on the priorities for the development of information law and the strengthening of national sovereignty in the digital age. The authors highlight the specific features and challenges of the legal framework for information sovereignty and information security of the Russian Federation, as well as the legal regulation of artificial intelligence safety.*

Keywords: *national sovereignty, information security, information legislation, information law, artificial intelligence, digital transformation, digital technologies*

Актуальность проблемы

Актуальность перспективных фундаментальных исследований, направленных на обеспечение национального суверенитета и достижение технологического лидерства, обусловлена их ключевой ролью в цивилизационном развитии России в целях противодействия вызовам и угрозам в условиях цифровой трансформации. На современном этапе реализация научно-технологической политики и национальных проектов в условиях цифровой трансформации определяет значение и особое положение информационного права, которое рассматривается уже не только как новое научное направление, но и как инновационная отрасль, активно развивающаяся в современных условиях.

Цифровая трансформация государственного управления и развитие экономики данных предопределяют необходимость укрепления национального суверенитета в информационной сфере, разработки новых доктринальных положений, направленных на выявление угроз и уязвимостей информационной безопасности, включая кибербезопасность цифровой среды, расширения использования технологий искусственного интеллекта и совершенствования правовых инструментов. В связи со стремительным развитием российского законодательства возникла потребность в правовом регулировании механизмов и установлении правовых режимов в сфере цифровых технологий².

Большое значение имеет защита интересов государства, общества и граждан в информационном пространстве от больших вызовов и угроз. Поэтому сегодня обеспечение государственного суверенитета в условиях цифровой трансформации, а также безопасность в киберпространстве приобретают стратегический характер. Необходимо быстрое развитие российской доктрины информационного права, информационного законодательства, а также международных правовых актов по регулированию информационно-коммуникационной среды³. Важно обеспечить в условиях цифровой трансформации противодействие распространению фейков, защиту русского языка и культурного суверенитета, культурных ценностей, информационно-психологической безопасности⁴. Предметом научных дискуссий являются также актуальные вопросы формирования цифрового, сетевого и научно-технологического суверенитета, требующие пристального внимания в условиях современных вызовов. Особое внимание следует уделить нарушениям одного из ключевых принципов международного права — соблюдения суверенитета государства.

Парадигма суверенной государственности как основа эффективной публичной власти в современной России

Теоретическое исследование категории суверенитета позволяет рассматривать его как концепт, анализ которого предполагает признание за субъектом права суверенного статуса лишь при условии его фактической независимости. Известные теоретики права сформулировали различные определения суверенитета как признака государства. Один из выдающихся теоретиков права профессор

² Полякова Т. А., Троян Н. А. Обеспечение суверенитета в информационном пространстве — стратегическая задача национальной политики // Правовая политика и правовая жизнь. 2024. № 1. С. 43.

³ Полякова Т. А., Минбалеев А. В., Наумов В. Б. Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве // Государство и право. 2025. № 1. С. 160—173.

⁴ Савенков А. Н. Философия права и становление российского государства-цивилизации : монография. М. : Наука, 2024 ; Его же. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. 2017. № 10. С. 10.



А. Б. Венгеров отмечал, что «государственный суверенитет является одной из важнейших черт государства и заключается в верховенстве и независимости от какой-либо иной власти, обладании правом и возможностью осуществлять внутреннюю и внешнюю политику от имени всего общества внутри и вне страны»⁵.

Несколько иная позиция у А. И. Порфирьева, который указывал, что «в юридической науке понятие суверенитета проходит терминологический кризис, который ставит вопрос об актуальности данного термина и заключается в том, что смысл, вкладываемый юридической наукой в это понятие, вступает в противоречие с его современным фактическим правовым содержанием»⁶. По нашему мнению, современный этап развития права в России свидетельствует о том, что внимание к данному вопросу отнюдь не ослабевает и сегодня, в условиях развернувшейся турбулентности в мире и процессов цифровизации, активно обсуждаются и вопросы так называемого когнитивного суверенитета. В. Д. Никишина включает в его содержание медиабезопасность, культурный суверенитет, технологический суверенитет, управленческий суверенитет и правовую безопасность. Такой подход позволяет рассматривать когнитивный суверенитет не как изолированное явление, а как сложную системную категорию, интегрирующую различные аспекты национальной безопасности⁷.

Важно различать понятие суверенитета, совокупность суверенных прав и отдельные полномочия государства. Теоретическую основу создания единых основ в этой сфере составляют доктринальные юридико-логические модели, детерминирующие суверенность российской системы права. Так, член-корреспондент РАН, космонавт Ю. М. Батуринов отмечает, что «парад суверенитетов» 1988—1990 гг. естественным образом вел к «войне законов» и параличу хозяйственной жизни и далее по принципу нарастающей обратной связи к растаскиванию «суверенных» территорий»⁸. Ученый определил, что «в пределах государства, по праву, нет власти выше, чем власть государственная: ее правовой авторитет выше, чем всякой другой власти, ее веления имеют правовую силу — это верховная власть, иначе называемая суверенной. Суверенитет, т.е. верховенство, является необходимым признаком верховной государственной власти»⁹.

Сегодня парадигма, возникшая как фундамент для укрепления государственности, суверенитета и независимости, приобретает современные интерпретации. Поэтому новые подходы акцентируют внимание на необходимости анализа новых элементов системы суверенной государственности, среди которых информационная, технологическая, демографическая, экологическая, энергетическая и иные формы суверенитета. По этому поводу академик РАН, профессор А. Н. Савенков

⁵ Венгеров А. Б. Теория государства и права : учебник. 2-е изд. М. : Омега-Л, 2005. С. 92.

⁶ Порфирьев А. И. Национальный суверенитет в правовой природе российского федерализма. М. : Книгодел, 2009. С. 3.

⁷ Никишина В. Д. Правовое обеспечение медиабезопасности и когнитивного суверенитета: вызовы социальной инженерии, гибридных войн и механизмов Web 3.0 (часть 1) // Lex russica. 2024. № 77 (11). С. 145—158.

⁸ Батуринов Ю. М. Парад суверенитетов в СССР (Декларация независимости 1988—1990 гг.). М., 2020.

⁹ Батуринов Ю. М. Указ. соч.

справедливо отмечает, что трансформация «парадигмы государственного суверенитета на основе тенденции правовой интерпретации рассматривается как в форме “мягкого права”, так и развития экстерриториального действия законодательства ряда стран»¹⁰.

В свете растущего влияния ИИ на общество в условиях цифровой трансформации целесообразно рассматривать право через призму новых явлений, современных общественных отношений, цифровых технологий, технологий блокчейна, изменения передачи и хранения больших данных. Однако их дефиниции сегодня, к сожалению, законодательно не закреплены. Поэтому, на наш взгляд, целесообразно проведение новых междисциплинарных исследований для более глубокого изучения сфер их применения и существующих взаимосвязей. Анализ общетеоретических подходов свидетельствует, что суверенитет является обязательным признаком государства и является многогранной категорией в информационном пространстве. В этой связи возрастает необходимость выработки нового концептуального подхода к вопросам, связанным с осмыслением понятия информационного суверенитета¹¹.

Сегодня информационно-правовой механизм обеспечения государственного суверенитета представляется как совокупность организационных, нормативных, функциональных и регулирующих общественных отношений. Для развития информационной инфраструктуры в Российской Федерации необходимо на международном уровне отстаивать суверенное право государства и определять информационную, технологическую и экономическую политику в национальном сегменте сети Интернет. Благодаря цифровым технологиям и международным связям Россия может быстрее внедрять инновации в цифровую среду. Это позволяет превращать научные идеи в высокотехнологичные продукты, востребованные во всем мире. В этой связи возникает необходимость разработки нового подхода к вопросам, связанным с понятием информационного суверенитета¹².

Полагаем, что дополнительного анализа требует взаимосвязь государственно-го, цифрового и культурного суверенитетов. Это обусловлено тем, что в условиях массовой цифровизации информационное пространство и цифровые сервисы стали для граждан основной средой получения знаний и доступа к информации. Поэтому в системе взаимосвязанных понятий суверенитета особое значение имеет междисциплинарная оценка роли цифровых платформ и сервисов, доминирующих в цифровом пространстве, а также степени их вовлеченности в современное геополитическое противостояние.

В целях противодействия угрозам значимость приобретает научное обоснование развития системы правового обеспечения национального суверенитета,

¹⁰ Савенков А. Н. Философия права, правовое мышление и глобальные проблемы современной цивилизации // Трансформация парадигмы права в цивилизационном развитии человечества: доклады членов РАН / под общ. ред. А. Н. Савенкова. М., 2019. С. 67—69.

¹¹ Полякова Т. А., Троян Н. А. Вопросы развития научно-технологической политики в Российской Федерации: правовое обеспечение национального суверенитета и технологического лидерства // Правовая политика и правовая жизнь. 2025. № 2. С. 250.

¹² Полякова Т. А., Троян Н. А. Обеспечение суверенитета в информационном пространстве — стратегическая задача национальной политики.



включая его цифровой, технологический и культурный аспекты, а также разработка соответствующих мер. Это необходимо для совершенствования правовых механизмов информационной политики и обеспечения защиты конфиденциальной информации. Для эффективного противодействия цифровым угрозам требуется объединение усилий мирового сообщества и развитие международного сотрудничества в сфере информационной безопасности.

Многие вызовы и угрозы носят трансграничный характер, поэтому нельзя отрицать значение правового регулирования и общепризнанных принципов и норм международного права в цифровой среде. Одним из приоритетных направлений внешней политики Российской Федерации в информационном пространстве является укрепление интеграции и расширение взаимодействия в рамках региональных объединений — ШОС, БРИКС, СНГ, ОДКБ, а также Союзного государства Республики Беларусь и Российской Федерации. Эффективное решение задач по нейтрализации трансграничных угроз в цифровой среде требует интеграции усилий международного сообщества.

В этой связи особое значение приобретает дальнейшее продвижение российской инициативы — проекта Конвенции по обеспечению международной информационной безопасности, внесенного в ООН. Данный проект базируется на основополагающих принципах международного права: суверенном равенстве государств и недопустимости вмешательства в их внутренние дела. Особого внимания в этой связи заслуживает принятие 24 декабря 2024 г. Генеральной Ассамблеей ООН и подписание Россией, а также рядом других государств так называемой Ханойской конвенции, направленной на противодействие преступности в информационной сфере. Эта конвенция признается международно-правовым актом нового поколения и является единственным универсальным международным договором ООН в форме конвенции по данному вопросу. Также заслуживает внимания утверждение Концепции информационной безопасности Союзного государства Республики Беларусь и Российской Федерации.

Одной из ключевых задач мировой экономики в условиях цифровизации является формирование новой экономической модели, способствующей созданию современной ценности — данных, которые и определяют стратегические приоритеты государства¹³. Национальный проект «Экономика данных и цифровая трансформация государства»¹⁴ направлен на развитие экономики данных. В число основных задач включены: сбор и хранение данных, обеспечение суверенитета и безопасности, а также развитие технологий искусственного интеллекта.

Важными представляются обеспечение национальной безопасности, укрепление суверенитета государства и защита национальных интересов, внедрение

¹³ Минбалеев А. В. Проблемы и перспективы реагирования российского законодательства на современные вызовы и угрозы в условиях цифровой трансформации // Информационные технологии в юридической деятельности: теле-право : монография / отв. ред. А. А. Волкова, Д. В. Огородов. М. : Проспект, 2024.

¹⁴ Национальный проект «Экономика данных и цифровая трансформация государства. Утв. протоколом Президиума Совета при Президенте РФ по стратегическому развитию и национальным проектам от 20.12.2024 № 12-пр // URL: <http://government.ru/rugovclassifier/923/about/> (дата обращения: 13.05.2026).

технологических инноваций, направленных на повышение качества жизни населения. Среди основных стратегических документов в этой области — Стратегия научно-технологического развития Российской Федерации¹⁵. В Концепции технологического развития на период до 2030 года¹⁶ технологический суверенитет определен как одна из ключевых целей. Укрепление суверенитета государства является одной из приоритетных задач обеспечения защищенности национальных интересов в цифровую эпоху. В Указе Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»¹⁷ суверенитет указан как ключевой фактор национальной безопасности, необходимость развития собственных технологий и производственных мощностей позволит стране уменьшить зависимость от иностранных технологий и обеспечит устойчивость к внешним вызовам и угрозам. Современное переосмысление правовых категорий и разработка новых механизмов регулирования будут способствовать повышению уровня технологического развития нашей страны¹⁸.

Заключение

В условиях динамичного развития цифровизации необходимы новые подходы, направленные на обеспечение национального суверенитета государства. Очевидно, что сегодня требуется совершенствование правового регулирования, обеспечивающее быструю адаптацию системы правовых способов, приемов и средств к новым вызовам. Одним из приоритетных направлений в настоящее время является развитие доктрины информационного права, включающей правовое обеспечение национальной и международной информационной безопасности (в том числе кибербезопасности и киберстабильности).

Формируемая доктринальная модель развития информационного права, новых объектов и субъектов в условиях цифровой трансформации и инновационного развития нацелена на научное обоснование и систематизацию правового регулирования в рассматриваемой сфере. На современном этапе представляется важным обеспечить создание и развитие собственных фундаментальных моделей

¹⁵ Указ Президента РФ от 28.02.2024 № 145 «О Стратегии научно-технологического развития Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 28.02.2024.

¹⁶ Распоряжение Правительства РФ от 20.05.2023 № 1315-р «Об утверждении Концепции технологического развития на период до 2030 года» // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>, 20.02.2024.

¹⁷ Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (ч. II). Ст. 5351.

¹⁸ Полякова Т. А., Троян Н. А., Петровская О. В. Правовое обеспечение укрепления технологического суверенитета Российской Федерации на основе реализации модели импортозамещения // Правовая политика и правовая жизнь. 2024. № 3. С. 281—293.



искусственного интеллекта. Они должны быть конкурентоспособными в мировом масштабе и обладать суверенитетом¹⁹.

БИБЛИОГРАФИЯ

1. Батурин Ю. М. Парад суверенитетов в СССР (Декларация независимости 1988—1990 гг.). — М., 2020. — 54 с.
2. Венгеров А. Б. Теория государства и права : учебник. — 2-е изд. — М. : Омега-Л, 2005. — 607 с.
3. Минбалеев А. В. Проблемы и перспективы реагирования российского законодательства на современные вызовы и угрозы в условиях цифровой трансформации // Информационные технологии в юридической деятельности: теле-право : монография / отв. ред. А. А. Волкова, Д. В. Огородов. — М. : Проспект, 2024. — 296 с.
4. Минбалеев А. В., Петровская О. В. Проблемы реализации принципа достоверности информации в условиях цифровой трансформации // Российский юридический журнал. — 2022. — № 4 (145). — С. 20—28.
5. Никишин В. Д. Правовое обеспечение медиабезопасности и когнитивного суверенитета: вызовы социальной инженерии, гибридных войн и механизмов Web 3.0 (часть 1) // Lex russica. — 2024. — № 77 (11). — С. 145—158.
6. Полякова Т. А., Минбалеев А. В., Наумов В. Б. Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве // Государство и право. — 2025. — № 1. — С. 160—173.
7. Полякова Т. А., Троян Н. А. Вопросы развития научно-технологической политики в Российской Федерации: правовое обеспечение национального суверенитета и технологического лидерства // Правовая политика и правовая жизнь. — 2025. — № 2. — С. 249—262.
8. Полякова Т. А., Троян Н. А. Обеспечение суверенитета в информационном пространстве — стратегическая задача национальной политики // Правовая политика и правовая жизнь. — 2024. — № 1. — С. 41—53.
9. Полякова Т. А., Троян Н. А., Петровская О. В. Правовое обеспечение укрепления технологического суверенитета Российской Федерации на основе реализации модели импортозамещения // Правовая политика и правовая жизнь. — 2024. — № 3. — С. 281—293.
10. Порфирьев А. И. Национальный суверенитет в правовой природе российского федерализма. — М. : Книгодел, 2009. — 294 с.
11. Рыбакова О. С. Российская модель формирования правосознания молодежи в условиях многополярного мира // Формирование многополярного мира: вызовы и перспективы : сборник докладов XI Московского юридического фо-

¹⁹ Распоряжение Правительства РФ от 03.11.2023 № 3097-р «Об утверждении стратегического направления в области цифровой трансформации транспортной отрасли РФ до 2030 года» // URL: <https://www.garant.ru/products/ipo/prime/doc/407851313/> (дата обращения: 13.04.2026).

рума (XXIV Международной научно-практической конференции) : в 3 ч. — М., 2024. — С. 322—328.

12. Савенков А. Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. — 2017. — № 10. — С. 5—18.
13. Савенков А. Н. Философия права и становление российского государства-цивилизации : монография. — М. : Наука, 2024. — 739 с.
14. Савенков А. Н. Философия права, правовое мышление и глобальные проблемы современной цивилизации // Трансформация парадигмы права в цивилизационном развитии человечества : доклады членов РАН / под общ. ред. А. Н. Савенкова. — М., 2019. — С. 67—69.





**Олеся Рамильевна
ГИМАДРИСЛАМОВА,**

доцент кафедры
гражданского права
Института права
Уфимского университета
науки и технологий,
кандидат юридических наук
giolesya@yandex.ru
450005, Россия, г. Уфа,
ул. Достоевского, д. 131

Многоуровневая правовая модель доступа к информации в цифровой среде

Аннотация. В статье обосновывается необходимость развития режимного подхода к доступу к информации в цифровой среде. Традиционное разграничение общедоступной информации и информации с ограниченным доступом сохраняет значение, но уже не объясняет современные формы обращения сведений в государственных информационных системах, цифровых сервисах, поисковой выдаче и исследовательских массивах. Цель исследования — разработать многоуровневую правовую модель доступа к информации, позволяющую соотнести общедоступность, ограничение доступа, конфиденциальность, публичный интерес, технологический контекст обработки сведений и риск причинения вреда. Используются формально-юридический, системный и доктринально-аналитический методы. Предложена четырехуровневая модель, включающая общедоступную информацию, информацию процедурно ограниченного доступа, конфиденциальную информацию и информацию, требующую повышенной правовой охраны. Сделан вывод о том, что уровень доступа является не новой классификацией информации, а аналитической характеристикой режима обращения сведений в правовом и технологическом контексте. **Ключевые слова:** доступ к информации, цифровая среда, правовой режим, информационное право, конфиденциальность, персональные данные, общедоступная информация, ограниченный доступ, публичный интерес, цифровая трансформация

DOI: 10.17803/2311-5998.2026.142.6.104-111

Olesia R. GIMADRISLAMOVA,

Associate Professor,
Department of Civil Law, Institute of Law,
Ufa University of Science and Technology,
Cand. Sci. (Law)
giolesya@yandex.ru
131, ul. Dostoevsky, Ufa, Russia, 450005

Multilevel Legal Model of Access to Information in the Digital Environment

Abstract. The article substantiates the need to develop a regime-based approach to access to information in the digital environment. The traditional division between publicly available and restricted-access information remains legally significant, but no longer fully reflects modern information flows involving state information systems, digital services, search engines and research datasets. The purpose of the study is to develop a multilevel legal

model of access to information that correlates public availability, restricted access, confidentiality, public interest, technological context and the risk of harm. The methodological framework is based on formal legal, systemic and doctrinal-analytical methods. The article proposes a four-level model that includes publicly available information, procedurally restricted information, confidential information and information requiring enhanced legal protection. It is concluded that the level of access should be regarded not as a new classification of information, but as an analytical characteristic of the legal regime governing the circulation of information in a legal and technological context.
Keywords: access to information, digital environment, legal regime, information law, confidentiality, personal data, publicly available information, restricted access, public interest, digital transformation

Действующее информационное законодательство сохраняет разграничение общедоступной информации и информации с ограниченным доступом. Однако в цифровой среде такой двухуровневый подход уже недостаточен: одни и те же сведения могут использоваться в государственном управлении, размещаться в открытом доступе, обрабатываться цифровыми сервисами, индексироваться поисковыми системами и включаться в исследовательские массивы. Поэтому допустимость доступа должна оцениваться не только по формальному отнесению сведений к общедоступной информации или информации с ограниченным доступом, но и по цели использования, статусу получателя, форме предоставления, риску причинения вреда и возможности контроля за дальнейшим обращением сведений. Такая постановка соответствует тенденции развития информационного права в условиях цифровой трансформации, изменяющей объекты и субъектов информационных отношений, а также способы обращения информации¹.

Цель статьи состоит в обосновании многоуровневой правовой модели доступа к информации, позволяющей в рамках единого режимного подхода соотнести общедоступность, ограничение доступа, конфиденциальность, публичный интерес, технологический контекст и риск причинения вреда. Нормативные предпосылки модели уже существуют: Конституция РФ, федеральные законы закрепляют базовые и специальные режимы доступа к информации, обработки персональных данных, доступа к информации о деятельности публичных органов и судов².

¹ См.: Полякова Т. А., Минбалева А. В., Кроткова Н. В. Цифровая трансформация как правовой феномен и ее влияние на развитие информационного права и законодательства // Государство и право. 2025. № 11. С. 207—208, 216 ; Полякова Т. А., Троян Н. А. Информационное право и цифровая реальность: развитие, приоритеты и проблемы в условиях цифровой трансформации // Правовая информатика. 2025. № 2. С. 31—32.

² Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru> ; Федеральные законы от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448 ;



Однако эти акты регулируют отдельные режимы и процедуры и не создают общую конструкцию, позволяющую определить, как должен изменяться уровень доступа при смене цели использования сведений, круга получателей, формы предоставления или риска причинения вреда. Поэтому проблема доступа рассматривается в статье в контексте систематизации информационного законодательства, выработки единого понятийного аппарата и согласования общих начал регулирования информационных и цифровых отношений.

Доктринальные предпосылки многоуровневой модели доступа

В российской доктрине сформированы предпосылки для построения многоуровневой модели доступа к информации. Они связаны с разработкой понятий механизма правового регулирования, правового режима и способа правового воздействия. При таком разграничении доступ анализируется не как единичное разрешение или запрет, а как элемент режима обращения сведений³. В исследованиях конфиденциальности показано, что ограничение доступа не исчерпывается запретом разглашения и предполагает учет цели режима, объекта, статуса субъектов, процедуры обращения сведений и механизма охраны⁴.

Для построения модели значимы также разграничение общего и специального режимов информации, систематизация информации ограниченного доступа и различение общедоступной и ограниченной служебной информации⁵. При этом конфиденциальность не следует понимать как универсальный синоним всей

от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3451 ; от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // СЗ РФ. 2009. № 7. Ст. 776 ; от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // СЗ РФ. 2008. № 52 (ч. I). Ст. 6217.

³ См.: *Алексеев С. С.* Теория права. 2-е изд. М. : Бек, 1995. С. 215—216, 242—243 ; *Его же.* Механизм правового регулирования в социалистическом государстве. М. : Юрид. лит., 1966. С. 29, 33—35 ; *Яковлев В. Ф.* Избранные труды. М. : Статут, 2012. Т. 2 : Гражданское право: история и современность. Кн. 1. С. 66.

⁴ См.: *Камалова Г. Г.* Правовое обеспечение конфиденциальности информации в цифровую эпоху: современное состояние институционализации и перспективы // Государство и право. 2019. № 6. С. 75—78 ; *Ее же.* Правовое обеспечение конфиденциальности информации в условиях развития информационного общества : дис. ... д-ра юрид. наук. М., 2020. С. 95—96, 100, 106—107.

⁵ См.: *Терещенко Л. К.* Правовой режим информации : автореф. дис. ... д-ра юрид. наук : 12.00.14. М., 2011. С. 13, 15—18 ; *Камалова Г. Г.* Вопросы систематизации информации ограниченного доступа // Вестник Удмуртского университета. Серия : Экономика и право. 2016. Т. 26. Вып. 2. С. 108—109 ; *Ее же.* Вопросы ограничения доступа к информации в системе государственного управления // Вестник Удмуртского университета. Серия : Экономика и право. 2015. Т. 25. Вып. 6. С. 91—92, 97—98 ; *Ее же.* О правовом режиме служебной тайны // Вестник Удмуртского университета. Серия : Экономика и право. 2014. Т. 24. Вып. 4. С. 145—147, 149.

информации ограниченного доступа, а персональные данные — как весь массив чувствительной информации⁶. Сегодня важно разработать модель доступа, систематизирующую подходы к открытому, процедурно ограниченному, конфиденциальному обращению информации и к обращению сведений повышенной правовой охраны в цифровой среде.

Понятие уровня доступа к информации и структура многоуровневой модели

Под уровнем доступа к информации предлагается понимать установленную правом степень допустимости получения, использования, передачи и дальнейшего обращения сведений, определяемую характером охраняемого интереса, целью использования, статусом субъекта доступа и риском вреда. В цифровой среде значение имеют условия допуска, форма предоставления, пределы последующего использования и возможность контроля за дальнейшим обращением сведений. Поэтому уровень доступа выступает аналитической характеристикой режима обращения сведений в правовом и технологическом контексте.

Четырехуровневая модель является минимально достаточной: двухуровневая схема не охватывает массив сведений, предоставляемых при соблюдении специальных процедур или условий, а трехуровневая не позволяет отделить обычную конфиденциальность от сведений, раскрытие которых создает повышенный, масштабный или труднообратимый вред. Разграничение уровней проводится по интенсивности правовой охраны, процедуре допуска, кругу субъектов, допустимости дальнейшего использования и масштабу возможного вреда.

Первый уровень образует общедоступная информация. Для нее действует презумпция открытости, а специального обоснования интереса к сведениям не требуется. Этот уровень обеспечивает свободу информационной деятельности, гласность, подотчетность публичной власти и общественный контроль. Вместе с тем в цифровой среде открытость не всегда означает допустимость любых способов последующего использования информации.

Второй уровень — информация процедурно ограниченного доступа. Это сведения, которые не исключаются из информационного оборота, но предоставляются при соблюдении установленной процедуры: с учетом статуса заявителя, цели использования, формы запроса, срока хранения или размещения, необходимости обезличивания, объема предоставляемых данных либо запрета на последующее распространение. Суть этого уровня состоит не в абсолютном запрете, а в правовой фильтрации доступа. Его предпосылки содержатся в правилах о предоставлении информации о деятельности публичных органов и судов, режимах частичного раскрытия сведений, конструкциях обезличивания и

⁶ См.: Бундин М. В. Система информации ограниченного доступа и конфиденциальность // Вестник Нижегородского университета имени Н.И. Лобачевского. 2015. № 1. С. 122, 126; Волчинская Е. К. Место персональных данных в системе информации ограниченного доступа // Право. Журнал Высшей школы экономики. 2014. № 4. С. 194—196, 199—201.



различении открытой и ограниченной служебной информации⁷. К этому уровню относятся сведения из государственных информационных систем, судебные и административные материалы, а также иные массивы данных, предоставляемые в обезличенном, агрегированном или частичном виде.

В цифровой среде процедурно ограниченный доступ особенно важен, поскольку обращение информации все чаще опосредуется государственными информационными системами, цифровыми платформами, сервисами, базами данных, ИТ-активами и алгоритмическими инструментами. Под влиянием цифровой трансформации в информационном праве формируются новые категории, объекты и субъекты информационных правоотношений, а также ставится вопрос о специализированных субъективных информационных правах⁸. Поэтому доступ следует оценивать не только как доступ к отдельному документу, но и как доступ к сведениям, включенным в цифровую инфраструктуру и последующие процессы обработки.

Третий уровень — конфиденциальная информация. Доступ к ней возможен только при наличии специального правового основания; круг субъектов ограничен, а обращение сведений подчинено обязанности нераспространения, учету, контролю и мерам ответственности. К этому уровню относятся виды информации ограниченного доступа, для которых законом установлен режим конфиденциальности в силу частного, публичного или смешанного интереса⁹. Здесь конфиденциальность выступает одним из уровней доступа, а не универсальным объяснением всей системы ограничения доступа к информации.

Четвертый уровень — информация, требующая повышенной правовой охраны. Он не образует нового вида тайны, а охватывает случаи, когда общего режима конфиденциальности недостаточно из-за масштаба возможного вреда, публичной функции информации, ее системного значения или связи с личной сферой человека. К этому уровню могут относиться отдельные массивы персональных данных¹⁰, сведения о частной жизни, государственно значимая информация¹¹, данные из систем, обеспечивающих функционирование публичной власти, а также иные сведения, утрата контроля над которыми способна повлечь системные последствия. Здесь необходимы дополнительные условия допуска, усиленный контроль, фиксация операций и осторожность при оценке общественного интереса к раскрытию сведений.

⁷ См.: *Ижаев О. А., Кутейников Д. Л.* Правовое регулирование порядка предоставления информации ограниченного доступа, содержащейся в государственных информационных системах, третьим лицам: опыт зарубежных стран // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 12. С. 166, 172—173.

⁸ См.: *Полякова Т. А., Минбалева А. В., Кроткова Н. В.* Указ. соч. С. 211—212.

⁹ См.: *Камалова Г. Г.* Правовой режим информации ограниченного доступа: вопросы формирования понятийного аппарата // Вестник Удмуртского университета. Серия : Экономика и право. 2016. Т. 26. Вып. 4. С. 120—121, 123.

¹⁰ См.: *Минбалева А. В.* Перспективные направления правового регулирования персональных данных // Юридический вестник ДГУ. 2024. Т. 52. № 4 (72). С. 153, 155.

¹¹ См.: *Камалова Г. Г.* О системе государственно-значимой информации ограниченного доступа // Вестник Саратовской государственной юридической академии. 2014. № 4 (99). С. 81—82.

Критерии разграничения уровней доступа и изменение правового режима сведений

Уровни доступа не являются статичными. Правовая квалификация сведений и режим доступа к ним могут изменяться в зависимости от цели использования, временного фактора, степени обезличивания, включения сведений в иной цифровой процесс обработки, круга субъектов доступа и масштаба возможного вреда. В этом отношении цифровая среда делает особенно заметным подход, согласно которому допустимость информационного потока зависит от контекста, а не только от формальной квалификации сведений¹².

Критерии разграничения уровней доступа должны образовывать систему. Базовое значение имеют цель использования сведений, характер охраняемого интереса, риск вреда и его масштаб; уточняющее — статус субъекта, возможность обезличивания или агрегирования данных, временной фактор и обратимость последствий раскрытия; корректирующее — прозрачность, подотчетность, контроль и поддержание доверия. Если сведения одновременно обладают признаками нескольких уровней доступа, решающее значение должна иметь совокупная оценка цели использования, круга субъектов доступа и риска последующего вреда. При сомнениях приоритет следует отдавать более высокому уровню защиты, если раскрытие сведений не обусловлено ясно выраженным публичным интересом и не сопровождается достаточными гарантиями ограничения вреда.

Необходимость контекстной оценки доступа подтверждается судебной практикой¹³. Практическое значение модели состоит в возможности закрепить общий набор критериев разграничения уровней доступа. Модель может рассматриваться как элемент будущей общей части информационного законодательства, поскольку задает общую логику распределения доступа, ограничений, процедур, гарантий и ответственности. В этом контексте значим вывод о движении к системной кодификации информационного законодательства, учитывающей особенности цифровой среды и базовые конструкции регулирования информационных правоотношений¹⁴.

¹² См.: *Nissenbaum H. Privacy as Contextual Integrity // Washington Law Review. 2004. Vol. 79. No. 1. P. 137—138, 155—156 ; Idem. Contextual Integrity Up and Down the Data Food Chain // Theoretical Inquiries in Law. 2019. Vol. 20. No. 1. P. 225—227.*

¹³ См., например: определение Конституционного Суда РФ от 12 февраля 2019 г. № 274-О «Об отказе в принятии к рассмотрению жалоб Безрукова Сергея Витальевича на нарушение его конституционных прав пунктом 1 статьи 152.2 Гражданского кодекса Российской Федерации» // Вестник Конституционного Суда РФ. 2019. № 3 ; постановление Пленума Верховного Суда РФ от 23 июня 2015 г. № 25 «О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации» // Бюллетень Верховного Суда РФ. 2015. № 8. П. 44.

¹⁴ См.: *Полякова Т. А., Минбалева А. В., Наумов В. Б. К вопросу о кодификации информационного законодательства в условиях цифровой трансформации // Государство и право. 2024. № 1. С. 89.*



Заключение

Таким образом, доступ к информации в цифровой среде требует развития режимного подхода: простого разграничения общедоступной информации и информации с ограниченным доступом недостаточно для учета цели использования сведений, круга субъектов, технологического контекста и риска последующего вреда. В отечественной доктрине выработаны элементы такого решения, однако цифровая трансформация требует объединить их в конструкцию, позволяющую учитывать не только содержание сведений, но и условия их обращения.

Многоуровневая правовая модель доступа к информации является одним из шагов в этом направлении. Ее значение состоит не в замене существующих режимов новой универсальной классификацией, а в создании аналитического инструмента, позволяющего соотносить открытость, ограничение доступа, публичный интерес, защиту личности и последствия обращения сведений. Такая модель может стать связующим элементом между доктриной информационного права, судебной практикой и будущей систематизацией информационного законодательства¹⁵.

БИБЛИОГРАФИЯ

1. *Алексеев С. С.* Механизм правового регулирования в социалистическом государстве. — М. : Юрид. лит., 1966. — 187 с.
2. *Алексеев С. С.* Теория права. — 2-е изд. — М. : Бек, 1995. — 320 с.
3. *Бундин М. В.* Система информации ограниченного доступа и конфиденциальность // Вестник Нижегородского университета имени Н.И. Лобачевского. — 2015. — № 1. — С. 124—130.
4. *Волчинская Е. К.* Место персональных данных в системе информации ограниченного доступа // Право. Журнал Высшей школы экономики. — 2014. — № 4. — С. 193—207.
5. *Ижаев О. А., Кутейников Д. Л.* Правовое регулирование порядка предоставления информации ограниченного доступа, содержащейся в государственных информационных системах, третьим лицам: опыт зарубежных стран // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2022. — № 12. — С. 164—173.
6. *Камалова Г. Г.* Вопросы ограничения доступа к информации в системе государственного управления // Вестник Удмуртского университета. — Серия : Экономика и право. — 2015. — Т. 25. — Вып. 6. — С. 91—98.
7. *Камалова Г. Г.* Вопросы систематизации информации ограниченного доступа // Вестник Удмуртского университета. — Серия : Экономика и право. — 2016. — Т. 26. — Вып. 2. — С. 103—109.

¹⁵ См.: *Полякова Т. А., Минбалева А. В., Наумов В. Б.* Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве России // Государство и право. 2025. № 1. С. 169—170.

8. Камалова Г. Г. О правовом режиме служебной тайны // Вестник Удмуртского университета. — Серия : Экономика и право. — 2014. — Т. 24. — Вып. 4. — С. 145—152.
9. Камалова Г. Г. О системе государственно-значимой информации ограниченного доступа // Вестник Саратовской государственной юридической академии. — 2014. — № 4 (99). — С. 80—86.
10. Камалова Г. Г. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества : дис. ... д-ра юрид. наук. — М., 2020. — 472 с.
11. Камалова Г. Г. Правовое обеспечение конфиденциальности информации в цифровую эпоху: современное состояние институционализации и перспективы // Государство и право. — 2019. — № 6. — С. 74—83.
12. Камалова Г. Г. Правовой режим информации ограниченного доступа: вопросы формирования понятийного аппарата // Вестник Удмуртского университета. — Серия : Экономика и право. — 2016. — Т. 26. — Вып. 4. — С. 118—125.
13. Минбалеев А. В. Перспективные направления правового регулирования персональных данных // Юридический вестник ДГУ. — 2024. — Т. 52. — № 4 (72). — С. 152—156.
14. Полякова Т. А., Минбалеев А. В., Кроткова Н. В. Цифровая трансформация как правовой феномен и ее влияние на развитие информационного права и законодательства // Государство и право. — 2025. — № 11. — С. 204—219.
15. Полякова Т. А., Минбалеев А. В., Наумов В. Б. К вопросу о кодификации информационного законодательства в условиях цифровой трансформации // Государство и право. — 2024. — № 1. — С. 81—91.
16. Полякова Т. А., Минбалеев А. В., Наумов В. Б. Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве России // Государство и право. — 2025. — № 1. — С. 160—173.
17. Полякова Т. А., Троян Н. А. Информационное право и цифровая реальность: развитие, приоритеты и проблемы в условиях цифровой трансформации // Правовая информатика. — 2025. — № 2. — С. 31—41.
18. Терещенко Л. К. Правовой режим информации : автореф. дис. ... д-ра юрид. наук. — М., 2011. — 55 с.
19. Яковлев В. Ф. Избранные труды. — М. : Статут, 2012. — Т. 2 : Гражданское право: история и современность. — Кн. 1. — 976 с.
20. Nissenbaum H. Contextual Integrity Up and Down the Data Food Chain // Theoretical Inquiries in Law. — 2019. — Vol. 20. — No. 1. — P. 221—256.
21. Nissenbaum H. Privacy as Contextual Integrity // Washington Law Review. — 2004. — Vol. 79. — No. 1. — P. 119—158.

Правовое обеспечение кибербезопасности



**Гульфия Гафиятовна
КАМАЛОВА,**

заведующий кафедрой
информационной
безопасности в управлении
Удмуртского
государственного
университета,
доктор юридических наук,
доцент
gulfia.kamalova@gmail.com
426034, Россия, г. Ижевск,
ул. Университетская, д. 1

Проблемы правового обеспечения доверия и информационной безопасности в цифровую эпоху¹

Аннотация. Статья посвящена информационно-правовым вопросам обеспечения безопасности цифровой среды посредством развития различных регуляторных механизмов, направленных на формирование доверия к информационно-коммуникационным технологиям и результатам их использования. Автором рассматриваются проблемы становления понятия «доверие» как информационно-правовой категории, а также целесообразность развития механизмов обеспечения доверия в цифровой среде, включающих достоверность и конфиденциальность данных, безопасность цифровых технологий и каналов связи. Отмечается, что необходимо повысить определенность в отношении критериев доверенности составляющих цифровой среды, усилить требования в части обеспечения цифрового суверенитета и локализации данных, а также создать правовые условия минимизации инцидентов информационной безопасности. В результате исследования сделан вывод, что лишь сочетание правового и технического регулирования позволит достичь доверия и безопасности в цифровой среде.

Ключевые слова: информационное право, цифровое право, доверие, информационная безопасность, цифровые технологии, цифровая среда, идентификация, конфиденциальность, доверенные технологии, цифровой суверенитет

DOI: 10.17803/2311-5998.2026.142.6.112-119

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 26-18-00897 «Создание правовой модели национального цифрового пространства доверия в целях обеспечения информационной безопасности и государственного суверенитета Российской Федерации».

Gulfia G. KAMALOVA,

Head of the Department of Information Security in Management,

Udmurt State University,

Dr. Sci. (Law), Associate Professor

gulfia.kamalova@gmail.com

1, ul. Universitetskaya, Izhevsk, Russia, 426034

Problems of Legal Assurance of Trust and Information Security in the Digital Age

Abstract. *The article is devoted to information and legal issues of ensuring the security of the digital environment through the development of various regulatory mechanisms aimed at building trust in information and communication technologies and the results of their use. The author examines the problems of the formation of the concept of “trust” as an information and legal category, as well as the expediency of developing trust mechanisms in the digital environment, including the reliability and confidentiality of data, the security of digital technologies and communication channels. It is noted that it is necessary to increase certainty regarding the criteria for the power of attorney of the components of the digital environment, strengthen the requirements for ensuring digital sovereignty and data localization, as well as create legal conditions for minimizing information security incidents. As a result of the study, it was concluded that only a combination of legal and technical regulation will allow to achieve trust and security in the digital environment.*

Keywords: *information law, digital law, trust, information security, digital technologies, digital environment, identification, confidentiality, trusted technologies, digital sovereignty*

Введение

В условиях динамичного внедрения цифровых технологий во все области жизнедеятельности человека и трансформации общественных отношений под их влиянием в научном пространстве активизируются правовые дискуссии о доверии к цифровым технологиям и результатам их применения. Вместе с тем понятие «доверие» как правовая категория пока остается институционально не оформленным и используется в праве на основе общих представлений о нем. В связи с этим в рамках настоящего исследования сделана попытка определить основные теоретические подходы, которые целесообразно рассматривать как основания для оформления понятия доверия в качестве информационно-правовой категории для последующего определения основных правовых средств его обеспечения и формирования механизма обеспечения доверия в цифровой среде.

При проведении исследования основным его стержнем выступила идея о том, что формирование доверия со стороны общества, государства и гражданина к цифровой среде предполагает достижение высокого уровня информационной безопасности цифровых сервисов и платформ, информационных систем



и информационной инфраструктуры в целом. Вместе с тем правовые вопросы достижения доверия к цифровой среде как результата обеспечения информационной безопасности этическими, правовыми, организационными и техническими средствами в настоящее время недостаточно исследованы и требуют научного осмысления. При этом автор исследования в работе исходит из того, что доверие в цифровой среде достижимо при обеспечении высокого качества цифровых данных, цифровой зрелости механизмов обеспечения информационной безопасности объектов цифровой среды, надежности каналов связи и добросовестности участников правоотношений, соответствия функционала цифровых сервисов ожиданиям субъекта правоотношений, что позволит формировать необходимое позитивное отношение к взаимодействию к цифровой среде.

Реализация национального проекта России «Экономика данных и цифровая трансформация государства»², направленного на усиление достигнутых результатов в области цифровой экономики, закономерно включает вопросы обеспечения кибербезопасности. Стратегически также важно, что Указом Президента РФ «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» в приоритетные задачи включено развитие цифровых платформ, управление данными, автоматизация транзакций, внедрение технологий больших данных и искусственного интеллекта, расширение предоставления государственных услуг в электронной форме и др.³ Решение указанных задач представляется невозможным без правового обеспечения доверия к цифровой среде и, соответственно, ее безопасности. В связи с этим целью настоящего исследования является комплексный анализ формирующихся правовых механизмов обеспечения доверия к цифровым технологиям в рамках построения национальной цифровой среды доверия.

Основная часть

Понятие «доверие» является междисциплинарным и вместе с тем наиболее разработанным в психологии, экономике, политологии, философии и социологии⁴. В праве интерес к вопросам доверия, в том числе на уровне диссертационных исследований, связан с вопросами эффективности права, обеспечением народного доверия, ответственности за злоупотребление доверием, доверия к полиции и другими, в том числе в рамках диссертационных исследований⁵. Вместе

² Национальный проект «Экономика данных и цифровая трансформация государства» // Официальный сайт Правительства России. URL: <http://government.ru/rugovclassifier/923/about/> (дата обращения: 06.03.2026).

³ См., например: Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // СЗ РФ. 2024. № 20. Ст. 2584.

⁴ См., например: *Скрипкина Т. П.* Доверие как социально-психологическое явление : дис. ... д-ра психол. наук. Ростов н/Д, 1998.

⁵ См., например: *Напольских И. М.* Доверие как условие эффективности действия права : автореф. дис. ... канд. юрид. наук. М., 2024.

с тем доверие и взаимосвязанные понятия сравнительно широко используются в законодательстве как самостоятельный термин или составная часть различных понятий, включая такие, как доверенность, злоупотребление доверием, доверенная третья сторона. Следовательно, даже сравнительно беглый анализ показывает, что доверие в праве является сложным феноменом, не только охватывающим эмоциональное отношение субъекта к другому субъекту или объекту, но и объективно выраженным в действиях, оно может подкрепляться правовыми гарантиями и влияет на правомерность определенных действий, а также взаимосвязано с правовой культурой и правосознанием участника правоотношений.

Экспоненциальное внедрение информационно-коммуникационных технологий и цифровая трансформация актуализировали вопрос о понятии доверия как информационно-правовой категории, что в области правового регулирования информационных отношений приобрело особое значение в связи с особенностями опосредованного характера информационного взаимодействия в цифровой среде. Хотя некоторые исследователи в области права⁶ обращались к вопросам формирования доверия в цифровой среде, вместе с тем такие исследования пока немногочисленны.

Следует отметить эволюцию концепции доверия в праве, которая проявляется в условиях цифровизации переходом от проявления в рамках исключительно межличностных отношений к необходимости институциональных норм в связи с опосредованным взаимодействием в цифровой среде. Обращает на себя внимание то, что исследователи рассматривают развитие цифровой среды доверия как одно из ключевых условий становления цифровой экономики⁷ и связывают ее с конфиденциальностью данных, достоверностью информации, ролью и правовым статусом субъектов взаимодействия и защищенностью среды взаимодействия. Указанное определяет возможный круг направлений правового воздействия на общественные отношения для формирования и поддержания доверия к цифровой среде, что определяет исследовательский интерес в рамках настоящего исследования.

Доверие в цифровой среде, именуемое порой цифровым доверием, может определяться через уверенность субъектов правоотношений в безопасности используемых информационно-технических средств и технологий, а также через предсказуемость результатов их использования⁸. Это может быть достигнуто путем выполнения установленных нормативными правовыми актами и документами по техническому регулированию требований к цифровым данным, безопасности

⁶ См., например: *Химченко А. И.* Вопросы формирования цифровой среды доверия как структурного элемента цифровизации государственного управления // Правовое государство: теория и практика. 2022. № 3 (69). С. 159—164 ; *Яковлева Е. А.* Правовая природа и сущность цифровой доверенной среды // Безопасность как стратегический национальный приоритет России в условиях современности : материалы Шестого международного транспортно-правового форума. М., 2024. С. 297—301.

⁷ *Терещенко Л. К.* Единая цифровая среда доверия как условие формирования цифровой экономики // Информационное право. 2020. № 4. С. 12—15.

⁸ *Кузнецов В. И., Кабытов П. П.* Теоретические подходы к категории «цифровая среда доверия» // Юридические исследования. 2021. № 2. С. 64—74.



информационных систем и цифровых сервисов, каналов связи, а также посредством определения субъектов взаимодействия в цифровой среде.

Меры обеспечения высокого качества данных, представленных в цифровой форме, играют одну из ключевых ролей в формировании доверия со стороны пользователей. Это напрямую связано с проблемами обеспечения достоверности цифровых данных и противодействия неправомерному распространению недостоверной информации. В связи с этим следует признать справедливым, что информационные угрозы, направленные на манипулирование общественным сознанием, искажение исторической памяти народа, подрыв доверия к государственным институтам и разрушение моральных ориентиров российского общества, являются наиболее опасными и подрывают доверие граждан к информации, представленной в цифровой среде.

Кроме того, значимое место занимает безопасность обработки персональных данных и иной, связанной с личностью человека и представленной в цифровой форме информации, утечка которой прямо или косвенно может нарушить его права. Принципы обработки персональных данных, включая минимизацию объема обрабатываемых данных, установленный законодательством потенциал определенного контроля со стороны субъекта персональных данных служат инструментами укрепления доверия граждан к действиям оператора персональных данных и информационным системам. Федеральные органы исполнительной власти осуществляют активное совершенствование конкретизированных требований к обработке персональных данных⁹. Реализация таких требований предполагает разработку и внедрение оператором широкого круга процедур и технических средств защиты данных. Усиливается юридическая ответственность в данной области.

Вместе с тем проблемы с утечкой персональных данных продолжают сохраняться¹⁰, что указывает на недостаточность существующих мер обеспечения безопасности цифрового оборота персональных данных. Кроме того, формируются дополнительные аспекты обеспечения безопасности персональных данных в цифровой форме в связи с тем, что в настоящее время цифровые платформы и сервисы в целях продвижения бизнеса и государственного управления обрабатывают значительные массивы данных граждан, которые не всегда могут быть строго отнесены к персональным данным, но вместе с тем взаимосвязаны с ними. Однако законодательство России не содержит норм об обязанности оператора платформы или сервиса применять риск-ориентированный подход для защиты цифровых данных пользователей, формирования системы защиты информации

⁹ Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 17.06.2025.

¹⁰ См., например: Крупнейшие утечки персональных данных за год // INFOWATCH. URL: <https://www.infowatch.ru/analytics/daydzhesty-i-obzory/krupneyshiye-utechki-personalnykh-dannykh-za-god> (дата обращения: 17.03.2026).

на всех этапах жизненного цикла и критериев определения уровня «цифровой зрелости» безопасности такой системы¹¹.

Отсутствие таких требований и правил обеспечения прозрачности механизмов обработки цифровых данных может усиливать недоверие граждан к современным цифровым платформам и сервисам, используемым в бизнес-процессах и системе государственного управления. Таким образом, необходимо специальное регулирование в области функционирования цифровых платформ и сервисов с целью повышения безопасности, предсказуемости и прозрачности цифровой среды обработки данных. Этой же цели служит предоставление информации о применении рекомендательных технологий¹².

Одним из важнейших условий обеспечения доверия является идентификация и аутентификация пользователей, направленная на повышение их защищенности и ответственности за действия в цифровой среде. Правовое обеспечение идентификации в цифровой среде имеет определенные особенности и предполагает дополнительные меры конфиденциальности информации, что отмечал В. Б. Наумов, который предложил развитие в информационном праве тайны идентификации¹³. Важное значение в связи с этим приобретают Единая система идентификации и аутентификации¹⁴ и Единая биометрическая система.

Институционально цифровое доверие формируется через безопасность информации, обеспечиваемой, наряду с правовыми институтами, посредством выполнения требований документов по стандартизации, сертификации средств защиты информации; процедур мониторинга и аудита; лицензирования деятельности в сфере защиты информации. Указанное позволяет достичь определенной предсказуемости уровня безопасности цифровых сервисов. Однако во многом этот процесс сегодня затрудняет правовая определенность в вопросах статуса операторов цифровых платформ, сервисов и экосистем.

Таким образом, эволюция моделей регулирования цифровой среды для обеспечения доверия к ней должна охватывать совершенствование защиты данных и требований к безопасности информационных систем и цифровых сервисов и включать не только правовые нормы, но и технические стандарты и организационные мероприятия, направленные на защиту данных. В связи с этим технические и организационные меры целесообразно закрепить в нормативных правовых актах как обязательные элементы обеспечения доверия. Формирование

¹¹ Полякова Т. А., Минбалева А. В. Понятие и правовая природа «цифровой зрелости» // Государство и право. 2021. № 9. С. 107—116.

¹² Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2025) «Об информации, информационных технологиях и о защите информации». Статья 10.2-2. // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

¹³ Наумов В. Б. Задача обеспечения тайны идентификации в информационном праве // Мониторинг правоприменения. 2019. № 3 (32). С. 70—75.

¹⁴ Постановление Правительства РФ от 28.11.2011 № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // СЗ РФ. 2011. № 49 (ч. V). Ст. 7284.



доверия к цифровой среде носит комплексный характер и требует сочетания технических мер, организационной практики и правового регулирования, что позволит гарантированно обеспечить целостность, доступность и конфиденциальность информации.

В настоящее время стратегическое значение для обеспечения доверия к безопасности обработки цифровых данных в России имеют локализация данных как инструмент контроля и защиты критических массивов информации и достижение цифрового суверенитета России, что обусловлено потенциалом национального контроля безопасности компонентов цифровой среды¹⁵. В связи с этим целесообразно развитие вопросов юридической ответственности, включая вопросы распределения ответственности между субъектами и ответственности за преднамеренные алгоритмические ошибки. Кроме того, по-прежнему недостаточно развита юридическая ответственность за утечки информации по вине операторов цифровых платформ и информационных систем.

Проблемы в области информационной безопасности цифровых платформ и сервисов могут вызывать алармизм у граждан, усиливать их скептицизм в отношении цифровой трансформации государства, что создает определенные правовые риски. Усиление информационных угроз и усложнение их структуры требуют сегодня формализации процедур реагирования на инциденты информационной безопасности. В связи с этим целесообразно законодательное введение понятия «инцидент информационной безопасности» и установление процедур реагирования на них не только в части защиты персональных данных, но и для других критически важных цифровых данных.

Таким образом, проведенное исследование показало, что для достижения доверия и информационной безопасности в цифровой среде целесообразно решить несколько взаимосвязанных организационно-правовых задач:

- сформировать теоретические основы правового обеспечения доверия в цифровой среде;
- законодательно определить понятие доверия в цифровой среде;
- повысить определенность в отношении критериев доверенности составляющих цифровой среды;
- усилить нормативно-правовые требования к обеспечению цифрового суверенитета и локализации обработки цифровых данных;
- создать правовые условия минимизации рисков инцидентов информационной безопасности.

В завершение следует отметить, что только комплексный подход к регулированию цифровых технологий, обеспечение прозрачности алгоритмов и усиление юридической ответственности операторов цифровых платформ и сервисов, а также сочетание правового и технического регулирования позволят достичь доверия и безопасности в цифровой среде.

¹⁵ Камалова Г. Г. Национальный технологический суверенитет в сфере цифровых технологий: вопросы правового обеспечения // Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. № 10 (122). С. 52—60.

БИБЛИОГРАФИЯ

1. Камалова Г. Г. Национальный технологический суверенитет в сфере цифровых технологий: вопросы правового обеспечения // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2024. — № 10 (122). — С. 52—60.
2. Кузнецов В. И., Кабытов П. П. Теоретические подходы к категории «цифровая среда доверия» // Юридические исследования. — 2021. — № 2. — С. 64—74.
3. Напольских И. М. Доверие как условие эффективности действия права : автореф. дис. ... канд. юрид. наук. — М., 2024. — 35 с.
4. Наумов В. Б. Задача обеспечения тайны идентификации в информационном праве // Мониторинг правоприменения. — 2019. — № 3 (32). — С. 70—75.
5. Полякова Т. А., Минбалеев А. В. Понятие и правовая природа «цифровой зрелости» // Государство и право. — 2021. — № 9. — С. 107—116.
6. Скрипкина Т. П. Доверие как социально-психологическое явление : дис. ... д-ра психол. наук. — Ростов н/Д, 1998. — 392 с.
7. Терещенко Л. К. Единая цифровая среда доверия как условие формирования цифровой экономики // Информационное право. — 2020. — № 4. — С. 12—15.
8. Химченко А. И. Вопросы формирования цифровой среды доверия как структурного элемента цифровизации государственного управления // Правовое государство: теория и практика. — 2022. — № 3 (69). — С. 159—164.
9. Яковлева Е. А. Правовая природа и сущность цифровой доверенной среды // Безопасность как стратегический национальный приоритет России в условиях современности : материалы Шестого международного транспортно-правового форума. — М., 2024. — С. 297—301.





**Зарина Тамерлановна
ЗОЛОЕВА,**

старший преподаватель
кафедры теоретико-
исторических
правовых дисциплин
Северо-Осетинского
государственного
университета имени Коста
Левановича Хетагурова,
кандидат юридических наук
4noiabria@mail.ru
362025, Россия,
г. Владикавказ,
ул. Ватутина, д. 44–46

Обеспечение кибербезопасности в государствах Южного Кавказа: сравнительно-правовой анализ

Аннотация. Статья посвящена сравнительно-правовому анализу подходов государств Южного Кавказа — Грузии, Азербайджана и Армении — к обеспечению кибербезопасности. Исследование обеспечения кибербезопасности на Южном Кавказе актуально в силу ряда факторов, связанных с геополитической ситуацией, технологическим развитием, угрозами кибератак и необходимостью обеспечения цифровой стабильности государств региона. Этот вопрос приобретает особую значимость в условиях растущей цифровизации, использования киберпространства в политических и военных целях, а также в контексте конкуренции глобальных и региональных акторов за влияние в регионе. Цель работы — проанализировать правовые механизмы регулирования кибербезопасности в трех государствах и выявить существующие проблемы в этой сфере. В ходе исследования рассмотрены ключевые нормативные правовые акты и документы стратегического планирования Грузии, Азербайджана и Армении в сфере обеспечения кибербезопасности.

На основе анализа выявлены общие тенденции, сделаны выводы о различиях в подходах указанных стран к обеспечению кибербезопасности, выявлены общие проблемы региона в сфере кибербезопасности.

Ключевые слова: информационное право, киберпространство, информационная безопасность, кибератаки, кибербезопасность, правовое регулирование кибербезопасности, Южный Кавказ, Грузия, Азербайджан, Армения

DOI: 10.17803/2311-5998.2026.142.6.120-127

Zarina T. ZOLOEVA,

Senior Lecturer, Department of Theoretical and Historical
Legal Disciplines, Kosta Levonovich Khetagurov
North Ossetian State University, Cand. Sci. (Law)

4noiabria@mail.ru

44–46, ul. Vatutina, Vladikavkaz,
Russia, 362025

Ensuring Cybersecurity in the South Caucasus States: a Comparative Legal Analysis

Abstract. This article provides a comparative legal analysis of the approaches of the South Caucasus states — Georgia, Azerbaijan, and Armenia — to ensuring cybersecurity. Research into cybersecurity in the South Caucasus is relevant due to a number of factors related to the geopolitical situation, technological development, the threat of cyberattacks, and the need to ensure

digital stability in the region. This issue is particularly significant in the context of increasing digitalization, the use of cyberspace for political and military purposes, and the competition between global and regional actors for influence in the region. The objective of this study is to analyze the legal mechanisms regulating cybersecurity in the three states and identify existing challenges in this area. The study examines key regulatory legal acts and strategic planning documents of Georgia, Azerbaijan, and Armenia in the area of cybersecurity. Based on the analysis, common trends were identified and conclusions were drawn about the differences in countries' approaches to ensuring cybersecurity. Common problems in the region were identified: a shortage of qualified personnel; dependence on foreign technologies; gaps in legislation; data leaks; low levels of information literacy among the population; and duplication of authority between agencies.

Keywords: information law, cyberspace, information security, cyberattacks, cybersecurity, legal regulation of cybersecurity, the South Caucasus, Georgia, Azerbaijan, Armenia

Введение

В настоящее время для государств Южного Кавказа проблема обеспечения кибербезопасности стоит достаточно остро в связи с довольно частыми случаями утечек конфиденциальной информации и кибератак. В январе 2025 г. стало известно о масштабной утечке данных граждан Грузии¹. В 2024 г. в Азербайджане в сеть попали личные данные граждан в результате кибератак². В Армении были зафиксированы массовое распространение фейковой информации, утечки данных, DDoS-атаки³ и т.д. Кроме того, для данных государств сохраняется проблема недостатка квалифицированных кадров и обладания навыками информационной и медийной грамотности, что требует развития правового обеспечения в сфере формирования культуры информационной и кибербезопасности⁴ и соблюдения кибергигиены. Сохраняется и проблема зависимости от зарубежных технологий.

Исследование опыта правового обеспечения кибербезопасности государств Южного Кавказа представляет большой научный интерес в связи с недостаточной

¹ Entire Georgian country population exposed in a massive data leak. URL: <https://cybernews.com/security/entire-georgian-country-population-exposed/> (дата обращения: 10.03.2026).

² Госслужба: Предотвращены целевые кибератаки на сайты государственных учреждений // URL: https://azertag.az/ru/xeber/gossluzhba_predotvrashcheny_celevye_kiberataki_na_saity_gosudarstvennyh_uchrezhdeniy_video-3301240 (дата обращения: 10.03.2026).

³ Все по-старому: российские аналитики назвали главную причину киберуязвимости Армении // URL: <https://am.sputniknews.ru/20250905/vse-po-staromu-rossiyskie-analitiki-nazvali-glavnyuyu-prichinu-kiberuyazvimosti-armenii-92904749.html> (дата обращения: 10.03.2026).

⁴ Полякова Т. А., Минбалеев А. В., Троян Н. А. Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. 2023. № 5. С. 131.



разработанностью данной проблематики и особым, стратегически важным для России географическим расположением данных государств.

Подходы государств Южного Кавказа к правовому регулированию кибербезопасности

В соответствии с исследованием, опубликованным на сайте Национального индекса кибербезопасности, Грузия в 2025 г. заняла 22-е место в мире и 16-е — в Европе⁵, Армения в данном рейтинге заняла 95-е, а Азербайджан — 52-е место. Эти данные свидетельствуют о том, что среди государств Южного Кавказа и в мире Грузия достигла высоких результатов в сфере обеспечения информационной безопасности.

Государства Южного Кавказа, реагируя на современные угрозы, формируют свою правовую базу в сфере обеспечения информационной безопасности⁶, кибербезопасности и построения цифрового суверенитета⁷, демонстрируя разные подходы, что, вероятно, связано с их современными геополитическими ориентациями, уровнем социально-экономического и политического развития.

В конституциях Грузии, Азербайджана и Армении содержатся нормы, косвенно связанные с обеспечением кибербезопасности, например, через защиту персональных данных (ст. 34 Конституции Армении); тайну связи (ст. 33 Конституции Армении, ст. 32 Конституции Азербайджанской Республики); провозглашение права на доступ к информации о деятельности публичных учреждений (ст. 18 Конституции Грузии), права свободно получать и распространять информацию (ст. 18 Конституции Грузии, ст. 50 Конституции Азербайджанской Республики) и др. В Конституции Грузии закреплено право каждого человека на доступ к Интернету и его свободное использование (п. 4 ст. 17), что, по нашему мнению, представляет собой основу для дальнейшего расширения правового статуса граждан в контексте киберправа.

Основополагающим документом Грузии, определяющим угрозы, риски и вызовы, основные направления политики безопасности, является Концепция национальной безопасности Грузии, в соответствии с которой целью страны является создание системы информационной безопасности, в которой пагубные последствия любой кибератаки будут сведены к минимуму⁸. Анализ Концепции

⁵ National Cyber Security index // URL: <https://ncsi.ega.ee/ncsi-index/> (дата обращения: 10.03.2026).

⁶ Койбаев Б. Г., Золоева З. Т. Развитие информационного общества в Азербайджанской Республике. Владикавказ : Северо-Осетинский государственный университет имени К. Л. Хетагурова, 2024. С. 7.

⁷ Лолаева А. С. Суверенитет 2.0: защита национальных интересов в эпоху цифровых гибридных войн // Российская правовая система: в поисках национальной идентичности : сборник докладов XIV Московской юридической недели : в 6 ч., Москва, 26—29 ноября 2024 года. М. : Университет имени О.Е. Кутафина (МГЮА), 2025. С. 408.

⁸ საქართველოს პარლამენტის დადგენილება «საქართველოს ეროვნული უსაფრთხოების კონცეფციის» დამტკიცების შესახებ 23.12.2011. № 5589-რს // URL: <https://www.matsne.gov.ge/ka/document/view/43156?publication=0> (дата обращения: 10.03.2026).

показывает, что данный документ нуждается в обновлении с учетом современных реалий и эффективного реагирования на современные угрозы и вызовы, стоящие перед страной, так как с момента ее принятия прошло 15 лет, во многом изменилась геополитическая ситуация, появились новые угрозы.

Ключевым документом Грузии в исследуемой сфере является также Закон «Об информационной безопасности» 2012 г., который закрепляет определения понятий «информационная безопасность», «киберпространство», «кибератака» и другие; устанавливает права и обязанности публичного и частного секторов, а также механизмы государственного контроля⁹. Анализ данного документа позволяет сделать вывод о том, что в нем в качестве взаимозаменяемых используются термины «информационная безопасность» и «кибербезопасность».

Национальная стратегия кибербезопасности на 2021—2024 гг. также играла важную роль в обеспечении кибербезопасности, которая рассматривалась как часть национальной безопасности страны¹⁰. Однако в Грузии с 2024 г. отсутствует стратегия в данной области, что, по нашему мнению, негативно влияет на обеспечение кибербезопасности.

Кроме того, в Грузии действует Закон «О защите персональных данных», принятый 14.06.2023, который регулирует обработку данных на территории страны, включая автоматизированные и неавтоматизированные системы, что, по нашему мнению, непосредственно влияет на устойчивость информационных систем к киберугрозам.

В Концепции национальной безопасности Азербайджанской Республики, принятой 23.05.2007, закреплено, что политика информационной безопасности страны базируется на комплексе мер по защите государственных, общественных и частных информационных ресурсов, а также на обеспечении национальных интересов в информационной сфере¹¹. Однако данная Концепция имеет ряд существенных недостатков, связанных с чрезмерной фокусировкой на конкретных угрозах, недостаточной проработкой некоторых аспектов безопасности, а также с институциональными пробелами.

В Азербайджане также действует Закон «О персональных данных» от 11.05.2010, который регулирует сбор, обработку и защиту персональных данных, включая трансграничную передачу. Однако критерии отнесения данных к категориям конфиденциальных или общедоступных не всегда четко определены, что создает простор для толкований и может приводить к нарушениям прав субъектов данных.

⁹ Закон Грузии от 05.06.2012 № 6391-Іс «Об информационной безопасности» // URL: <https://matsne.gov.ge/ru/document/view/1679424?publication=4> (дата обращения: 10.02.2026).

¹⁰ საქართველოს მთავრობის დადგენილება «საქართველოს კიბერუსაფრთხოების 2021—2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ». 30.09.2021. № 482 // URL: <https://matsne.gov.ge/ka/document/view/5263611?publication=0> (дата обращения: 10.03.2026).

¹¹ Концепция национальной безопасности Азербайджанской Республики. Утв. распоряжением Президента Азербайджанской Республики от 23.05.2007 № 2198 // URL: <https://ir.rudn.ru/books/b1/p5/01.pdf> (дата обращения: 10.03.2026).



Указ Президента Азербайджана от 29.12.2004 «О мерах по обеспечению информационной безопасности в государственных органах Азербайджанской Республики» обязывает не включать в состав информационных систем и сетей связи, а также других информационных систем и сетей, используемых для обмена информацией (в том числе глобальной информационной сети Интернет), информационные системы, сети связи и персональные компьютеры, на которых обрабатывается служебная информация, содержащая государственную тайну либо служебную информацию ограниченного распространения¹².

В Азербайджанской Республике вопросы кибербезопасности получили закрепление сравнительно недавно — 28.08.2023 распоряжением Президента Азербайджанской Республики была утверждена Стратегия информационной и кибербезопасности на 2023—2027 гг.¹³ Однако, как показал ее анализ, определения термина «кибербезопасность» в тексте не содержится. В то же время она учитывает современные тренды и проблемы кибербезопасности и делает упор на выявление рисков безопасности в информационном пространстве, а также на укрепление готовности к угрозам, связанным с информационной агрессией и искажением фактов, нарушением национальных ценностей, и борьбу с киберпреступностью.

Представляется, что данная Стратегия демонстрирует новый подход, характеризующий переходом от модели реактивного реагирования на кибератаки и иные инциденты, к построению целостной национальной экосистемы кибербезопасности. Кроме того, в качестве ее особенности необходимо назвать комплексный подход, охватывающий не только технические аспекты, но и совершенствование законодательства, международное сотрудничество и др.

Представляется важным также отметить, что Азербайджан активно продвигает концепцию цифрового нейтралитета, настаивая на том, что кибертехнологии не должны использоваться для вмешательства во внутренние дела других стран.

В Армении важное место в системе регулирования отношений в исследуемой сфере занимает Стратегия кибербезопасности, принятая в 2017 г., в которой основной упор делается на защиту критически важной информационной инфраструктуры¹⁴. На наш взгляд, важно отметить, что в Стратегии акцент сделан на необходимость сотрудничества государственного и частного секторов с целью защиты критически важной информационной инфраструктуры частного сектора от кибератак, включая банковский сектор, государственные услуги и телекоммуникации.

С 04.01.2026 в Армении вступил в силу Закон «О кибербезопасности», который определяет кибербезопасность как комплекс организационных, технических

¹² Azərbaycan Respublikası Prezidentinin Fərmanı 29.12.2004-cü il № 172 «Azərbaycan Respublikasının dövlət orqanlarında informasiya təhlükəsizliyinin təmin edilməsi üzrə tədbirlər haqqında» // URL: <https://e-qanun.az/framework/5572> (дата обращения: 10.03.2026).

¹³ Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023—2027-ci illər üçün Strategiyası // URL: <https://itkk.gov.az/az/strategiya/strategiya-haqqinda> (дата обращения: 10.03.2026).

¹⁴ Стратегия кибербезопасности Армении 2017 г. // Единый веб-сайт для публикации правовых актов. URL: <https://www.e-draft.am/projects/581/about> (дата обращения: 10.03.2026).

и программных мер по защите информации в цифровых системах и сетях. Закон нацелен на создание безопасного киберпространства и защиту критически важной инфраструктуры, государственных и частных информационных систем¹⁵. Здесь следует подчеркнуть, что Закон обязывает частные компании соблюдать нормы кибергигиены и сообщать о киберинцидентах в органы государственной власти, а также четко определяет перечень критически важных объектов.

Проведенный анализ позволяет сделать вывод о том, что в государствах Южного Кавказа правовое обеспечение в сфере кибербезопасности находится в стадии формирования. Однако сохраняется проблема наличия пробелов в законодательстве этих государств, а также сохраняется несоответствие мировым стандартам кибербезопасности¹⁶. По нашему мнению, в условиях постоянного совершенствования информационных технологий и возрастания количества киберугроз существует необходимость дальнейшего совершенствования нормативно-правовой базы¹⁷, включая ужесточение ответственности за кибератаки, а также разработки законов, учитывающих успешные международные практики.

Развитие институциональных механизмов в сфере обеспечения кибербезопасности в государствах Южного Кавказа

Важную роль в обеспечении кибербезопасности играют и институциональные механизмы. Так, в результате исследования установлено, что в государствах Южного Кавказа применяются разные подходы к наименованию и статусу органов, ответственных за обеспечение кибербезопасности. Так, в Грузии обеспечение кибербезопасности относится к компетенции таких органов, как Бюро кибербезопасности при Министерстве обороны, Группа помощи Бюро кибербезопасности, Агентство по обмену данными при Министерстве юстиции.

В Азербайджане вопросы обеспечения кибербезопасности подведомственны Государственной службе специальной связи и информационной безопасности, а также Службе электронной безопасности при Министерстве цифрового развития и транспорта.

В Республике Армения вопросы обеспечения информационной безопасности отнесены к компетенции Службы национальной безопасности при Правительстве Республики Армения, а также автономного органа, формируемого Национальной группой реагирования на компьютерные чрезвычайные ситуации.

¹⁵ ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՕՐԵՆԸ «ԿԻԲԵՐԱՆԱՎՏԱՆԳՈՒԹՅԱՆ ՄԱՍԻՆ ԸՆԴՈՒՆՈՒՄԷ Ե 04.12.2025. № ՅՕ-442-Ն // URL: <http://www.parliament.am/legislation.php?sel=show&id=10064&lang=arm&enc=utf8> (дата обращения: 10.03.2026).

¹⁶ *Мкртчян А. Р.* Сравнительный анализ правовых стандартов кибербезопасности: Республика Армения и международное право // Международная Восемнадцатая годовичная научная конференция : сборник научных статей, Ереван, 2—6 декабря 2024 года. Ереван : Российско-Армянский (Славянский) университет, 2025. С. 95—104.

¹⁷ *Койбаев Б. Г., Усова Ю. В., Золоева З. Т.* Особенности реализации государственной политики в сфере развития информационного общества в Азербайджанской Республике // Современная наука и инновации. 2023. № 2 (42). С. 170.



Таким образом, в государствах Южного Кавказа сформирован организационный механизм противодействия угрозам кибербезопасности, однако исследователи отмечают проблемы дублирования полномочий силовых структур¹⁸, отсутствия скоординированного подхода¹⁹. Представляется, что это может затруднять эффективное реагирование на кибератаки, в связи с чем существует необходимость в модернизации.

Выводы

Правовая база в сфере кибербезопасности в государствах Южного Кавказа формируется на основе национальных законов, документов стратегического планирования и международных обязательств. Законодательные инициативы преимущественно ориентированы на обеспечение безопасности ключевых секторов экономики и системы государственного управления.

Из государств Южного Кавказа вопросы кибербезопасности ранее всех закрепила Грузия. В Армении и Азербайджане нормативные акты, регулирующие данные вопросы, были приняты позднее. До этого регулирование общественных отношений в данной сфере осуществлялось при помощи положений документов, регламентирующих вопросы информационной безопасности.

Анализ текущего состояния правового обеспечения кибербезопасности на Южном Кавказе позволяет сделать вывод о наличии устойчивой тенденции к усилению регуляторных мер в данной сфере. Наблюдается активное создание специализированных институтов, осуществляющих противодействие киберугрозам. При этом темпы и подходы к развитию нормативно-правовой базы в государствах региона существенно различаются. В то же время данные государства сталкиваются с необходимостью адаптации законодательства к быстро меняющейся цифровой среде, что сопровождается нехваткой квалифицированных кадров и необходимостью осуществления международного сотрудничества.

Государства Южного Кавказа демонстрируют разные подходы к правовому регулированию кибербезопасности и разную степень проработки регуляторных механизмов.

Так, подход Грузии в настоящее время характеризуется регулированием кибербезопасности в рамках Закона «Об информационной безопасности».

Республика Армения сделала шаг к системному регулированию посредством принятия Закона «О кибербезопасности», особенностью подхода этой страны является также закрепление необходимости сотрудничества государственного и

¹⁸ Ларссон Р., Квашилава Г. Информационная безопасность Грузии: проблемы развития информационно-коммуникационных технологий и создания программ в этой области // URL: https://ca-c.org.ru/journal/2003/journal_rus/cac-05/15.larrus.shtml (дата обращения: 10.03.2026).

¹⁹ Овакимян А. А. Политика Республики Армения в контексте обеспечения кибербезопасности // Шестнадцатая годовичная научная конференция : сборник научных статей конференции, приуроченной к 25-летию основания РАУ, Ереван, 5—9 декабря 2022 года. Ереван : Российско-Армянский (Славянский) университет, 2023. С. 306—312.

частного секторов с целью защиты критически важной информационной инфраструктуры.

Подход Азербайджанской Республики характеризуется сочетанием национального законодательства об информационной безопасности и документов стратегического планирования в сфере обеспечения кибербезопасности.

БИБЛИОГРАФИЯ

1. *Койбаев Б. Г., Золоева З. Т.* Развитие информационного общества в Азербайджанской Республике. — Владикавказ : Северо-Осетинский государственный университет имени К. Л. Хетагурова, 2024. — 172 с.
2. *Койбаев Б. Г., Усова Ю. В., Золоева З. Т.* Особенности реализации государственной политики в сфере развития информационного общества в Азербайджанской Республике // Современная наука и инновации. — 2023. — № 2 (42). — С. 168—174.
3. *Лолаева А. С.* Суверенитет 2.0: защита национальных интересов в эпоху цифровых гибридных войн // Российская правовая система: в поисках национальной идентичности : сборник докладов XIV Московской юридической недели : в 6 ч., Москва, 26—29 ноября 2024 года. — М. : Университет имени О.Е. Кутафина (МГЮА), 2025. — С. 406—409.
4. *Мкртчян А. Р.* Сравнительный анализ правовых стандартов кибербезопасности: Республика Армения и международное право // Международная Восемнадцатая годичная научная конференция : сборник научных статей, Ереван, 2—6 декабря 2024 года. — Ереван : Российско-Армянский (Славянский) университет, 2025. — С. 95—104.
5. *Овакимян А. А.* Политика РА в контексте обеспечения кибербезопасности // Шестнадцатая годичная научная конференция : сборник научных статей конференции, приуроченной к 25-летию основания РАУ, Ереван, 5—9 декабря 2022 года. — Ереван : Российско-Армянский (Славянский) университет, 2023. — С. 306—312.
6. *Полякова Т. А., Минбалева А. В., Троян Н. А.* Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. — 2023. — № 5. — С. 131—144.





**Кира Кирилловна
ТАРАН,**

доцент кафедры
информационного права
и цифровых технологий
Университета имени
О.Е. Кутафина (МГЮА),
кандидат юридических наук
taran.kira@yandex.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

Цифровой профиль: правовые проблемы и вопросы кибербезопасности¹

Аннотация. Статья посвящена развитию цифрового профиля в Российской Федерации. Рассмотрены ведущие документы, на основе которых развивается технология цифрового профиля и реализуется ее использование государственными органами РФ, кредитными, финансовыми организациями, работодателями и т.д. В статье выделены разновидности цифрового профиля, которые формируются в зависимости от целей взаимодействия лица с государственными и муниципальными органами, работодателями и др. Использование цифрового профиля повышает уровень кибербезопасности в стране, поскольку правоохранительные органы на основе цифрового профиля могут оперативнее получить информацию о правонарушителе. В статье также уделено внимание вопросам равенства цифровой информации документам в бумажном формате, (не)обязательности использования цифрового профиля финансовыми организациями, этическим и иным вопросам, которые необходимо учитывать при развитии правового регулирования данной технологии.

Ключевые слова: цифровой профиль, кибербезопасность, персональные данные, информационное право

DOI: 10.17803/2311-5998.2026.142.6.128-135

Kira K. TARAN,

Associate Professor of the Department of Information Law and Digital Technologies
of the Kutafin Moscow State Law University (MSAL),
Cand. Sci. (Law)

taran.kira@yandex.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Digital Profile, Legal and Cybersecurity Issues

Abstract. The article examines the development of digital profiles in the Russian Federation. Key documents of the digital profile technology development and its implementation by Russian government agencies, credit and financial institutions, employers, and others are esteemed in the article. The article identifies the different types of digital profiles, which are formed according to individual's goals for interacting with government and municipal authorities, employers, and others. Using a digital profile improves cybersecurity in

¹ Статья подготовлена в рамках выполнения работ по государственному заданию на тему «Развитие правовой системы в условиях обеспечения технологического лидерства Российской Федерации: национальные приоритеты и международные вызовы (FSMW-2026-0005)». Регистрационный номер: 126022017763-1.

the country, as law enforcement agencies can use a digital profile to obtain information about offenders quicker. The article also addresses the equality of digital information with paper documents, the optional/mandatory nature of digital profile use by financial institutions, ethical and other issues that must be considered when developing legal regulation of this technology.

Keywords: digital profile, cybersecurity, personal data, information law

Цифровой профиль — это сведения о физическом лице, которые дают о нем информацию определенного рода, причем это могут быть сведения различного характера, и для субъектов в цифровой среде они могут иметь разное значение. А. В. Минбалеев, Т. А. Полякова, В. В. Виноградова говорят о том, что цифровой профиль является «важнейшим фактором, обуславливающим персонализацию в общественной жизни, самореализацию... личной жизни и профессиональной деятельности»². Авторы обращают внимание на то, что данные, составляющие цифровой профиль, являются точными и достоверными, а также говорят о важности цели, с которой создается цифровой профиль.

Согласно Сценарию использования инфраструктуры цифрового профиля физического лица³ (версия 1.50) от 26.11.2025, разработанному Министерством цифрового развития, связи и массовых коммуникаций РФ (далее — Сценарий цифрового профиля физического лица), цифровой профиль представляет собой совокупность цифровых записей о гражданине. Можно выделить особенность, связанную с тем, что в законодательстве больше внимания уделяется цифровому профилю физического лица, чем юридического, хотя данные о юридическом лице могут быть тоже информативны как в финансовой сфере, так и в предпринимательской деятельности.

Термин «цифровой профиль» очень тесно связан с такими понятиями, как «цифровая личность» и «цифровой след». Цифровую личность, скорее, характеризуют действия лица в Интернете: посещение сайтов, которые представляют для нее интерес, использование социальных сетей, мессенджеров. Примечательно, что в литературе понятия «цифровая личность» и «цифровой профиль» могут охватываться термином «пользовательские данные»⁴.

Цифровой профиль может включать в себя интересы цифровой личности, если лицо будет аутентифицироваться со своим цифровым профилем при использовании сервисов в Интернете. Цифровой след — это конкретное действие лица в Интернете, оно может быть как негативного характера (например, буллинг), так и нейтрального и даже позитивного (например, участие в опросах, которые могут

² Виноградова Е. В., Минбалеев А. В., Полякова Т. А. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации // Правоприменение. 2021. Т. 5. № 4. С. 5—19.

³ Сценарии использования инфраструктуры цифрового профиля физического лица от 26.11.2025 // Минцифры. URL: <https://digital.gov.ru/documents/scenarii-ispolzovaniya-infrastruktury-cifrovogo-profilya-fizicheskogo-licza> (дата обращения: 25.03.2026).

⁴ Филиппова С. Ю., Харитонов Ю. С., Щербак Н. В. Правовое регулирование электронной коммерции : учебное пособие. М. : Юстицинформ, 2024.



быть анонимными) и т.д. С точки зрения повышения уровня кибербезопасности в информационном пространстве объединение цифрового профиля с цифровой личностью поможет правоохранительным органам быстрее выявлять злоумышленников, оборот товаров, запрещенных к распространению, лиц, которые занимаются травлей и буллингом в Интернете, и т.д. О. А. Степанов и М. М. Степанов говорят о важности идентификации цифровой личности в Интернете в связи с тем, что могут передаваться персональные данные конкретного человека⁵.

Отправной точкой развития цифрового профиля можно условно назвать 2019 г., когда на заседании президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности была утверждена концепция цифрового профиля. Задачей проекта ставилось обеспечение доступа через портал государственных услуг к данным о гражданине или юридическом лице. С этого момента ведомства начали разрабатывать дорожные карты, чтобы лица смогли пользоваться «суперсервисами», которые упростят взаимодействие между лицами и государственными органами⁶.

С 2019 г. проводится эксперимент по работе с цифровым профилем, установленный постановлением Правительства РФ от 03.06.2019 № 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» (далее — Постановление № 710). Этот длительный эксперимент был начат 01.07.2019, завершение планируется к 31.12.2030, и к настоящему моменту уровень оказания государственных услуг с развитием цифрового профиля повысился.

Круг участников эксперимента является широким (п. 3 Постановления № 710), включает субъектов, которые участвуют на обязательной и добровольной основе. Министерства, включая Министерство цифрового развития, связи и массовых коммуникаций РФ, Министерство экономического развития РФ, являются обязательными участниками. Добровольными участниками являются фонды, Центральный банк РФ, Судебный департамент при Верховном Суде РФ, Центральная избирательная комиссия РФ, ПАО «Ростелеком», Научно-исследовательский институт «Восход», высшие исполнительные органы государственной власти субъектов РФ, кредитные организации, операторы связи, физические лица, работодатели, многофункциональные центры предоставления государственных и муниципальных услуг и др.

Задача эксперимента — создание системы с точными данными, которые обладают взаимосвязью и единством в федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и

⁵ Степанов О. А., Степанов М. М. О цифровой идентичности человека в виртуальном пространстве // Российская юстиция. 2025. № 10. С. 30—35.

⁶ Максим Акимов провел заседание президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности / Правительство России. 29.03.2019 // URL: <http://government.ru/news/36205/> (дата обращения: 17.03.2026).

муниципальных услуг в электронной форме». На основе работы такой системы физические лица (граждане и иностранные граждане, лица без гражданства, юридические лица, индивидуальные предприниматели) могут получать информацию от государственных органов. Цифровой профиль может использоваться кредитными, страховыми организациями, операторами финансовых платформ, операторами связи и иными субъектами для упрощения и улучшения качества взаимодействия с заинтересованными физическими лицами (гражданами РФ, иностранными гражданами, лицами без гражданства, юридическими лицами и индивидуальными предпринимателями).

Разновидности цифрового профиля в зависимости от сферы его использования

В зависимости от сферы использования разновидности цифрового профиля следующие:

1. Цифровой профиль для работы с государственными информационными сервисами и государственными услугами.

2. Финансовый профиль, который характеризует финансовое состояние лица, наличие задолженностей, займов, кредитов и т.д. В России ведется формирование цифрового профиля на основе использования системы межведомственного взаимодействия, при которой используется система идентификации и аутентификации. Согласно письму Минцифры России от 19.01.2026 № МШ-П24-2389, цифровой профиль уже используют такие компании, как «МТС-Банк», «Т-Банк», страховая компания «Сбербанк Страхование» и др. В связи с активным внедрением цифрового профиля в финансовую сферу возникает вопрос, является ли цифровой профиль подтверждением наличия или отсутствия у лица задолженностей. Цифровой профиль является источником информации о финансовом положении лица, но обращение к цифровому профилю на данный момент является не обязательным, а, скорее, вспомогательным ресурсом, поскольку получить информацию о задолженности лица вполне возможно из иных источников, которые активно использовались до формирования данной технологии.

3. Кредитный профиль — кредитная история пользователя банка, аналитическая информация, собранная сотрудниками банка по вопросам кредитной стабильности клиента.

4. Медицинский профиль — информация о заболеваниях, методах лечения и обращениях физического лица за государственной медицинской помощью.

5. Цифровой профиль сотрудника организации. Работодатель собирает о соискателе и в дальнейшем о сотруднике организации большое количество сведений, причем ст. 86 ТК РФ не определяет перечень персональных данных, которые может получить сотрудник отдела кадров, т.е. цифровой профиль составляют как резюме, так и документы, которые предоставляет соискатель, в том числе и медицинские документы. Более того, цифровой профиль сотрудника организации будет пополняться, поскольку работодатель может использовать систему контроля за тем, как сотрудник выполняет работы, системы контроля посещения места работы (пробивание пропуска), видеонаблюдение, контроль за телефонными



переговорами, т.е. большой массив дополнительных данных. Л. И. Филющенко поднимает вопросы, связанные с цифровым профилем сотрудника, поскольку работодатели также участвуют в формировании цифрового профиля на добровольной основе, что ведет к возникновению споров в контексте обработки персональных данных⁷. О. В. Щербакова в контексте развития профессиональных навыков выделяет цифровой профиль школьника, студента в рамках вуза⁸, что уже реализуется в российских вузах.

6. Профиль, формируемый на основе использования электронных торговых платформ и маркетплейсов, где пользователь не только оставляет свои персональные данные, такие как фамилия, имя, отчетов, адрес регистрации, номер банковской карты, но и дает маркетплейсу сведения о своих предпочтениях, пунктах выдачи, которые он посещает, а также об иных своих интересах, поскольку лицо может быть переадресовано на сайт маркетплейса с другого сайта благодаря контекстной рекламе.

Сведения, формирующие цифровой профиль, собираются из различных источников, это могут быть как открытые данные, так и те сведения, которые формируются на основе взаимодействия с органом государственной власти. Например, справка СТД-ПФР из пенсионного фонда дает работодателю информацию о местах работы соискателя, должностях и их изменениях, временных промежутках, когда соискатель работал, а когда находился без работы. Социальный фонд России обеспечивает медицинские выплаты и тоже формирует цифровой профиль личности.

Классификация, представленная в настоящей статье, не является исчерпывающей и может быть дополнена.

Цифровой профиль формируется благодаря Единой биометрической системе, Единой системе идентификации и аутентификации, Единому регистру населения и др. Не следует путать тот факт, что данные реестры изначально были созданы для учета сведений, а не для цифрового профилирования.

Сценарий цифрового профиля физического лица подготовлен для реализации постановления Правительства РФ от 03.06.2019 № 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах». Согласно документу цифровой профиль гражданина формируется на основе ряда данных, таких как: 1) данные, которые содержатся в Единой системе идентификации и аутентификации (ЕСИА); 2) данные, которые формируются на основе запросов из государственных реестров; 3) цифровые согласия, которые связаны с цифровым профилем. Цифровой профиль важен и крайне удобен для взаимодействия с порталом государственных услуг, а также с банками.

Работа с цифровым профилем возможна в двух форматах: онлайн и офлайн. В процессе работы онлайн пользователь — физическое лицо — использует мобильное приложение, информационный портал или сайт, в то время как в

⁷ *Филющенко Л. И.* Цифровой профиль работника: проблемы защиты персональных данных // *Законы России: опыт, анализ, практика.* 2024. № 11. С. 93—97.

⁸ *Щербакова О. В.* Цифровой профиль гражданина: межведомственное взаимодействие и перспективы расширения // *Российский юридический журнал.* 2025. № 4. С. 131—144.

офлайн-режиме происходит личное взаимодействие физического лица с сотрудниками, предоставляющими услуги, организациями.

В контексте работы с персональными данными важное значение имеет дача согласия физическим лицом на доступ к его данным, в том числе и к персональным. Сценарий цифрового профиля физического лица предусматривает четыре шага: запрос согласия, выдачу согласия, запрос данных из инфраструктуры, рассылку информации об изменениях данных в цифровом профиле (опциональный шаг). В документе детально описываются особенности реализации данных шагов.

В распоряжении Правительства РФ от 16.03.2024 № 637-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления» содержится план мероприятий по развитию Минцифры России с 2024 по 2030 г.

В целях повышения безопасности в России запланировано создание цифрового профиля для иностранного гражданина согласно Указу Президента РФ от 09.07.2025 № 467 «О государственном информационном ресурсе “Цифровой профиль иностранного гражданина”» (далее — Указ Президента РФ № 467). Цифровой профиль иностранного гражданина должен быть сформирован Министерством внутренних дел РФ до 30.06.2026. Планируется создание технологической инфраструктуры, которая будет аккумулировать информацию по вопросам миграционного учета иностранных граждан и лиц без гражданства; о целях въезда, проживания, пребывания на территории РФ; о привлечении к административной ответственности; о наличии у иностранного лица и лица без гражданства недвижимости, транспортного средства и т.д.

Указ Президента РФ № 467 утверждает широкий перечень сведений (из 25 пунктов) о том, какая информация должна быть включена в цифровой профиль. Цифровой профиль иностранного гражданина формируется на основе сведений, предоставленных МВД России, Минцифры России, ФСБ России, МИД России, Минсельхозом России, МЧС России, Росреестром, Социальным фондом России, ФНС России, Минпросвещения России, Минобрнауки России, Рособrnадзором, Роспотребнадзором, Банком России, Федеральным фондом обязательного медицинского страхования. Подробный перечень сведений и межведомственное взаимодействие позволит повысить уровень безопасности в стране.

Правовые проблемы, возникающие с использованием цифрового профиля

Можно отметить следующие правовые проблемы при использовании цифрового профиля:

1. *Правовая защита данных.* В правовое поле попадают персональные данные, но не попадают данные, которые не являются персональными, но могут быть с ними связаны. В качестве примера можно привести адреса пунктов выдачи на маркетплейсе, которыми пользуется лицо, или аналитику запросов лица при использовании маркетплейса.

Интересной представляется идея С. В. Соловкина о развитии неявных принципов правового регулирования сбора данных о человеке: «бремя определения



судьбы данных возложено на самих субъектов»⁹. Сложно не согласиться с ученым, поскольку цифровая среда накладывает на субъекта обязанность понимать, что его данные, в том числе и персональные данные, могут быть использованы в противоправных целях.

2. *Утечка данных.* В законодательстве есть нормы, регламентирующие ответственность лиц в связи с утечкой персональных данных, но в локальных актах компаний этот вопрос может быть не проработан детально, и в итоге привлечь к ответственности сотрудника будет невозможно. Ученые говорят о недостаточности регулирования цифрового профиля, в том числе и в рамках проведения экспериментального правового режима¹⁰.

3. *Излишек данных, включенных в цифровой профиль физического лица.* Данные могут меняться, есть ли смысл использовать вычислительные ресурсы (включая расходы на электроэнергию и износ оборудования) на данные, которые неактуальны? Предполагается, что нужно установить периодичность обновления цифрового профиля в целях работы с государственными и муниципальными органами.

4. *Этика использования цифрового профиля в целях повышения кибербезопасности и нивелирования утечки персональных данных.* Эффективность цифрового профиля в сфере оказания государственных услуг не вызывает сомнений, но вместе с тем доступ сотрудников к таким данным должен быть ограничен в рамках трудовых обязанностей сотрудника, а также конкретным вопросом, с которым обращается лицо. Предполагается, что для этого должно фиксироваться, по какому вопросу сотрудник организации обращался к цифровому профилю физического лица, иностранного гражданина, лица без гражданства, индивидуального предпринимателя и юридического лица. Формирование детализированных локальных актов для работы с цифровым профилем поможет избежать нарушений в сфере законодательства о персональных данных.

5. *Цифровой профиль и соответствие данных, которые в нем содержатся, актуальным документам.* Большой объем данных не исключает ошибок, внесение данных с ошибкой тоже возможно. Цифровой профиль может стать основой для цифрового паспорта и предъявления своего цифрового идентификатора в качестве удостоверяющего документа.

6. *Равенство действий в цифровом профиле действиям, которые лицо осуществляет в реальности.* Как и любая технология, цифровой профиль может быть подвергнут хакерской атаке и взлому. Поэтому возникает вопрос: юридически значимые действия, такие как подача заявления мошенниками, всегда ли должны приравниваться к действиям лица?

7. *Возможность обжалования и отмены решений.* Использование такой серьезной технологии, данных и документов, на основе которых могут быть приняты юридически значимые действия, должны быть оспоримыми в легкодоступной для лиц форме. Использование чат-ботов и упрощение работы специалистов для такой сферы является недопустимым.

⁹ Соловкин С. В. Автоматизированный сбор данных о человеке: неясные принципы правового регулирования // Вестник Университета имени О.Е. Кутафина (МГЮА). 2023. № 2. С. 90—100.

¹⁰ Филющенко Л. И. Указ. соч.

При исследовании цифрового профиля возникает вопрос: нужно ли использовать опыт Китая в отношении социальных кредитов — Программу-план создания системы социального кредита (2014—2020), принятую Государственным советом КНР 27.06.2014? Проект предусматривал рейтинг действий гражданина, на который могут влиять правонарушения и иные действия граждан. Сложно сказать, насколько этот опыт успешен, представляется, что ведение таких рейтингов имеет пользу для государства, для работодателей, но в то же время может нанести серьезный психологический вред личности.

Цифровизация неотвратимо меняет образ взаимодействия между лицами и государственными органами. Использование цифрового профиля позволяет не только ускорить взаимодействие, но и повысить его качество, поскольку данные защищаются не только благодаря правовой базе, но и средствами шифрования данных. Уровень развития регулирования отношений по использованию цифрового профиля в Российской Федерации является высоким. Апробация технологии показывает, что нужно уделить большее внимание вопросам равенства электронных документов бумажным, обновлению цифрового профиля, экономии и бережному использованию ресурсов.

БИБЛИОГРАФИЯ

1. Виноградова Е. В., Минбалеев А. В., Полякова Т. А. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации // Правоприменение. — 2021. — Т. 5. — № 4. — С. 5—19.
2. Соловкин С. В. Автоматизированный сбор данных о человеке: неявные принципы правового регулирования // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2023. — № 2. — С. 90—100.
3. Степанов О. А., Степанов М. М. О цифровой идентичности человека в виртуальном пространстве // Российская юстиция. — 2025. — № 10. — С. 30—35.
4. Филиппова С. Ю., Харитонова Ю. С., Щербак Н. В. Правовое регулирование электронной коммерции : учебное пособие. — М. : Юстицинформ, 2024. — 340 с.
5. Филющенко Л. И. Цифровой профиль работника: проблемы защиты персональных данных // Законы России: опыт, анализ, практика. — 2024. — № 11. — С. 93—97.
6. Цифровая трансформация и государственное управление: научно-практическое пособие. — М. : Инфотропик Медиа, 2022.
7. Щербакова О. В. Цифровой профиль гражданина: межведомственное взаимодействие и перспективы расширения // Российский юридический журнал. — 2025. — № 4. — С. 131—144.





**Петр Анатольевич
ЛЕСНИКОВ,**

основатель и управляющий
партнер
юридической фирмы
«Лесников, Ильичев
и Партнеры»,
кандидат юридических наук
lesnikovpro@gmail.com
454100, Россия,
г. Челябинск,
просп. Ленина, д. 55

Административно-правовые аспекты обеспечения кибербезопасности в цифровой таможенной инфраструктуре

Аннотация. Статья посвящена исследованию административно-правовых аспектов обеспечения кибербезопасности в цифровой таможенной инфраструктуре Российской Федерации. Анализируются: правовая природа таможенной информационной инфраструктуры как объекта критической информационной инфраструктуры; система субъектов административно-правового регулирования кибербезопасности в таможенной сфере и разграничение их компетенций; режим защиты сведений, обрабатываемых в ЕАИС ТО.

Выявляются структурные пробелы в регулировании: отсутствие специального правового режима кибербезопасности таможенных данных, неурегулированность ответственности за кибератаки на таможенную инфраструктуру, пробелы в правовом регулировании трансграничного информационного обмена в условиях кибератак. Предлагается концепция таможенного киберсуверенитета как административно-правовой категории.

Ключевые слова: кибербезопасность, информационное право, цифровая таможенная инфраструктура, критическая информационная инфраструктура, ЕАИС ТО, ФТС России, таможенные данные, административно-правовое регулирование, киберсуверенитет, информационная безопасность, ФСТЭК России

DOI: 10.17803/2311-5998.2026.142.6.136-143

Petr A. LESNIKOV,

founder and managing partner of the law firm
“Lesnikov, Ilyichev and Partners” (Chelyabinsk),
Cand. Sci. (Law)

lesnikovpro@gmail.com

55, prosp. Lenina, Chelyabinsk, Russia, 454100

Administrative and Legal Aspects of Cybersecurity in Digital Customs Infrastructure

Abstract. The article is devoted to the study of administrative and legal aspects of ensuring cybersecurity in the digital customs infrastructure of the Russian Federation. The following are analyzed: the legal nature of the customs information infrastructure as an object of critical information infrastructure (CII); the system of subjects of administrative and legal regulation of cybersecurity in the customs sphere and the delineation of their competencies; the regime of protection of information processed in the EAI TO.

Structural gaps in regulation are identified: the absence of a special legal regime for cybersecurity of customs data, the lack of regulation of liability for cyberattacks on the customs infrastructure, and gaps in the legal regulation of cross-border information exchange in the context of cyberattacks. The concept of “customs cyber sovereignty” as an administrative and legal category is proposed.

Keywords: cybersecurity, information law, digital customs infrastructure, critical information infrastructure, EAIS TO, FCS of Russia, customs data, administrative and legal regulation, cyber sovereignty, information security, FSTEC of Russia

Цифровая трансформация таможенного администрирования, обеспечившая значительный прирост эффективности таможенных процедур, одновременно породила принципиально новые риски в сфере информационной безопасности. Единая автоматизированная информационная система таможенных органов¹ (ЕАИС ТО), обрабатывающая ежегодно свыше 5 млн деклараций на товары, содержит массивы данных, представляющих исключительную ценность — коммерческую, разведывательную и стратегическую. Компрометация данных ЕАИС ТО способна не только причинить ущерб конкретным участникам внешнеэкономической деятельности, но и нанести серьезный вред государственным интересам в сфере обеспечения экономической безопасности.

Мировая практика фиксирует устойчивую тенденцию к росту числа кибератак на таможенные и иные пограничные информационные системы. В 2021 г. масштабной кибератаке подвергся Южноафриканский порт Дурбан и сопряженные таможенные системы²; в 2023 г. фиксировались попытки несанкционированного доступа к системам таможенного оформления ряда государств ЕАЭС. Российская таможенная инфраструктура, включенная в глобальные цепочки обмена данными с иностранными таможенными администрациями, объективно подвержена аналогичным угрозам.

Вместе с тем административно-правовое регулирование кибербезопасности применительно к таможенной инфраструктуре остается фрагментарным. Российское законодательство в сфере информационной безопасности формировалось преимущественно применительно к общим категориям государственных информационных систем и объектов критической информационной инфраструктуры, не учитывая специфику таможенной сферы — ее трансграничного характера, высокой степени интеграции с информационными системами ЕАЭС и иностранных государств, а также тройственного правового режима обрабатываемых данных (коммерческая тайна, государственная тайна, персональные данные одновременно).

¹ Приказ ФТС России от 17.06.2010 № 1154 (ред. от 28.07.2017) «Об утверждении Положения о Единой автоматизированной информационной системе таможенных органов» // URL: <https://www.alta.ru/tamdoc/10pr1154/> (дата обращения: 09.05.2026).

² Case Study 17: Port of Durban, South Africa // URL: <https://resilientmaritimelogistics.unctad.org/guidebook/case-study-17-port-durban-south-africa> (дата обращения: 09.05.2026).



Цель настоящей статьи — исследовать административно-правовые механизмы обеспечения кибербезопасности в цифровой таможенной инфраструктуре, выявить пробелы действующего регулирования и предложить концептуальную модель таможенного киберсуверенитета как инструмента их устранения.

Правовое основание для квалификации цифровой таможенной инфраструктуры в качестве объекта критической информационной инфраструктуры создает Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»³. Согласно ст. 2 данного Закона к критической информационной инфраструктуре относятся объекты, функционирование которых критически важно для обороны страны, государственного управления, финансовой системы, топливно-энергетического комплекса, транспортной системы и иных стратегических отраслей.

Таможенные органы включены в перечень субъектов критической информационной инфраструктуры (КИИ) косвенно — через категорию государственных органов, осуществляющих функции в сфере государственного управления и обеспечения экономической безопасности. Постановление Правительства РФ от 08.02.2018 № 127⁴, утвердившее правила категорирования объектов КИИ, распространяется на ФТС России в части ЕАИС ТО. Вместе с тем специальных актов, определяющих порядок категорирования объектов КИИ применительно к таможенной информационной инфраструктуре, не принято.

Анализ структуры ЕАИС ТО позволяет выделить несколько категорий объектов, подлежащих отнесению к КИИ. Первая — системы обработки таможенных деклараций: нарушение их работоспособности влечет прекращение таможенного оформления на всей территории страны, что является угрозой экономической безопасности государства. Вторая — системы управления рисками: несанкционированный доступ к ним позволяет манипулировать результатами таможенного контроля в интересах недобросовестных участников ВЭД или иностранных разведок. Третья — системы межведомственного электронного взаимодействия: их компрометация создает угрозу утечки персональных данных и сведений о товарных потоках стратегического значения.

Вместе с тем действующее категорирование объектов КИИ применительно к таможенной инфраструктуре не в полной мере соответствует реальному уровню угроз. ЕАИС ТО в части обработки деклараций отнесена к третьей (наименее высокой) категории значимости объектов КИИ, тогда как реальные последствия нарушения ее работоспособности — полная остановка таможенного оформления — объективно соответствуют критериям первой категории. Данное несоответствие влечет занижение требований к защищенности системы.

³ Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 07.04.2025) «О безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ. 2017. № 31 (ч. I). Ст. 4736 ; 2025. № 15. Ст. 1784.

⁴ Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 07.11.2025) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // СЗ РФ. 2018. № 8. Ст. 1204 ; 2025. № 45. Ст. 6775.

Принципиальной особенностью таможенной информационной инфраструктуры, отличающей ее от иных объектов КИИ, является ее трансграничный характер. ЕАИС ТО интегрирована с информационными системами таможенных органов государств — членов ЕАЭС в рамках Интегрированной информационной системы внешней и взаимной торговли⁵ (ИИСВВТ), а также осуществляет информационный обмен с таможенными администрациями иностранных государств в рамках двусторонних соглашений о взаимном признании. Данная интеграция создает дополнительные векторы кибератак, которые законодательство о КИИ в части трансграничного измерения практически не регулирует.

Административно-правовое регулирование кибербезопасности применительно к таможенной инфраструктуре осуществляется множеством субъектов, компетенция которых не разграничена в достаточной мере. Данное «компетенционное рассеивание» является одной из ключевых системных проблем в рассматриваемой сфере.

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является регулятором в сфере защиты информации, не составляющей государственную тайну, и ключевым органом в части обеспечения безопасности КИИ. Применительно к таможенной инфраструктуре ФСТЭК России осуществляет: методологическое руководство категорированием объектов КИИ; утверждение требований по безопасности значимых объектов КИИ; государственный контроль в области обеспечения безопасности значимых объектов КИИ⁶. Вместе с тем ФСТЭК России не располагает отраслевой экспертизой применительно к специфике таможенных информационных систем и не участвует в разработке технических регламентов ЕАИС ТО.

Федеральная служба безопасности РФ осуществляет координацию деятельности по обеспечению безопасности КИИ (ст. 6 Федерального закона № 187-ФЗ), эксплуатирует Национальный координационный центр по компьютерным инцидентам (НКЦКИ) и осуществляет разведывательную деятельность применительно к иностранным киберугрозам. Применительно к таможенной инфраструктуре ФСБ России, помимо общей координирующей роли, осуществляет защиту сведений, составляющих государственную тайну (в части таможенной разведки, профилей рисков СУР, оперативной информации).

Министерство цифрового развития, связи и массовых коммуникаций РФ устанавливает требования к государственным информационным системам (ГИС) применительно к их архитектуре, использованию отечественного программного обеспечения и размещению данных на территории Российской Федерации. Данные требования распространяются на ЕАИС ТО в части, не регулируемой специальными нормами таможенного законодательства. Конфликт компетенций между

⁵ Решение Коллегии ЕЭК от 27.01.2015 № 5 «Об утверждении Правил электронного обмена данными в интегрированной информационной системе внешней и взаимной торговли» // URL: <https://www.alt.ru/tamdoc/15kr0005/> (дата обращения: 09.05.2026).

⁶ Постановление Правительства РФ от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // СЗ РФ. 2018. № 9. Ст. 1393.



Минцифры и ФТС России периодически возникает применительно к требованиям об использовании российского программного обеспечения: ряд компонентов ЕАИС ТО исторически разработан на основе иностранных платформ.

Сама ФТС России обладает компетенцией в сфере кибербезопасности таможенной инфраструктуры в качестве ее оператора. Соответствующие функции осуществляются Главным управлением информационных технологий (ГУИТ) ФТС России совместно с Центральным информационно-техническим таможенным управлением (ЦИТТУ), являющимся правопреемником ГНИВЦ ФТС России — подведомственным учреждением, выступающим технологическим оператором ЕАИС ТО. Разграничение ответственности между ФТС России как субъектом КИИ и ЦИТТУ как техническим оператором в нормативных актах прямо не определено.

Описанная конфигурация субъектов регулирования характеризуется дублированием полномочий в одних аспектах (защита ГИС от несанкционированного доступа находится в сфере компетенции и ФСТЭК России, и ФСБ России, и Минцифры одновременно) при наличии значимых белых пятен в других (трансграничная кибербезопасность таможенных систем, защита данных в рамках интеграционных систем ЕАЭС).

Данные, обрабатываемые в ЕАИС ТО, характеризуются исключительной правовой сложностью с точки зрения режима их охраны. Они не являются однородной категорией — в составе таможенных данных одновременно присутствуют сведения, подпадающие под различные правовые режимы ограниченного доступа.

Первая категория — государственная тайна. К ней относятся сведения о профилях рисков СУР, содержащие методологию таможенной «разведки»; данные оперативных таможенных расследований; сведения, составляющие военную тайну, в части деклараций на товары военного и двойного назначения. Правовой режим данной категории определяется Законом РФ от 21.07.1993 № 5485-1 «О государственной тайне»⁷ и является наиболее строгим.

Вторая категория — коммерческая тайна. Сведения, содержащиеся в таможенных декларациях (наименование товаров, их количество, стоимость, сведения о контрагентах), могут составлять коммерческую тайну декларантов. Режим защиты данной категории определяется Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне»⁸. Утечка данных сведений вследствие кибератаки нарушает права декларантов и может влечь гражданско-правовую ответственность оператора системы.

Третья категория — персональные данные. Декларации на товары содержат персональные данные физических лиц — грузополучателей, перевозчиков, представителей декларантов. Правовой режим защиты данной категории определяется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных

⁷ Закон РФ от 21.07.1993 № 5485-1 (ред. от 08.08.2024) «О государственной тайне» // СЗ РФ. 1997. № 41. Ст. 8220—8235 ; 2024. № 33 (ч. I). Ст. 4945.

⁸ Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 08.08.2024) «О коммерческой тайне» // СЗ РФ. 2004. № 32. Ст. 3283 ; 2024. № 33 (ч. I). Ст. 4947.

данных»⁹ и требованиями ФСТЭК России¹⁰ по защите информационных систем, персональных данных.

Четвертая категория — открытые данные. Часть таможенной статистики подлежит обязательному публичному раскрытию. Вместе с тем грань между агрегированными данными, подлежащими публикации, и деперсонализированными данными, из которых при соответствующей обработке могут быть выделены персональные или коммерчески чувствительные сведения, нормативно не определена, что создает риск деанонимизации через открытые данные.

Сосуществование нескольких правовых режимов в рамках единой информационной системы создает принципиальную проблему: требования по защите, установленные для каждого режима в отдельности, разработаны применительно к «чистым» случаям, тогда как ЕАИС ТО объединяет в одной архитектуре данные всех перечисленных категорий. Это требует либо применения к системе в целом наиболее строгого из применимых режимов (что избыточно для части данных), либо технологического разделения данных по категориям (что технически сложно и нормативно не предусмотрено).

Трансграничный характер таможенной деятельности предопределяет необходимость интеграции ЕАИС ТО с информационными системами иностранных государств и международных организаций. Данная интеграция осуществляется по нескольким каналам:

- в рамках ЕАЭС — через ИИСВВТ, оператором которой является ЕЭК;
- в рамках двусторонних соглашений ФТС России с иностранными таможенными администрациями о взаимном признании и обмене предварительной информацией;
- в рамках международных программ (программа ВТамО SafeCargo, программы ВТО по упрощению процедур торговли).

Трансграничная интеграция создает уникальный класс киберугроз — угрозы, реализуемые через внешние информационные каналы. Компрометация информационной системы государства — партнера по обмену данными может создать вектор атаки на ЕАИС ТО через защищенные каналы межведомственного взаимодействия. Данный вектор принципиально отличается от традиционных внешних атак тем, что атакующий использует легитимные технические средства доступа.

Правовое регулирование трансграничной кибербезопасности таможенной инфраструктуры находится в зачаточном состоянии. Соглашения ФТС России с иностранными таможенными администрациями об обмене предварительной информацией, как правило, содержат общие положения о защите передаваемых данных, однако не устанавливают конкретных технических требований к кибербезопасности и не предусматривают механизмов ответственности за нарушение данных требований.

⁹ Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) «О персональных данных» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3451 ; 2025. № 26 (ч. I). Ст. 3486.

¹⁰ Приказ ФСТЭК России от 11.04.2025 № 117 // URL: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-utverzhdeny-prikazom-fstek-rossii-ot-11-aprelya-2025-g-n-117> (дата обращения: 09.05.2026).



На уровне ЕАЭС ситуация несколько лучше¹¹. При этом к минусам относятся рекомендательный характер таких соглашений, а также тот факт, что они не охватывают специфику киберугроз применительно к таможенным данным.

Особую проблему представляет правовой режим данных ЕАИС ТО в ситуации кибератаки, осуществленной с территории иностранного государства. Российское законодательство о КИИ не содержит норм, регулирующих порядок ответных мер при установлении государственной принадлежности кибератаки, что является принципиальным пробелом с учетом тенденции к государственно спонсируемым кибератакам на инфраструктуру критически важных объектов.

Система административно-правовых санкций за нарушения в сфере кибербезопасности, применимых к таможенной инфраструктуре, характеризуется принципиальной неполнотой. КоАП РФ содержит ряд составов, потенциально применимых в данном контексте, однако они не формируют целостного механизма ответственности.

Статья 13.12 КоАП РФ предусматривает ответственность за нарушение правил защиты информации (штраф для юридических лиц от 15 000 до 25 000 рублей). Данный состав применим в случае нарушения оператором ЕАИС ТО требований ФСТЭК России по защите информации. Вместе с тем санкции данной статьи несопоставимо малы по отношению к масштабу возможного ущерба от нарушений в сфере таможенной кибербезопасности.

Статья 13.11 КоАП РФ устанавливает ответственность за нарушение законодательства о персональных данных. Применительно к ЕАИС ТО данный состав актуален в случае утечки персональных данных участников ВЭД вследствие кибератаки или ненадлежащей защиты системы. Однако специфика оператора ГИС (каковым является ФТС России) предполагает исключение из ряда обязанностей, установленных для операторов персональных данных в частном секторе.

Уголовно-правовая защита таможенной инфраструктуры обеспечивается гл. 28 УК РФ «Преступления в сфере компьютерной информации» (ст. 272—274.1). В части, специально посвященной объектам КИИ, ст. 274.1 УК РФ предусматривает ответственность за неправомерное воздействие на критическую информационную инфраструктуру. Применительно к таможенным системам данный состав является наиболее релевантным, однако его использование осложняется проблемой установления и доказывания государственной принадлежности кибератак.

Принципиальным пробелом является отсутствие механизма ответственности ФТС России как оператора ЕАИС ТО за ненадлежащее обеспечение кибербезопасности, повлекшее утечку данных или нарушение работоспособности системы. В данном случае участник ВЭД, пострадавший от утечки коммерческих данных вследствие кибератаки, реализовавшейся через недостаточно защищенную ЕАИС ТО, лишен эффективного правового средства защиты: иск к государству по ст. 1069 ГК РФ требует доказывания конкретного противоправного деяния должностного лица, тогда как системные недостатки защиты под данную конструкцию не подпадают.

Совокупность выявленных проблем обуславливает необходимость формирования специальной административно-правовой концепции, объединяющей

¹¹ Рекомендации Коллегии Евразийской экономической комиссии от 12.03.2019 № 9 «О перечне стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза» // URL: <https://www.garant.ru/products/ipo/prime/doc/72097708/> (дата обращения: 09.05.2026).

разрозненные требования к кибербезопасности таможенной инфраструктуры в системную правовую конструкцию. Автор предлагает концепцию таможенного киберсуверенитета как совокупности правовых механизмов, обеспечивающих суверенный контроль государства над цифровой таможенной инфраструктурой и обрабатываемыми в ней данными.

Таможенный киберсуверенитет как административно-правовая категория включает четыре компонента:

- 1) технологический суверенитет — обязательное использование при функционировании ЕАИС ТО сертифицированного российского программного обеспечения, отечественных средств криптографической защиты информации и размещение данных исключительно на серверах, физически находящихся на территории Российской Федерации. Данный компонент частично реализован через требования Минцифры России о переходе ГИС на российское ПО, однако применительно к ЕАИС ТО его реализация нормативно не закреплена;
- 2) информационный суверенитет — установление правовых ограничений на передачу данных ЕАИС ТО иностранным государствам и международным организациям, включая исчерпывающий перечень передаваемых категорий данных, порядок и условия их передачи, механизм приостановления обмена данными при возникновении угрозы кибератаки через каналы межведомственного взаимодействия;
- 3) операционный суверенитет — обязательная локализация всех процессов технической эксплуатации и обновления ЕАИС ТО на территории Российской Федерации, исключение привлечения иностранных специалистов или компаний к работам, дающим доступ к данным ЕАИС ТО, без специального разрешения ФСБ России. Данный компонент актуализирован с учетом практики санкционного давления, при котором иностранные поставщики ПО прекращали техническую поддержку государственных систем;
- 4) юрисдикционный суверенитет — установление исключительной юрисдикции российских органов власти над инцидентами в сфере кибербезопасности ЕАИС ТО, включая право ФСБ России проводить расследование кибератак без согласования с иностранными органами, даже если атака осуществлена с территории иностранного государства, с которым действует соглашение о правовой помощи по киберделам.

Концепция таможенного киберсуверенитета не означает изоляции таможенной инфраструктуры от международных систем обмена данными — она предполагает создание четких правовых рамок для такого обмена, обеспечивающих государственный контроль над его условиями и возможность оперативного ограничения в случае возникновения угроз.

Аналогичные концепции реализуются в ряде государств: Китай имплементировал систему контроля трансграничных потоков данных применительно к государственным инфраструктурным системам; ЕС разрабатывает концепцию цифрового суверенитета (Digital Sovereignty¹²) применительно к данным критической инфраструктуры.

¹² Digital sovereignty for Europe // URL: [https://www.europarl.europa.eu/thinktank/en/document/eprs_bri\(2020\)651992](https://www.europarl.europa.eu/thinktank/en/document/eprs_bri(2020)651992) (дата обращения: 09.05.2026).

Образование и права человека в условиях цифровизации общества



**Руслан Абдусаламович
АБДУСАЛАМОВ,**

заведующий кафедрой
информационного
права и информатики
Дагестанского
государственного
университета,

кандидат педагогических
наук, доцент

abd-rus@yandex.ru

367000, Россия, Республика
Дагестан, г. Махачкала,
ул. Магомета Гаджиева,
д. 43А

Публично-правовое обеспечение цифровой трансформации высшего образования в Российской Федерации

Аннотация. В статье исследуется цифровая трансформация высшего образования как особый правовой феномен в контексте национальных целей развития Российской Федерации и проекта «Экономика данных и цифровая трансформация государства». На основе доктринальных подходов информационного права автором разграничены понятия «цифровизация» и «цифровая трансформация» применительно к сфере высшего образования. Проанализированы публично-правовые механизмы, реализуемые федеральными органами власти и субъектами РФ. Раскрыто влияние цифровой трансформации на образовательные правоотношения, правовой статус вузов, обучающихся и научно-педагогических работников, а также на режим ИТ-активов и оценку цифровой зрелости. Выявлены проблемы фрагментированности правового регулирования, отсутствия единого режима электронной информационно-образовательной среды, использования искусственного интеллекта, обеспечения технологического суверенитета и региональной асимметрии. Определены перспективные направления совершенствования законодательства, включая систематизацию информационного законодательства, экспериментальные правовые режимы и цифровые платформы в образовании.

Ключевые слова: электронная информационно-образовательная среда, искусственный интеллект в образовании, цифровая зрелость, ИТ-активы, экспериментальный правовой режим, цифровые платформы, региональная асимметрия

DOI: 10.17803/2311-5998.2026.142.6.144-152

Ruslan A. ABDUSALAMOV,

Head of the Department of information law and informatics,

Dagestan State University Law Institute,

Cand. Sci. (Pedagogical), Associate professor

abd-rus@yandex.ru

43A, ul. Magomet Gadzhiev, Makhachkala, Republic of Dagestan, Russia, 367000

Public Legal Support for the Digital Transformation of Higher Education in the Russian Federation

Abstract. *The article examines the digital transformation of higher education as a special legal phenomenon in the context of the national development goals of the Russian Federation and the project “Data Economics and Digital Transformation of the State”. Based on the doctrinal approaches of information law, the author distinguishes the concepts of “digitalization” and “digital transformation” in relation to higher education. The article analyzes the public legal mechanisms implemented by federal authorities and subjects of the Russian Federation, including the regions of the North Caucasus Federal District. The impact of digital transformation on educational legal relations, the legal status of universities, students and research and teaching staff, as well as on the regime of IT assets and the assessment of digital maturity is revealed. The problems of fragmented legal regulation, the lack of a unified regime of the electronic information and educational environment, the use of artificial intelligence, ensuring technological sovereignty and regional asymmetry are revealed. Promising areas for improving legislation have been identified, including the systematization of information legislation, experimental legal regimes and digital platforms in education.*

Keywords: *electronic information and educational environment, artificial intelligence in education, digital maturity, IT assets, experimental legal regime, digital platforms, regional asymmetry*

Актуальность проблемы

Закрепление цифровой трансформации государственного и муниципального управления, экономики и социальной сферы в качестве одной из национальных целей развития Российской Федерации на период до 2030 года и на перспективу до 2036 года предопределяет стратегическое значение публично-правового обеспечения процессов внедрения цифровых технологий в социально значимых сферах.

Образовательные организации высшего образования являются непосредственными объектами трансформационных процессов, реализуемых в рамках национального проекта «Экономика данных и цифровая трансформация государства». Именно вузы выступают системообразующим звеном кадрового, научного и технологического обеспечения цифровой трансформации страны в целом.



Вместе с тем действующее законодательство пока не образует целостной публично-правовой модели обеспечения цифровой трансформации высшего образования. Отдельные положения Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», подзаконных актов Министерства науки и высшего образования РФ формируют фрагментированный регуляторный массив, который в условиях стремительного развития цифровой среды не в полной мере отвечает потребностям системного нормативного правового регулирования.

Цифровая трансформация высшего образования как особый правовой феномен

Доктринальный анализ цифровой трансформации высшего образования предполагает обращение к категориальному аппарату, сформированному в рамках современной школы информационного права. Опираясь на методологические подходы Т. А. Поляковой, А. В. Минбалева и Н. В. Кротковой¹, цифровизацию следует трактовать как процесс перехода на цифровые технологии, охватывающий все сферы жизнедеятельности общества, в результате которого появляется возможность использования новейших технологий для наиболее эффективной реализации тех или иных функций. Цифровая трансформация представляет собой более сложный феномен, охватывающий широкий спектр изменений, связанных с применением цифровых технологий, и ориентированный на комплексное стратегическое преобразование процессов с целью адаптации к изменяющимся условиям, использования цифровых возможностей для создания новых ценностей и достижения конкурентного преимущества.

Цифровая трансформация высшего образования представляет собой комплексное стратегическое преобразование образовательной организации высшего образования и системы высшего образования в целом, направленное на достижение стратегических целей развития государства, отвечающее критериям социально-экономической эффективности и реализуемое на основе системы инициатив по приоритетному внедрению отечественных цифровых технологий, обороту цифровых данных об обучении, развитию кадров, компетенций и культуры для цифровой трансформации, обеспечению национальной информационной безопасности и технологического суверенитета.

Цифровая трансформация высшего образования реализуется одновременно в нескольких взаимосвязанных плоскостях:

- в сфере образовательных правоотношений (изменение содержания, форм и способов реализации образовательных программ);
- организации деятельности субъектов высшего образования (преобразование правового статуса образовательных организаций, обучающихся, научно-педагогических работников);

¹ Полякова Т. А., Минбалева А. В., Кроткова Н. В. Цифровая трансформация как правовой феномен и ее влияние на развитие информационного права и законодательства // Государство и право. 2025. № 11. С. 207—209.

- объектов правового регулирования (формирование специальных правовых режимов в отношении электронной информационно-образовательной среды, ИТ-активов, цифровых данных об обучении);
- публично-правового обеспечения (создание системы публичного управления процессами цифровой трансформации).

Также она характеризуется комплексным межотраслевым характером, требующим согласованного применения норм информационного, образовательного, административного, гражданского права, и обладает стратегическим характером, обусловленным детерминированностью процессов цифровой трансформации актами стратегического планирования.

Публично-правовые механизмы обеспечения цифровой трансформации высшего образования

Публично-правовое обеспечение цифровой трансформации высшего образования формируется посредством реализации полномочий целостной системы органов государственной власти, обладающих различной предметной компетенцией. Системообразующее значение имеет Министерство науки и высшего образования РФ, которое разрабатывает стратегические документы цифровой трансформации высшего образования, методические рекомендации по созданию и развитию электронной информационно-образовательной среды (ЭИОС), требования к информационным системам и цифровым сервисам, используемым в образовательном процессе, формирует ведомственную программу цифровой трансформации.

Особую координирующую роль выполняет Министерство цифрового развития, связи и массовых коммуникаций РФ, обеспечивающее реализацию национального проекта «Экономика данных и цифровая трансформация государства». Совместно с автономной некоммерческой организацией «Цифровая экономика» и Роскачеством Минцифры РФ разрабатывает методические основы оценки цифровой зрелости организаций, в том числе образовательных, что создает нормативно-техническую базу для измерения результативности цифровой трансформации.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций реализует контрольно-надзорные полномочия в области защиты персональных данных обучающихся и научно-педагогических работников, контроля за обработкой данных в ЭИОС, исполнения требований законодательства об ограничении доступа к информации, распространение которой запрещено или ограничено. Эти полномочия приобретают принципиальное значение в условиях значительного увеличения объемов обработки цифровых данных об обучении и формирования цифровых профилей участников образовательных отношений², применения биометрических технологий идентификации в образовательном процессе.

² См.: Виноградова Е. В., Полякова Т. А., Минбалева А. В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации // Правоприменение. 2021. Т. 5. № 4. С. 5—19.

Региональный уровень реализации национального проекта «Экономика данных и цифровая трансформация государства» предполагает разработку региональных проектов цифровой трансформации, в том числе в сфере образования. На уровне субъекта РФ формируются собственные подходы к организации взаимодействия региональных органов исполнительной власти с образовательными организациями высшего образования, к развитию региональных цифровых платформ в сфере образования, к интеграции образовательных информационных систем с государственными информационными системами регионального уровня.

Для СКФО характерно сочетание разветвленной сети образовательных организаций высшего образования с сохраняющейся асимметрией состояния цифровой инфраструктуры по сравнению с центральными регионами страны, а также с особой ролью высшего образования как инструмента формирования единого культурно-образовательного пространства и обеспечения территориальной целостности государства. В Республике Дагестан реализуется значительный объем образовательных программ высшего образования; важную роль в региональной системе подготовки кадров играет Дагестанский государственный университет, выступающий методологическим и инфраструктурным центром цифровой трансформации высшего образования в регионе и обеспечивающий разработку и апробацию управленческих решений в области ЭИОС, информационной безопасности и оборота цифровых данных об обучении.

Влияние цифровой трансформации на образовательные правоотношения и правовой статус их субъектов

Вуз становится не только организатором образовательного процесса в традиционном понимании, но и оператором цифровых платформ, оператором персональных данных значительного количества субъектов, владельцем (правообладателем) ИТ-активов, субъектом учета цифровой зрелости.

Категория «ИТ-активы», получившая нормативное закрепление в постановлении Правительства РФ от 01.07.2024 № 900³, имеет особое значение для сферы высшего образования. К ИТ-активам вуза следует относить информационные системы (включая ЭИОС, системы электронного документооборота, информационные системы обеспечения научно-исследовательской деятельности, библиотечные информационные системы), компоненты информационно-телекоммуникационной инфраструктуры, программно-технические комплексы, базы данных научных и образовательных ресурсов, программное обеспечение учебного назначения. Учет и управление ИТ-активами вуза приобретает не только организационно-управленческое, но и публично-правовое значение, поскольку эти активы рассматриваются в качестве ресурсной основы цифровой трансформации образовательной организации и непосредственно влияют на показатели ее цифровой зрелости.

³ Постановление Правительства РФ от 01.07.2024 № 900 «О порядке учета ИТ-активов, используемых для осуществления деятельности по цифровой трансформации системы государственного (муниципального) управления» // СЗ РФ. 2024. № 28. Ст. 4028.

Правовое положение обучающихся в цифровой среде высшего образования характеризуется расширением каталога субъективных прав, реализуемых исключительно или преимущественно в цифровом формате: право на доступ к ЭИОС, право на использование электронных образовательных ресурсов, право на формирование индивидуальной образовательной траектории на основе цифровых данных об обучении, право на цифровую идентичность участника образовательных отношений. Одновременно у обучающихся возникают новые обязанности, связанные с соблюдением правил использования цифровой среды, обеспечением информационной безопасности на пользовательском уровне, добросовестным использованием цифровых инструментов при подготовке учебных заданий и выполнении научно-исследовательских работ.

Особое значение приобретает обеспечение прав обучающихся в условиях применения технологий искусственного интеллекта в образовательном процессе и при оценивании результатов обучения. Возникают принципиальные правовые вопросы: о правовых последствиях использования генеративных моделей искусственного интеллекта при выполнении учебных заданий, о пределах применения автоматизированной оценки знаний, о праве обучающегося на «человеческое решение» в значимых для него образовательных ситуациях. Концептуальные подходы к решению этих вопросов могут быть выработаны на основе модели «человек — слабая сторона», предложенной В. Б. Наумовым в контексте безоголосного внедрения цифровых технологий и обоснованной им на Восьмых Бачиловских чтениях⁴. Указанная модель предполагает признание необходимости специальной правовой защиты человека в его взаимоотношениях с системами искусственного интеллекта и иными цифровыми технологиями, что в сфере высшего образования имеет особое значение в силу естественно сложившейся асимметрии информационных и организационных возможностей образовательной организации и обучающегося.

Расширяется круг профессиональных обязанностей, связанных с разработкой электронных образовательных ресурсов, ведением электронного документооборота, использованием цифровых инструментов оценивания. Возникают сложные вопросы охраны авторских прав на материалы, размещаемые в ЭИОС, защиты прав преподавателя при использовании его лекций и иных результатов интеллектуальной деятельности в обучении нейронных сетей, обеспечения цифровой приватности педагогического работника.

Цифровая зрелость образовательной организации высшего образования — категория, восходящая к работам Т. А. Поляковой и А. В. Минбалева⁵, — представляет собой интегральную правовую характеристику, отражающую степень готовности вуза к реализации задач цифровой трансформации. Данная характеристика включает не только технические показатели (наличие и качество цифровой инфраструктуры), но и организационно-правовые (сформированность нормативной базы внутренних актов, наличие политик информационной безопасности,

⁴ Наумов В. Б. Право и «Батлерианский джихад»: размышления об угрозах использования искусственного интеллекта // Информационное общество. 2025. № 2. С. 131—147.

⁵ См.: Полякова Т. А., Минбалева А. В. Понятие и правовая природа «цифровой зрелости» // Государство и право. 2021. № 9. С. 107—116.

эффективность механизмов защиты персональных данных, уровень цифровых компетенций кадрового состава). Закрепление цифровой зрелости в качестве показателя эффективности деятельности образовательной организации позволяет интегрировать соответствующие требования в систему государственного контроля и надзора в сфере высшего образования.

Проблемы и перспективы публично-правового регулирования цифровой трансформации высшего образования

Анализ современного состояния правового регулирования позволяет выделить ряд существенных проблем, препятствующих эффективному публично-правовому обеспечению цифровой трансформации высшего образования:

1. Фрагментированность правового регулирования, выражающаяся в распределении соответствующих норм между различными отраслями законодательства (образовательное, информационное, о персональных данных, об интеллектуальных правах, об экспериментальных правовых режимах) при отсутствии единого концептуального подхода. Решение этой проблемы видится в рамках реализации идеи систематизации информационного законодательства, обоснованной в работах Т. А. Поляковой, А. В. Минбалева и В. Б. Наумова⁶, в том числе путем включения в перспективный Информационный кодекс РФ специальных норм, посвященных публично-правовому режиму использования информационных технологий в социально значимых сферах, к числу которых относится высшее образование.

2. Отсутствие единого правового режима ЭИОС. Действующее законодательство закрепляет требование о наличии электронной информационно-образовательной среды в каждой образовательной организации (ч. 3 ст. 16 Федерального закона «Об образовании в Российской Федерации»), однако нормативное содержание данной категории остается фрагментарным. Не определены юридическая природа ЭИОС, правовой режим ее отдельных компонентов, объем прав и обязанностей пользователей, требования к ее взаимодействию с государственными информационными системами в сфере образования. Решение данной проблемы предполагает разработку специального федерального нормативного правового акта, закрепляющего публично-правовые основы создания, функционирования и развития ЭИОС.

3. Необходимость формирования правовых режимов использования технологий искусственного интеллекта в высшем образовании. Применение генеративных, агентских и иных видов искусственного интеллекта в обучении создает принципиально новые правовые ситуации, связанные с авторством создаваемых при их участии произведений, с ответственностью за результаты автоматизированного оценивания, с защитой данных обучающихся, используемых для обучения моделей. Перспективным направлением представляется использование

⁶ Полякова Т. А., Минбалева А. В., Наумов В. Б. К вопросу о кодификации информационного законодательства в условиях цифровой трансформации // Государство и право. 2024. № 1. С. 81—91.

механизма экспериментальных правовых режимов для апробации правовых конструкций, регулирующих применение искусственного интеллекта в образовательном процессе, и последующего совершенствования законодательства на основе полученных результатов.

4. Обеспечение технологического суверенитета и информационной безопасности в сфере высшего образования. В условиях геополитических вызовов и санкционного давления особое значение приобретают использование отечественных цифровых решений в образовательном процессе, защита критически важных для системы высшего образования информационных систем, противодействие информационно-психологическим угрозам в отношении обучающихся.

5. Проблемы, связанные с правовым режимом цифровых платформ в высшем образовании. Активное развитие цифровых образовательных платформ требует выработки четкой нормативной модели их функционирования. Как обоснованно отмечает А. В. Минбалева, цифровая платформа представляет собой сложный информационный объект и сложную социотехническую систему, что обуславливает многоуровневый характер ее правового регулирования⁷. В образовательной сфере данная проблематика требует специального регулирования, учитывающего особенности образовательных правоотношений и публичный интерес в сохранении единства образовательного пространства.

6. Необходимость правового регулирования оборота цифровых данных об обучении. В рамках цифровой трансформации формируются значительные массивы данных, отражающие траекторию обучения каждого обучающегося, его учебные достижения, поведенческие характеристики в цифровой среде. Эти данные имеют как индивидуальное (для участника образовательных отношений), так и системное (для развития системы образования) значение, что предопределяет необходимость их специального правового режима с учетом баланса публичного и частного интересов⁸.

Выводы и предложения

Цифровая трансформация высшего образования представляет собой особый правовой феномен, который обладает специфическими характеристиками: системообразующим значением высшего образования для подготовки кадров цифровой экономики и обеспечения технологического суверенитета; сложной структурой образовательных правоотношений, преобразуемых под воздействием цифровых технологий; разнообразием субъектов и объектов, вовлекаемых в процессы цифровых преобразований.

Публично-правовое обеспечение цифровой трансформации высшего образования требует системного подхода, основанного на согласованной деятельности

⁷ См.: Полякова Т. А., Минбалева А. В., Кроткова Н. В. Указ. соч. С. 215.

⁸ См.: Полякова Т. А., Наумов В. Б., Минбалева А. В. Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве России // Государство и право. 2025. № 1. С. 160—173.

Минобрнауки России, Минцифры России, Роскомнадзора, иных федеральных органов исполнительной власти, а также субъектов РФ. Доктринальное осмысление соответствующих процессов создает необходимую теоретическую основу для совершенствования законодательства. Обсуждение проблем цифровой трансформации на ведущих научных площадках способствует выработке согласованных подходов к публично-правовому регулированию.

Перспективными направлениями развития законодательства следует признать систематизацию информационного законодательства с учетом потребностей сферы высшего образования, формирование специального правового режима ЭИОС, использование экспериментальных правовых режимов для апробации цифровых инноваций в образовании, формирование комплексных правовых основ применения искусственного интеллекта в обучении и оценивании, обеспечение технологического суверенитета и информационной безопасности в сфере высшего образования.

Реализация указанных направлений обеспечит системное и эффективное публично-правовое обеспечение цифровой трансформации высшего образования в Российской Федерации, отвечающее как национальным целям развития государства, так и интересам участников образовательных отношений.

БИБЛИОГРАФИЯ

1. *Виноградова Е. В., Полякова Т. А., Минбалеев А. В.* Цифровой профиль: понятие, механизмы регулирования и проблемы реализации // *Правоприменение*. — 2021. — Т. 5. — № 4. — С. 5—19.
2. *Наумов В. Б.* Право и «Батлерианский джихад»: размышления об угрозах использования искусственного интеллекта // *Информационное общество*. — 2025. — № 2. — С. 131—147.
3. *Полякова Т. А., Минбалеев А. В.* Понятие и правовая природа «цифровой зрелости» // *Государство и право*. — 2021. — № 9. — С. 107—116.
4. *Полякова Т. А., Минбалеев А. В., Кроткова Н. В.* Цифровая трансформация как правовой феномен и ее влияние на развитие информационного права и законодательства // *Государство и право*. — 2025. — № 11. — С. 204—219.
5. *Полякова Т. А., Минбалеев А. В., Наумов В. Б.* К вопросу о кодификации информационного законодательства в условиях цифровой трансформации // *Государство и право*. — 2024. — № 1. — С. 81—91.
6. *Полякова Т. А., Наумов В. Б., Минбалеев А. В.* Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве России // *Государство и право*. — 2025. — № 1. — С. 160—173.

К вопросу о «новых» правах человека в контексте цифрового конституционализма

Аннотация. Предпринята попытка анализа системы прав человека последнего поколения, сформировавшихся благодаря достижениям прорывных технологий, с позиции концепции цифрового конституционализма.

Отмечено, что институт государственного управления эволюционирует под влиянием множества факторов, в том числе цифровых технологий, детерминировавших появление цифрового государства и цифрового конституционализма, характеризующихся изменением характера и способа взаимодействия основных участников правоотношений — государства, общества и гражданина.

Утверждается, что система прав человека, трансформировавшаяся под влиянием цифровых технологий, привела к появлению не только цифровых прав человека, но и ряда примыкающих к ним прав. Среди последних особое внимание уделяется нейроправам, обеспечивающим защиту целостности и неприкосновенности человеческой личности при взаимодействии с технологиями.

По результатам исследования сделан вывод о необходимости дальнейшего теоретического осмысления системы цифровых прав человека в неразрывной связи с совокупностью нейроправ с целью защиты не только способов взаимодействия с киберсредой, но и охраны уникальной человеческой личности от неправомерных модификаций. Обосновывается целесообразность осмысления концепции цифрового конституционализма, системы цифровых и близких к ним прав в правовых позициях высшего судебного органа конституционного контроля с целью выявления конституционно-правового смысла указанных категорий и обеспечения их надлежащей реализации и защиты.

Ключевые слова: цифровая трансформация, сквозные цифровые технологии, киберпространство, цифровое государство, цифровой конституционализм, цифровые права человека, нейроправа



**Татьяна Викторовна
ПАШНИНА,**

доцент кафедры
общетеоретических
правовых дисциплин
Уральского филиала
Российского
государственного
университета правосудия
имени В.М. Лебедева,
кандидат юридических
наук, доцент
pashninatv_chel@mail.ru
454135, Россия,
г. Челябинск,
ул. Энергетиков, д. 63

DOI: 10.17803/2311-5998.2026.142.6.153-160

Tatiana V. PASHNINA,

*Associate Professor of the Department of General Theoretical Legal Disciplines
of Ural branch of the Russian State University of Justice named V.M. Lebedev,*

Cand. Sci. (Law), Associate Professor,

pashninatv_chel@mail.ru

63, ul. Energetikov, Chelyabinsk, Russia, 454135

On the Issue of «New» Human Rights in the Context of Digital Constitutionalism

Abstract. *This study presents a comprehensive analysis of the contemporary human rights system, shaped by breakthrough technologies, within the framework of digital constitutionalism.*

The evolution of public administration is increasingly driven by transformative factors, most notably end-to-end digital technologies. These advancements have given rise to the concepts of the digital state and digital constitutionalism, fundamentally reshaping the nature and dynamics of interactions among the key participants in legal relations: the state, society, and the individual. As digital technologies redefine the human rights landscape, they have not only led to the emergence of digital human rights but also prompted the development of a range of related rights. Among these, neuro-rights occupy a particularly significant place. They are designed to safeguard the integrity and inviolability of the human person in the context of technological interaction, addressing emerging risks associated with cognitive and neural data. The findings of this research underscore the critical need for further theoretical exploration of the digital human rights system — especially its intrinsic connection with neuro-rights. Such understanding is essential not only to regulate interactions within the cyber environment but also to protect the unique human personality from unlawful or invasive “modifications” that could compromise personal autonomy and dignity.

Finally, the study substantiates the necessity of integrating the concept of digital constitutionalism and the system of digital and related rights into the legal positions of the supreme judicial body of constitutional control. The expediency of understanding the concept of digital constitutionalism and the system of digital and related rights in the legal positions of the supreme judicial body of constitutional control is substantiated in order to identify the constitutional and legal meaning of these categories and ensure their proper implementation and protection.

Keywords: *digital transformation, end-to-end digital technologies, cyberspace, digital state, digital constitutionalism, digital human rights, neuro rights*

Актуальность проблемы

Современный мир, вступивший на путь гонки технологий, переживает эпоху трансформации институтов, насчитывающих тысячелетнюю историю и казавшихся

незыблемыми. К таким институтам относится институт государства, в условиях цифровой трансформации изменившего способы государственного управления и превратившегося в государство цифровое.

Термин «цифровое государство» не имеет ни конституционного, ни иного нормативного закрепления, однако он нашел достаточно детальное осмысление в трудах представителей как юридической науки, так и иных областей знаний.

Под *цифровым государством* исследователи предлагают понимать:

- «способ осуществления информационных аспектов государственной деятельности, основанный на использовании информационно-компьютерных систем, а также новый тип государства, основанный на использовании цифровых технологий»¹;
- «информационно-технологическую организацию политико-правового взаимодействия граждан и органов публичной власти»² и др.

Несмотря на различия формулировок, очевидно, что государство может стать цифровым только в результате цифровой трансформации государственного аппарата и способа государственного управления.

Вектор такой трансформации был задан рядом стратегических документов. Цифровое государство меняет не только способ государственного управления, но и саму суть взаимоотношений государства, общества и гражданина, нашедших воплощение в концепции цифрового конституционализма.

Сущность и подсистемы цифрового конституционализма

Конституционные поправки 2020 г. лишь точно регулируют вопросы, касающиеся применения информационных технологий и обеспечения информационной безопасности³ и никаких концептуальных формулировок не содержат, однако, по справедливому утверждению Е. В. Алферовой, «они становятся отправной точкой для реализации в российском законодательстве концепции цифрового суверенитета личности, дальнейшего укрепления гарантий соблюдения конституционных прав и свобод личности в киберпространстве»⁴.

¹ Мамитова Н. В. Цифровое государство в современном обществе: теория и практика // Право.by. 2022. № 5 (79). С. 109.

² Золаев Э. А. Цифровое государство как новый этап развития общества // Креативная экономика. 2021. Т. 15. № 5. С. 1592.

³ К таким конституционным поправкам относится п. «и» ст. 71, включивший информацию, информационные технологии и связь в предметы ведения Российской Федерации и п. «м» ст. 71, также отнесший к ведению центральной власти «обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных». См.: Конституция Российской Федерации (принята всенарод. голосованием 12.12.1993, с изм., одобренными в ходе общерос. голосования 01.07.2020) // URL: <http://www.pravo.gov.ru>, 04.07.2020.

⁴ Алферова Е. В. «Цифровые» новеллы Конституции Российской Федерации: взгляд ученых-юристов (Обзорная статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4 : Государство и право. 2023. № 4. С. 97.

Соответственно, ни определения понятий цифрового государства, цифрового конституционализма, цифрового суверенитета, ни закрепления конституционных цифровых прав на уровне Основного закона и иного конституционного законодательства дано не было. Тем не менее изменения в способе государственного управления и, соответственно, характере взаимоотношений основных акторов — государства, общества и гражданина — на конституционном уровне являются достаточно очевидными, что породило появление концепции цифрового конституционализма.

Понятие «цифровой конституционализм» считается относительно новым в науке конституционного права и в силу этого дискуссионным.

Говоря о сущности категории «конституционализм», С. Ю. Поярко в отмечает, что долгое время это был «феномен, исторически формировавшийся как результат борьбы за ограничение власти и обеспечение прав человека, как совокупность идей, принципов и институтов, направленных на утверждение правового порядка, в котором власть действует в пределах, очерченных законом и справедливостью. Однако в условиях стремительно изменяющейся реальности, когда государство сталкивается с новыми вызовами — от экспансии цифровых технологий до изменения геополитического баланса и углубления глобализационных процессов, — прежние концептуальные основания конституционализма оказываются под давлением и требуют переосмысления». Одной из концепций, появившихся в результате попытки найти ответы на вызовы современности, стала концепция цифрового конституционализма⁵, при этом «идея цифрового конституционализма в своем генезисе опирается на признание того, что цифровая среда — это не просто технологическое расширение офлайн-реальности, а новая форма общественного бытия, обладающая собственными структурами власти, механизмами воздействия и нормативными режимами»⁶.

Так, И. А. Кравец, стоящий у истоков этой идеи, считает, что современный конституционализм в настоящее время испытывает влияние со стороны информационных факторов, результатом чего является «конституционализация информационного и цифрового пространства... происходит цифровизация конституционной коммуникации и конституционных прав и свобод, их техническое оснащение посредством цифровых технологий»⁷.

Исследователи отмечают, что «цифровой конституционализм предстает как сложная и амбивалентная концепция, в которой традиционные идеи верховенства права, демократии и прав человека приобретают новые формы»⁸.

Одним из ключевых элементов цифрового конституционализма является цифровизация личности, что, соответственно, порождает необходимость

⁵ Поярко в С. Ю. Трансформация конституционализма в современном обществе: концептуальные основания // Право и политика. 2025. № 4. С. 106.

⁶ Гончаров В. В., Поярко в С. Ю., Савченко М. С. Цифровой конституционализм: эволюция правовых принципов в условиях цифровизации современного общества // Общество: политика, экономика, право. 2025. № 8. С. 205.

⁷ Кравец И. А. Цифровой конституционализм: методологические и правовые аспекты // Государство и право. 2022. № 1. С. 24.

⁸ Гончаров В. В., Поярко в С. Ю., Савченко М. С. Указ. соч. С. 206.

адекватного регулирования ее правового статуса с учетом возможностей, вызовов и угроз киберпространства.

Система цифровых прав человека

В теории конституционного права сформировано устойчивое мнение о том, что одним из важнейших вопросов, входящих в предмет ее изучения, является вопрос о том, каково правовое положение личности в государстве и на каких принципах строятся взаимоотношения человека и государства. Соответственно, для отрасли конституционного права одним из основополагающих институтов будет институт правового положения личности, ключевую роль в котором играет триада: принципы, права и обязанности, также эволюционирующие под влиянием цифровой революции.

Поскольку базовый элемент правового статуса — цифровые права, появившиеся благодаря информационным технологиям, не нашли законодательного закрепления в источниках конституционного права, консенсуса относительно того, что включать в данную категорию, в научном сообществе не сформировалось⁹.

К правам, появившимся в процессе цифровизации, — *цифровым правам человека* — исследователи относят:

- *право на доступ к Интернету*, включающее ряд правомочий: «а) право на доступ к Интернету, б) право не быть отключенным, в) право на свободный поиск информации, г) право на безопасное использование Интернета и право на защиту от нежелательной информации»¹⁰;
- *право на защиту цифровых следов*, включающее: а) право на забвение, вытекающее из положений Федерального закона от 13.07.2015 № 264-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации” и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации»¹¹ и означающее «возможность полного уничтожения своего цифрового следа»; б) право на цифровую

⁹ В российском законодательстве нашел отражение узкий подход к цифровым правам, реализованный в ст. 141.1 ГК РФ, согласно которому таковыми «признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам» (Гражданский кодекс РФ, часть первая, от 30.11.1994 № 51-ФЗ // СЗ РФ. 1994. № 32. Ст. 3301).

¹⁰ См.: Минбалева А. В. Воздействие конституционных прав и свобод человека и гражданина на развитие информационного права в условиях цифровизации современного общества // Юридическое образование и юридическая наука в России: современные тенденции и перспективы развития : сб. материалов Всерос. науч.-практич. конф. Курск, 2019. С. 207 ; Талапина Э. В. Эволюция прав человека в цифровую эпоху // Труды Института государства и права РАН. 2019. № 3. С. 130—131.

¹¹ СЗ РФ. 2015. № 29 (ч. I). Ст. 4390.

смерть, подразумевающее «возможность наследования цифровой информации умершего пользователя сети»¹²;

— *право на цифровизацию и отказа от нее*¹³.

Выделяют также ряд других прав: «право на цифровую автономию, право на недискриминацию в цифровой среде, право на равный доступ к цифровой инфраструктуре и глобальным сервисам»¹⁴ и др.

В целом можно констатировать, что перечисленные права либо конкретизируют имеющиеся конституционные права: на информацию, неприкосновенность частной жизни, личную и семейную тайну и т.д., либо вытекают из норм информационного законодательства, как упомянутое право на забвение.

Нейроправа как часть совокупности прав цифровой личности

Однако изучение цифровых прав человека будет неполным без анализа группы примыкающих к ним прав, сформировавшихся на стыке информационных и биологических прав — *нейроправ*, отвечающих за защиту целостности человеческой личности от негативного воздействия прорывных технологий.

Данная категория сформировалась благодаря достижениям в области нейротехнологий¹⁵, которые относятся к группе сквозных технологий, способных применяться совместно с технологиями искусственного интеллекта (Дорожная карта развития сквозной цифровой технологии «Нейротехнологии и искусственный интеллект»¹⁶), а также технологиями виртуальной и дополненной реальности (проекты Центра Национальной технологической инициативы¹⁷).

Система нейроправ также является предметом научной дискуссии, начало которой было положено в конце 1990-х гг.

Наиболее авторитетным среди зарубежных исследований данного вопроса признается классификация, данная Иенцой Марцелло и Роберто Андорно,

¹² Захаров А. Е. Развитие нового поколения прав человека в эпоху цифровых технологий // Государственная служба и кадры. 2025. № 1. С. 40.

¹³ Алферова Е. В. Указ. соч. С. 107—108.

¹⁴ Амелин В. Ю., Пахомова Н. А., Кретова С. Права четвертого поколения: защита цифровых следов и проблема геополитической сегрегации цифровых прав // Проблемы развития современного общества : сборник научных статей 11-й Всерос. нац. научно-практ. конф. : в 4 т. Курск : Университетская книга, 2026. С. 134.

¹⁵ Под нейротехнологиями понимаются «технологии, которые используют или помогают понять работу мозга, мыслительные процессы, высшую нервную деятельность, в том числе технологии по усилению, улучшению работы мозга и психической деятельности» (ГОСТ Р 59277-2020 «Системы искусственного интеллекта. Классификация систем искусственного интеллекта». П. 3.34).

¹⁶ URL: <https://digital.gov.ru/uploaded/files/07102019ii.pdf> (дата обращения: 03.05.2026).

¹⁷ Центр компетенций НТИ по направлению «Нейротехнологии, технологии виртуальной и дополненной реальности». URL: https://nti2035.ru/technology/competence_centers/fefu.php (дата обращения: 03.05.2026).

выделивших «право на когнитивную свободу, ментальную конфиденциальность, ментальную целостность и психологическую преемственность (непрерывность)»¹⁸.

Одним из наиболее полных отечественных исследований является работа Д. А. Беловой, предложившей выделять следующие виды нейроправ: «право на когнитивную свободу; право на неприкосновенность нейронных данных; право на психическую неприкосновенность и право на психическую целостность (непрерывность)»¹⁹.

Независимо от особенностей классификации, неизменным является то, что нейроправа защищают саму сущность человеческой личности, ее индивидуальность от возможных «модификаций».

В силу того что в основе нейроправ лежит информация (нейроданные), а также общего генезиса, полагаем целесообразным рассматривать нейроправа в совокупности с правами цифровыми.

Выводы и предложения

Подытоживая вышесказанное, считаем необходимым сформулировать ряд положений:

1. *Цифровой конституционализм* обусловлен новым характером взаимодействия основных акторов — государства, общества и гражданина на учрежденческом уровне в эпоху прорывных цифровых технологий, изменивших, как уже отмечалось ранее, способ государственного управления и взаимодействия основных участников правоотношений.

Включение соответствующих положений в текст Основного закона считаем преждевременным, однако дальнейшее теоретическое осмысление данной концепции представляется целесообразным в качестве концептуальной базы адаптации Российского государства и права к вызовам киберсреды.

2. Полагаем необходимым дальнейшее теоретическое осмысление системы цифровых прав человека — базового элемента цифрового конституционализма — в неразрывной связи с совокупностью нейроправ с целью защиты не только способов взаимодействия с киберсредой, но и охраны уникальности человеческой личности.

Представляется, что дальнейшее закрепление нейроправ пойдет по тому же пути, что и существующих цифровых прав, и будет связано с дальнейшим развитием информационного законодательства.

3. Перспективным видится осмысление цифрового конституционализма и его элементов, и прежде всего цифровых прав основных субъектов правоотношений, через призму правовых позиций Конституционного Суда РФ, как было в случае с включением в текст Конституции РФ понятия «публичная власть». Такой шаг позволит выявить конституционно-правовой смысл указанных категорий и обеспечить их надлежащую реализацию и защиту.

¹⁸ Цит. по: Корнехо Я. Нейроправа, нейротехнологии и персональные данные: обзор проблем психологической автономии // Journal of Digital Technologies and Law. 2024. № 2 (3). Р. 720.

¹⁹ Белова Д. А. Нейроправо. Правовой аспект исследования применения нейротехнологий : монография. М. : Проспект, 2025. С. 99.



БИБЛИОГРАФИЯ

1. *Алферова Е. В.* «Цифровые» новеллы Конституции Российской Федерации: взгляд ученых-юристов (обзорная статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. — Серия 4 : Государство и право. — 2023. — № 4. — С. 92—108.
2. *Амелин В. Ю., Пахомова Н. А., Кротова С.* Права четвертого поколения: защита цифровых следов и проблема геополитической сегрегации цифровых прав // Проблемы развития современного общества : сборник научных статей 11-й Всероссийской национальной научно-практической конференции : в 4 т., Курск, 19—20 января 2026 г. — Курск : Университетская книга, 2026. — С. 130—136.
3. *Белова Д. А.* Нейроправо. Правовой аспект исследования применения нейротехнологий : монография. — М. : Проспект, 2025. — 118 с.
4. *Гончаров В. В., Поярков С. Ю., Савченко М. С.* Цифровой конституционализм: эволюция правовых принципов в условиях цифровизации современного общества // Общество: политика, экономика, право. — 2025. — № 8. — С. 203—215.
5. *Захаров А. Е.* Развитие нового поколения прав человека в эпоху цифровых технологий // Государственная служба и кадры. — 2025. — № 1. — С. 39—42.
6. *Золотов Э. А.* Цифровое государство как новый этап развития общества // Креативная экономика. — 2021. — Т. 15. — № 5. — С. 1583—1594.
7. *Корнехо Я.* Нейроправа, нейротехнологии и персональные данные: обзор проблем психологической автономии // Journal of Digital Technologies and Law. — 2024. — № 2 (3). — Р. 711—728.
8. *Кравец И. А.* Цифровой конституционализм: методологические и правовые аспекты // Государство и право. — 2022. — № 1. — С. 19—33.
9. *Мамитова Н. В.* Цифровое государство в современном обществе: теория и практика // Право.by. — 2022. — № 5 (79). — С. 108—116.
10. *Минбалеев А. В.* Воздействие конституционных прав и свобод человека и гражданина на развитие информационного права в условиях цифровизации современного общества // Юридическое образование и юридическая наука в России: современные тенденции и перспективы развития (к 15-летию юрид. факультета Курского гос. ун-та) : сб. материалов Всерос. науч.-практич. конф. — Курск, 2019. — С. 204—212.
11. *Поярков С. Ю.* Трансформация конституционализма в современном обществе: концептуальные основания // Право и политика. — 2025. — № 4. — С. 105—122.
12. *Талапина Э. В.* Эволюция прав человека в цифровую эпоху // Труды Института гос-ва и права РАН. — 2019. — № 3. — С. 122—146.
13. *Ienca Marcello, Roberto Andorno.* Towards new human rights in the age of neuroscience and neurotechnology // Life Sciences, Society and Policy. — 2017. — № 13. — Р. 1—27.

Моральные императивы в праве ЮАР: концепция Ubuntu и конституционные вызовы

Аннотация. История Южно-Африканской Республики характеризуется противоречиями, борьбой и конфликтами. Однако существует общая и объединяющая основа — концепция убунту, которая приобрела особое значение в правовом дискурсе после отмены апартеида. Убунту представляет собой философскую концепцию и образ жизни. Одним из наиболее известных выражений, передающих ее суть, является афоризм: «Человек становится человеком благодаря другим людям». Эта концепция предлагает оригинальные подходы к решению социальных, экономических и политических проблем африканского континента для обеспечения общего благополучия общества. Данная концепция направлена на деколонизацию южноафриканского права, где моральные императивы способствуют преобразованию конституционализма в контекстуально обоснованную систему социальной справедливости, преодолевающую наследие апартеида. Концепция убунту стала основой трансформационного конституционализма в ЮАР и признается в качестве конституционной ценности.

Ключевые слова: африканская философия, убунту, конституционализм, Конституционный суд, права человека



**Елена Александровна
СОРОКИНА,**

научный сотрудник
сектора прав человека
Института государства
и права РАН,
кандидат юридических наук
sorokina_ea@mail.ru
119019, Россия, г. Москва,
ул. Знаменка, д. 10

DOI: 10.17803/2311-5998.2026.142.6.161-169

E. A. SOROKINA,

Research fellow of the Human Rights Department
of the Institute of State and Law
of The Russian Academy of Sciences,
Cand. Sci. (Law)
sorokina_ea@mail.ru

10, ul. Znamenka, Russia, Moscow, 119019

Moral Imperatives in South African Law: The Concept of Ubuntu and Constitutional Challenges

Abstract. South Africa has a history of deep divisions characterised by strife and conflict. However, there exists a general and unifying basis — the concept of Ubuntu, which has acquired a special significance in the legal discourse in post-apartheid South Africa.

Ubuntu is a philosophical concept and a way of life. One of the most well-known expressions conveying its essence is the aphorism: “A person is a person through other people”. This concept offers original approaches to solving social, economic, and political problems of the African continent to ensure the common well-being of society. Ubuntu contributes to the decolonization of South African law, where moral imperatives contribute to the

© Сорокина Е. А., 2026

transformation of constitutionalism into a contextually grounded system of social justice that overcomes the legacy of apartheid. Ubuntu has become the foundation of transformative constitutionalism in South Africa and is recognized as a constitutional value.

Keywords: African philosophy, Ubuntu, constitutionalism, Constitutional Court, human rights

Убунту часто определяется как африканское равенство¹, африканское достоинство², африканское правосудие³, африканский гуманизм⁴, африканская ценность⁵, конституционная ценность⁶, социальная ценность⁷ и другие аналогичные понятия. Точное определение этого термина представляет собой сложную задачу, поскольку его сущность раскрывается через множество коннотаций и смысловых нюансов, которые носят оценочный характер⁸. Убунту является многогранным и сложным явлением, сформировавшимся на протяжении веков на африканском континенте; это одновременно образ жизни, мировоззрение и философия⁹.

В исследованиях акцентируется внимание, что колониальное управление привнесло в Южную Африку западную парадигму прав человека, оставив

¹ Bennett T. W. Ubuntu: An African Equity // Potchefstroom Electronic Law Journal. 2017. Vol. 14. No. 4. P. 29—61.

² Metz T. Ubuntu as a Moral Theory and Human Rights in South Africa // African Human Rights Law Journal. 2011. Vol. 11. No. 2. P. 532—559.

³ Elechi O. O., Morris S. V. C., Schauer E. J. Restoring Justice (Ubuntu): An African Perspective // International Criminal Justice Review. 2010. Vol. 20. Is. 1. P. 73—85.

⁴ Lenta P. The Changing Face of The Law: Ubuntu, Religion and the Politics Legality // Explorations in Contemporary Continental Philosophy of Religion / ed. by D-P. Baker, P. Maxwell. Amsterdam ; New York, 2003. P. 155—174.

⁵ Bohler-Müller N. The Story of an African Value. Focus: Ten Years after Makwanyane // Southern African Public Law. 2005. Vol. 20. Is. 2. P. 266—280.

⁶ Albertyn C. Values in the South African Constitution // An Inquiry into the Existence of Global Values. Through the Lens of Comparative Constitutional Law / ed. by D. Davis, A. Richter, Ch. Saunders. Oxford, 2015, P. 345 ; Mbeki T. Let Africa Lead: African Transformational Leadership for 21st Century Business. Johannesburg, 2013. P. xii.

⁷ Dithlake K. J. Thirty Years of Democracy in South Africa: Reflecting on Social Work and Climate Change Challenges through a Ubuntu Lense // Decolonizing Western-Indigenous Dialogues: Interwoven Epistemologies for Multiple Modernities / ed. by K. Kiewitt, R. Lutz, G. Cajete, M. do Carmo dos Santos Gonçalves, K. J. Dithlake. London, 2025. P. 186.

⁸ Подробнее см.: Mokgoro Y. Ubuntu and the Law in South Africa // Ubuntu and the Law: African Ideals and Post-Apartheid Jurisprudence / ed. by C. Drucilla, M. Nyoko. New York, 2012. P. 317—323.

⁹ Мосейко А. Н. Ценностно-этическая система в Африке южнее Сахары. От прошлого — к будущему // Ученые записки Института Африки РАН. 2023. № 3. С. 113 ; Mbeki T. Op. cit. P. xii.

неизгладимый след в правовой и политической структуре страны¹⁰. Вместе с тем западные модели конституционализма, а также традиция связывания идеи прав человека прежде всего с индивидуальной свободой в самых разных ее проявлениях, автономией и достоинством личности часто вступали в противоречие с африканскими концепциями, такими как убунту. Последняя делает акцент на коллективном благополучии, взаимозависимости и социальной гармонии, воплощая моральный императив взаимной ответственности¹¹.

Начиная с 1990-х гг. концепция убунту стала основой для конституционного развития в ЮАР¹². Временная Конституция 1993 г. включала положение, подчеркивающее необходимость преодоления наследия апартеида, приведшего к многочисленным нарушениям прав человека. Вместо возмездия и мести предлагалось сосредоточиться на создании будущего, основанного, среди прочего, на убунту, что рассматривалось как положительный шаг, поскольку свидетельствовало о признании африканских традиций и ценностей в национальной правовой системе¹³.

Однако в действующей Конституции, принятой в 1996 г., термин «убунту» был исключен, что вызвало критику со стороны ряда экспертов¹⁴. Существует также противоположная точка зрения, согласно которой его включение не являлось обязательным, поскольку в преамбуле акцентируется внимание на социальной справедливости, отражающей дух этой концепции¹⁵. Кроме того, ст. 39 Конституции предписывает судебным органам при толковании руководствоваться ценностями открытого и демократического общества, основанного на человеческом достоинстве, равенстве и свободе, а также придерживаться духа, смысла и целей Билля о правах. В данном контексте особо подчеркивается, что наряду с конституционными ценностями, такими как достоинство, равенство и свобода, признаются имплицитные, обладающие равным статусом, включая убунту¹⁶.

¹⁰ Подробнее см.: *Ndlovu-Gatsheni S. J.* Decoloniality as the Future of Africa // *History Compass*. 2015. Vol. 13. No. 10. P. 485—496.

¹¹ *Cornell D.* Is there a Difference that Makes a Difference between uBuntu and Dignity? // *Southern African Public Law*. 2010. Vol. 25. No. 2. P. 384 ; *Белов С. А.* Ценности незападных политических традиций // *Сравнительное конституционное обозрение*. 2024. Т. 33. № 2. С. 83—84.

¹² *Khunou S. F., Nthai S.* The Contribution of Ubuntu to the Development of Constitutional Jurisprudence in a Democratic South Africa // *Ubuntu, Good Faith and Equity: Flexible Legal Principles in Developing a Contemporary Jurisprudence* / ed. by F. Diedrich. Claremont, 2012. P. 53—54.

¹³ *Moosa E.* Tensions in Legal and Religious Values in the 1996 South African Constitution // *Beyond Rights Talk and Culture Talk: Comparative Essays on the Politics of Rights and Culture* / ed. by M. Mamdani. Cape Town, 2000. P. 130.

¹⁴ *Moosa E.* Op. cit. P. 131.

¹⁵ Подробнее см.: *Radebe S. B., Phooko M. R.* Ubuntu and the Law in South Africa: Exploring and Understanding the Substantive Content of Ubuntu // *South African Journal of Philosophy*. 2017. Vol. 36. No. 2. P. 239—251 ; *Nkosi S.* Ubuntu and South African Law: Its Juridical Transformative Impact // *Southern African Public Law*. 2018. Vol. 33. No. 1. P. 1—20.

¹⁶ *Himonga C., Taylor M., Pope A.* Reflections on Judicial Views of Ubuntu // *Potchefstroom Electronic Law Journal*. 2013. Vol. 16. No. 5. P. 380.

Впервые данная концепция нашла отражение в решении по делу *S v. Makwanyane and Another*¹⁷, в котором оценивалась конституционность законодательства, предусматривающего применение наказания в виде смертной казни¹⁸.

При рассмотрении данного дела судьи прежде всего опирались на концепцию убунту, чтобы обосновать переход к правопорядку, способному преодолеть жестокость и репрессивность предыдущего режима¹⁹. Убунту при этом описывалась как ценностная система, включающая солидарность внутри сообщества, сострадание, уважение, признание человеческого достоинства и стремление к коллективному единству²⁰.

Концепция убунту, лежащая в основе этого подхода, основывается на представлении о том, что личность человека формируется и развивается благодаря его взаимодействию с другими людьми. В связи с этим система уголовного правосудия должна не только учитывать личность преступника, но и вовлекать сообщество в процессы его реабилитации, перевоспитания и возвращения к полноценной жизни.

Такой подход предполагает активное участие общества, что способствует укреплению социальных связей и созданию условий для восстановления справедливости. Таким образом, совершение преступления и его последствия рассматриваются не только как проблема отдельного человека, но и как вызов всему сообществу. Ответственность за реагирование на противоправные деяния возлагается и на общество, которое должно стремиться к восстановлению гармонии и поддержанию устойчивых социальных отношений²¹.

В последующих решениях по уголовным делам судебные органы обращались к концепции убунту для обоснования назначения более мягких наказаний (учитывая обстоятельства дела, личность обвиняемого, степень раскаяния, его социальную роль в сообществе и готовность добровольного возмещения ущерба и примирения с потерпевшим)²².

Концепция убунту приобрела особое значение в делах о защите социально-экономических прав, связанных с выселениями. В деле *Port Elizabeth Municipality*

¹⁷ South African Constitutional Court (далее — SACC). *S v. Makwanyane and Another*. CCT 3/94. 6 June 1995. ZACC 3.

¹⁸ С 1995 г. по настоящее время термин «убунту» упоминается в 43 решениях Конституционного суда. Подсчитано автором на основании информации, опубликованной на сайте Южноафриканского института правовой информации. См.: The Southern African Legal Information Institute // URL: <https://www.saii.org/content/about-saii-0.html> (дата обращения: 25.02.2026).

¹⁹ *S v. Makwanyane and Another*. Paras 223, 306, 311.

²⁰ *S v. Makwanyane and Another*. Paras 223—227, 235—251, 260, 306—313.

²¹ *Mangena F. Restorative Justice's Deep Roots in Africa* // South African Journal of Philosophy. 2015. Vol. 34. Is. 1. P. 6.

²² См.: High Court (North Gauteng). *S v. Sibiyi*. 461/09. 11 August 2009. ZAGPPHC 173 ; North West High Court (Mafikeng). *S v. Maluleka*. CA 20/2008. 4 August 2008. ZANWHC 23 ; Western Cape High Court (Cape Town). *S v. Matiwane*. CU/2115/2011. 13 August 2012. ZAWCHC 159. Такой подход нашел применение не только в уголовном, но и в деликтном праве. См., например: SACC. *Dikoko v. Mokhatla*. CCT 62/05. 3 August 2006. ZACC 10.

*v. Various Occupiers*²³ (далее — PE Municipality) Конституционный суд отклонил апелляцию на решение Верховного апелляционного суда муниципалитета города Порт-Элизабет, добивавшегося выселения 68 человек с незаконно занятого участка²⁴. Согласно действующему законодательству, судебные органы могут выдать приказ о выселении только в том случае, если он является «справедливым и равноправным», учитывая обстоятельства конкретного дела (в частности, длительность проживания на определенном земельном участке и возможность предоставления альтернативного жилья)²⁵.

В этом деле Конституционный суд отказал в выдаче такого приказа, подчеркнув, что оценка справедливости и равноправия выселения требует учета конституционных ценностей, включая убунту. Суд отметил необходимость установления баланса между правом жильцов на доступ к адекватному жилью и защитой от незаконного выселения, с одной стороны, и правами собственников земли — с другой. Это необходимо для реализации идеи заботливого общества, основанного на добрососедстве и взаимной поддержке²⁶. Суд также указал, что Конституция и действующее законодательство в этой сфере воплощают дух убунту, объединяющий индивидуальные права с философией коммунитаризма, являющейся частью культурного наследия большинства населения, что обязывает судебные органы привносить элементы милосердия и сострадания в формальные структуры права²⁷. Акцентировалось внимание на том, что в случаях выселений существует необходимость добросовестного взаимодействия со сторонами для поиска взаимоприемлемых решений, обосновывая это тем, что конституционно неприемлемо рассматривать людей как «невыносимую социальную проблему»²⁸.

Подход, основанный на участии и взаимодействии, согласуется с концепцией убунту, которая подчеркивает важность диалога, достижение консенсуса, а также таких ценностей, как коллективная солидарность, сострадание, уважение, человеческое достоинство, единство и взаимопонимание²⁹.

Конституционный суд установил, что выселяемые проживали на занятом участке земли в течение нескольких лет, при этом отсутствовала необходимость в их выселении, а органы власти не предприняли должных усилий для взаимодействия с ними и учета их потребностей в альтернативном жилье. Отказ в выдаче приказа о выселении демонстрирует ключевую роль человеческого достоинства и основ концепции убунту в принятии подобных решений. Если бы приказ о выселении был выдан, жильцам пришлось бы переехать в неблагополучный район с отсутствием необходимых условий, что нарушило бы их человеческое достоинство и противоречило основам концепции убунту.

²³ SACC. Port Elizabeth Municipality v. Various Occupiers. CCT 53/03. 1 October 2004. ZACC 7.

²⁴ Port Elizabeth Municipality v. Various Occupiers. Paras 8—10.

²⁵ The Prevention of Illegal Eviction from and Unlawful Occupation of Land Act 1998 // Government Gazette. 5 June 1998. Vol. 396. No. 18964.

²⁶ PE Municipality. Paras 13, 37.

²⁷ PE Municipality. Para. 37.

²⁸ PE Municipality. Para. 39, 41, 45.

²⁹ См.: Сорокина Е. Конструктивное взаимодействие как средство защиты социально-экономических прав в Южно-Африканской Республике // Сравнительное конституционное обозрение. 2025. Т. 34. № 3. С. 111.

Кроме того, Конституционный суд пришел к выводу, что, несмотря на необходимость соблюдения права собственности землевладельцев, его реализация в данном случае не предполагала рационального использования земли. Применение положений действующего законодательства, обязывающего собственников позволять жильцам оставаться на их земле безвозмездно до предоставления государством альтернативного жилья, иллюстрирует взаимную ответственность членов общества друг перед другом, закрепленную в концепции убунту. Таким образом, собственники обязаны проявлять терпимость, заботу и сострадание к другим членам сообщества.

В деле *City of Johannesburg Metropolitan Municipality v Blue Moonlight Properties 39 (Pty) Ltd and Another*³⁰ (далее — *Blue Moonlight Properties*) Конституционный суд вновь подчеркнул важность человеческого достоинства, интерпретируемого через призму концепции убунту, при принятии решений о вынесении приказов о выселении. Основное отличие между делами *PE Municipality* и *Blue Moonlight Properties* заключалось в том, что в последнем случае, хотя приказ о выселении был вынесен, его исполнение было отложено на восемь месяцев, чтобы органы власти смогли предоставить альтернативное жилье в непосредственной близости от текущего места проживания выселяемых. На собственника возложили обязанность разрешить проживающим оставаться на его территории на протяжении этого периода без какой-либо компенсации. Как и в деле *PE Municipality*, отсутствие компенсации собственнику со стороны выселяемых или государства объяснялось моральными императивами концепции убунту. Этот аспект также тесно связан с моделью восстановительного правосудия, направленной на устранение последствий исторических несправедливостей, таких как выселение людей без учета их жизненных обстоятельств, путем поиска согласованного и гармоничного разрешения споров³¹.

Следует подчеркнуть, что Конституционный суд четко обозначил пределы подобных ограничений. Хотя собственник должен проявлять «достаточное терпение» (*somewhat patient*), однако от него нельзя ожидать предоставления бесплатного жилья на неопределенный срок³².

Следует отметить, что в настоящее время предлагается пересмотреть подход к защите социально-экономических прав, делая акцент на необходимости принятия убунту-ориентированной модели. Этот подход предполагает замену стандарта разумности (*reasonableness review*), который был принят Конституционным судом для защиты данных прав, поскольку он не учитывает африканский контекст. В данном случае подчеркивается, что убунту предлагает реляционную перспективу, рассматривая социально-экономические права как коллективные обязательства сообщества, а не индивидуальные притязания³³.

³⁰ SACC. *City of Johannesburg Metropolitan Municipality v. Blue Moonlight Properties 39 (Pty) Ltd and Another*. CC. 1 December 2011. ZACC 33.

³¹ *Bennett W. T. Ubuntu: An African Jurisprudence*. Cape Town: Juta, 2018. P. 79.

³² *Blue Moonlight Properties*. Paras 30—41, 97.

³³ *Gcumeni F. G. A., Rautenbach C. Rethinking Socio-Economic Rights in South Africa: Embracing Ubuntu as a Transformative Legal Framework // Legal Pluralism and Critical Social Analysis*. 2025. Vol. 57. Is. 2—3. P. 105—128.

Существуют различные точки зрения относительно интеграции концепции убунту в правоприменительную практику. Основной критике подвергается ее многозначность и неопределенность, что может привести к субъективной интерпретации со стороны судей³⁴. В связи с этим утверждается, что полисемия убунту затрудняет ее использование в качестве основы для конституционного толкования³⁵.

Кроме того, подход Конституционного суда к конституционным ценностям также вызывает вопросы. Отмечается, что судебная власть нередко упоминает моральные императивы убунту как неоспоримые истины («маленькие божества»), не подвергая их критическому анализу и не учитывая их особенностей и онтологического статуса³⁶.

Вместе с тем гибкость концепции убунту предоставляет возможность ее адаптации к условиям трансформационного конституционализма, обогащая правовую систему и процесс правоприменения живой традицией, отвечая актуальным потребностям южноафриканского общества. Кроме того, важно учитывать, что южноафриканские судьи восприняли моральные императивы убунту через нарративы, передаваемые из поколения в поколение. Многие из них до назначения на судебские должности работали в сфере защиты прав человека и имеют непосредственное представление о масштабах нарушений прав, затронувших большую часть южноафриканского населения. Тот факт, что один судья может выделять одну ценность в определенном контексте, а другой — другую, не умаляет их значимости. Судьи осознают тот факт, что ценности и защита прав тесно взаимосвязаны и являются неотъемлемой частью конституционного развития³⁷.

В целом считается, что южноафриканское право должно быть адаптировано к местным условиям³⁸. Однако более детальные аспекты этого процесса остаются недостаточно проработанными. Несмотря на это, судебная власть, основываясь на концепции убунту, способствует данному процессу.

³⁴ Himonga C., Taylor M., Pope A. Op. cit. P. 372.

³⁵ uBuntu and the Law: African Ideals and Postapartheid Jurisprudence / eds. by D. Cornell, N. Muvangua. New York, 2012. P. 10.

³⁶ Kroeze I. J. Doing Things with Values: The Case of uBuntu // uBuntu and the Law: African Ideals and Postapartheid Jurisprudence / eds. by D. Cornell, N. Muvangua. New York, 2012. P. 333—343.

³⁷ Nkosi S. Ubuntu and South African Law: Its Juridical Transformative Impact // Southern African Public Law. 2018. Vol. 33. No. 1. P. 6—7.

³⁸ См.: Rautenbach Ch. Exploring the Contribution of Ubuntu in Constitutional Adjudication — Towards the Indigenization of Constitutionalism in South Africa? // Constitutional Adjudication in Africa / ed. by C. Fombad. Oxford : Oxford University Press, 2017. P. 309 ; Gcumeni F. G. A., Rautenbach C. Rethinking Socio-Economic Rights in South Africa: Embracing Ubuntu as a Transformative Legal Framework // Legal Pluralism and Critical Social Analysis. 2025. Vol. 57. Is. 2—3. P. 105—128 ; Sesanti S. The Exclusion of Ubuntu from South Africa's Constitution: Implications for Pan-Africanism and Violent 'Xenophobia' // African Studies. 2025. Vol. 84. No. 3. P. 191—207.

БИБЛИОГРАФИЯ

1. Белов С. А. Ценности незападных политических традиций // Сравнительное конституционное обозрение. — 2024. — Т. 33. — № 2. — С. 73—88.
2. Мосейко А. Н. Ценностно-этическая система в Африке южнее Сахары. От прошлого — к будущему // Ученые записки Института Африки РАН. — 2023. — № 3. — С. 110—124.
3. Сорокина Е. Конструктивное взаимодействие как средство защиты социально-экономических прав в Южно-Африканской Республике // Сравнительное конституционное обозрение. — 2025. — Т. 34. — № 3. — С. 107—125.
4. Albertyn C. Values in the South African Constitution // An Inquiry into the Existence of Global Values. Through the Lens of Comparative Constitutional Law / ed. by D. Davis, A. Richter, Ch. Saunders. — Oxford : Hart Publishing, 2015. — P. 321—416.
5. Bennett T. W. Ubuntu: An African Equity // Potchefstroom Electronic Law Journal. — 2017. — Vol. 14. — No. 4. — P. 29—61.
6. Bennett T. W. Ubuntu: An African Jurisprudence. — Cape Town : Juta, 2018. — 223 p.
7. Bohler-Müller N. The Story of an African Value. Focus: Ten Years after Makwanyane // Southern African Public Law. — 2005. — Vol. 20. — Iss. 2. — P. 266—280.
8. uBuntu and the Law: African Ideals and Postapartheid Jurisprudence / eds. by D. Cornell, N. Muvangua. — New York : Fordham University Press, 2012. — 466 p.
9. Cornell D. Is there a Difference that Makes a Difference between uBuntu and Dignity? // Southern African Public Law. — 2010. — Vol. 25. — No. 2. — P. 382—399.
10. Dithake K. J. Thirty Years of Democracy in South Africa: Reflecting on Social Work and Climate Change Challenges through a Ubuntu Lense // Decolonizing Western-Indigenous Dialogues: Interwoven Epistemologies for Multiple Modernities / ed. by K. Kiewitt, R. Lutz, G. Cajete, M. do Carmo dos Santos Gonçalves, K. J. Dithake. — London : Bloomsbury Publishing, 2025. — P. 183—194.
11. Elechi O. O., Morris S. V. C., Schauer E. J. Restoring Justice (Ubuntu): An African Perspective // International Criminal Justice Review. — 2010. — Vol. 20. — Iss. 1. — P. 73—85.
12. Gcumeni F. G. A., Rautenbach C. Rethinking Socio-Economic Rights in South Africa: Embracing Ubuntu as a Transformative Legal Framework // Legal Pluralism and Critical Social Analysis. — 2025. — Vol. 57. — Iss. 2—3. — P. 105—128.
13. Himonga C., Taylor M., Pope A. Reflections on Judicial Views of Ubuntu // Potchefstroom Electronic Law Journal. — 2013. — Vol. 16. — No. 5. — P. 371—429.
14. Khunou S. F., Nthai S. The Contribution of Ubuntu to the Development of Constitutional Jurisprudence in a Democratic South Africa // Ubuntu, Good Faith and Equity: Flexible Legal Principles in Developing a Contemporary Jurisprudence / ed. by F. Diedrich. — Claremont : Juta, 2012. — P. 49—69.
15. Kroeze I. J. Doing Things with Values: The Case of uBuntu // uBuntu and the Law: African Ideals and Postapartheid Jurisprudence / eds. by D. Cornell, N. Muvangua. — New York : Fordham University Press, 2012. — P. 333—343.

16. *Lenta P.* The Changing Face of The Law: Ubuntu, Religion and the Politics Legality // *Explorations in Contemporary Continental Philosophy of Religion* / ed. by D-P. Baker, P. Maxwell. — Amsterdam ; New York : Rodopi, 2003. — P. 155—174.
17. *Mangena F.* Restorative Justice's Deep Roots in Africa // *South African Journal of Philosophy*. — 2015. — Vol. 34. — Is. 1. — P. 1—12.
18. *Mbeki T.* Let Africa Lead: African Transformational Leadership for 21st Century Business. — Johannesburg: Vezubuntu Publishing, 2013.
19. *Metz T.* Ubuntu as a Moral Theory and Human Rights in South Africa // *African Human Rights Law Journal*. — 2011. — Vol. 11. — No. 2. — P. 532—559.
20. *Mokgoro Y.* Ubuntu and the Law in South Africa // *Ubuntu and the Law: African Ideals and Post-Apartheid Jurisprudence* / ed. by C. Drucilla, M. Nyoko. — New York : Fordham University Press, 2012. — P. 317—323.
21. *Moosa E.* Tensions in Legal and Religious Values in the 1996 South African Constitution // *Beyond Rights Talk and Culture Talk: Comparative Essays on the Politics of Rights and Culture* / ed. by M. Mamdani. — Cape Town : David Phillip Publishers, 2000. — P. 121—135.
22. *Ndlovu-Gatsheni S. J.* Decoloniality as the Future of Africa // *History Compass*. — 2015. — Vol. 13. — No. 10. — P. 485—496.
23. *Nkosi S.* Ubuntu and South African Law: Its Juridical Transformative Impact // *Southern African Public Law*. — 2018. — Vol. 33. — No. 1. — P. 1—20.
24. *Radebe S. B., Phooko M. R.* Ubuntu and the Law in South Africa: Exploring and Understanding the Substantive Content of Ubuntu // *South African Journal of Philosophy*. — 2017. — Vol. 36. — No. 2. — P. 239—251.
25. *Rautenbach C.* Exploring the Contribution of Ubuntu in Constitutional Adjudication — Towards the Indigenization of Constitutionalism in South Africa? // ed. C. Fombad *Constitutional Adjudication in Africa*. — Oxford : Oxford University Press, 2017. — P. 293—312.
26. *Sesanti S.* The Exclusion of Ubuntu from South Africa's Constitution: Implications for Pan-Africanism and Violent 'Xenophobia' // *African Studies*. — 2025. — Vol. 84. — No. 3. — P. 191—207.



**Ирина Сергеевна
ПЛАТИЦЫНА,**

генеральный директор
ООО «Персонал М»

smolich08@mail.ru

109651, Россия, г. Москва,
Батайский проезд, д. 35



**Юрий Григорьевич
ШПАКОВСКИЙ,**

профессор кафедры
экологического
и природоресурсного права
Университета имени
О.Е. Кутафина (МГЮА),
доктор юридических наук,

профессор

yurii-rags@yandex.ru

125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

Искусственный интеллект: экономические и правовые аспекты инноваций в эпоху цифровой трансформации Большой Евразии¹

Аннотация. В Послании Федеральному Собранию в феврале 2024 г. Президент Российской Федерации особо остановился на необходимости достижения технологического суверенитета в сквозных сферах, которые обеспечивают устойчивость всей экономики страны. В этих условиях большое научное значение и актуальность имеет трансформация цифровизации России, ЕАЭС на основе ускоренного внедрения технологий искусственного интеллекта.

Авторы статьи акцентируют внимание на том, что интенсивная цифровая трансформация актуализирует потребность в формировании институциональной среды и стандартов, регламентирующих разработку и имплементацию цифровых решений. Особое внимание уделяется стратегической значимости технологий искусственного интеллекта, которые в условиях геополитической нестабильности и санкционного давления трансформируются в ключевой инструмент поддержания экономического суверенитета и национальной безопасности.

В статье анализируется современный этап развития искусственного интеллекта. Особое внимание уделяется цифровой трансформации промышленности в лидирующих в этой области странах (США, Германии, Китае) и России. Изучаются государственная политика США, Китая и России в сфере искусственного интеллекта, а также правовые вызовы регулирования результатов интеллектуальной деятельности, созданных с помощью искусственного интеллекта, и необходимость адаптации правовых институтов без их радикального слома.

Ключевые слова: искусственный интеллект, Большая Евразия, цифровая трансформация, ЕАЭС, правовое регулирование ИИ, национальные стратегии ИИ, санкционное давление

DOI: 10.17803/2311-5998.2026.142.6.170-180

Irina S. PLATITSYNA,

General Director of LLC "Personnel M"

smolich08@mail.ru

35, Bataysky proyezd, Moscow, Russia, 109651

Yuri G. SHPAKOVSKII,

Professor, Ecological and

Natural Resources Law Department of the

Kutafin Moscow State Law University (MSAL),

Dr. Sci. (Law), Professor

yurii-rags@yandex.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

**Artificial Intelligence:
Economic and Legal Aspects of Innovation
in the Era of Digital Transformation in Greater Eurasia**

Abstract. *In his Address to the Federal Assembly in February 2024, the President of the Russian Federation emphasized the need to achieve technological sovereignty in cross-cutting areas that ensure the sustainability of the entire country's economy. In this context, the transformation of Russia's and the EAEU's digitalization based on the accelerated implementation of artificial intelligence technologies holds significant scientific importance and relevance.*

The authors of the article emphasize that intensive digital transformation highlights the need to create an institutional environment and standards that regulate the development and implementation of digital solutions. Special attention is paid to the strategic importance of artificial intelligence technologies, which are transforming into a key tool for maintaining economic sovereignty and national security in the context of geopolitical instability and sanctions pressure.

The article analyzes the current stage of artificial intelligence development. Special attention is paid to the digital transformation of industry in leading countries (the United States, Germany, and China) and Russia. The study examines the state policies of the United States, China, and Russia in the field of artificial intelligence, as well as the legal challenges of regulating the results of intellectual activity created using artificial intelligence and the need to adapt legal institutions without radically changing them.

Keywords: *artificial intelligence, Greater Eurasia, digital transformation, EAEU, legal regulation of AI, national AI strategies, and sanctions pressure.*

Прогресс невозможен без изменений, и те,
кто не способен изменить свои взгляды,
не могут изменить ничего.

Джордж Бернард Шоу

Сегодня можно констатировать, что искусственный интеллект (ИИ) окончательно перешел из технологической повестки в сферу «большой политики». Почему с уверенностью можно об этом говорить? Искусственный интеллект играет все более важную роль в различных сферах нашей жизни, но его влияние уже не ограничивается отдельными областями. Развитие ИИ имеет значительные последствия для глобального порядка и международных отношений. Фундаментальная трансформация системы международных отношений под влиянием ИИ обостряет противоречие между технологическим развитием и глобальной стабильностью.

Сегодня о проблемах развития ИИ мы говорим исключительно в контексте цифровизации. Хотя цифровизация и искусственный интеллект — два тесно связанных, но не тождественных понятия, в современном мире ИИ становится ключевым инструментом и ускорителем цифровой трансформации.

В 2024 г. Генеральная Ассамблея ООН приняла первую резолюцию о регулировании ИИ. В Резолюции содержится призыв «преодолеть разрыв в сфере искусственного интеллекта и иных цифровых технологий между странами и в них», а также обеспечивать равный и справедливый доступ к преимуществам цифровой трансформации и безопасных систем ИИ².

Но реально ли в современном мире выстроить справедливую и равноправную модель развития ИИ, когда 90 % всех ИИ-мощностей сконцентрированы в США и Китае? В этих условиях глобальные факторы развития технологий ИИ становятся предметом пристального внимания исследователей и политиков. Особенно актуальным является выявление объективных предпосылок формирования глобального управления развитием ИИ в странах Большой Евразии, а главное — противостоять растущему влиянию на развитие данной сферы США и Европейского Союза.

Важно отметить, что в современном мире этап развития технологий, связанный с ИИ, характеризуется беспрецедентной скоростью изменений: распространение ИИ в мире во второй половине 2025 г. охватило 16,3 % населения (в разных странах доля варьируется от 5,1 до 64 %³).

Ведущие мировые державы и корпорации активно трансформируют промышленность, переходя от традиционного производства к интеллектуальным системам.

Каждые несколько месяцев появляются языковые модели, значительно превосходящие предыдущие версии по возможностям: можно привести в пример переход от Claude Opus 4.7 к Claude Opus 4.8 (Anthropic, май 2026), выпуск MAI-Thinking-1 (Microsoft, июнь 2026), Gemini 3.5 Flash (Google), а также очередные

² URL: <https://new.ras.ru/press-center/pervuyu-rezolyutsiyu-o-regulirovanii-iskusstvennogo-intellekta-prinyala-generalnaya-assambleya-onn/> (дата обращения: 09.07.2026).

³ URL: https://www.rbc.ru/technology_and_media/25/01/2026/696f789f9a7947d7f698bcd0 (дата обращения: 25.06.2026).

итерации GPT-5.x (OpenAI). Это заставляет компании и государства ускорять инвестиции в инфраструктуру и кадры. В результате способность быстро адаптироваться и направлять развитие ИИ в устойчивое русло превратится в ближайшие годы в ключевое конкурентное преимущество для стран и бизнеса.

На государственном уровне подобный подход к ускоренному внедрению ИИ в производственный сектор активно поддерживается в США. Хотя китайские компании, работающие в высокотехнологической отрасли, заметно усилили конкуренцию с американскими, однако первенство в мировой технологической сфере по-прежнему удерживают Соединенные Штаты. Благодаря этому они могут сами решать, кому, на каких условиях и в каком объеме передавать собственные разработки, а также оказывать влияние на международные информационные потоки. В результате большие языковые модели, созданные крупнейшими IT-корпорациями США, распространяются все шире⁴.

В США рассматривают ИИ прежде всего как геополитическую гонку с Китаем. При этом политика в сфере ИИ строится на трех ключевых принципах: максимальное ускорение развития американского искусственного интеллекта, минимальное государственное регулирование, в частности на уровне штатов, и идеологическая нейтральность ИИ в государственном секторе. В основе президентской политики лежит ряд основополагающих документов, основным из которых является *Winning the Race: America's AI Action Plan* (White House, 2025) — стратегический план, который определил вектор развития американского ИИ на ближайшие годы. Документ опирается на три ключевых столпа: максимальное ускорение инноваций путем снятия регуляторных барьеров (*Accelerate AI Innovation, Build*), масштабное строительство дата-центров и энергетической инфраструктуры (*American AI Infrastructure*) и лидерство в международной дипломатии и безопасности в сфере ИИ (*Lead in International AI Diplomacy and Security*), в том числе продвижение американских стандартов на международной арене и противодействие технологическому доминированию Китая⁵.

Другим важным документом стал Указ “*Preventing Woke AI in the Federal Government*” (Trump, 2025), который ввел идеологический критерий в государственные закупки ИИ. Согласно этому документу, федеральные органы могут приобретать только те модели больших языковых моделей (LLM), которые соответствуют принципам идеологической нейтральности⁶. Этот Указ стал первым случаем, когда идеологическая ориентация ИИ-моделей была напрямую закреплена как критерий государственной политики США.

⁴ Панцеров К. А. Технологии искусственного интеллекта как основа обеспечения технологического суверенитета: вызовы и угрозы для стран ЕАЭС // Евразийская интеграция: экономика, право, политика. 2026. Т. 20. № 2.

⁵ White House. (2025). *Winning the Race: America's AI Action Plan*. July 2025 // URL: <https://www.whitehouse.gov/wp-content/uploads/2025/07/americas-ai-action-plan.pdf> (дата обращения: 17.06.2026).

⁶ Trump D. J. Executive Order 14319 — *Preventing Woke AI in the Federal Government*, July 23, 2025 // Federal Register. 2025. Vol. 90. No. 142. P. 35389—35391. URL: <https://www.federalregister.gov/documents/2025/07/28/2025-14217/preventing-woke-ai-in-the-federal-government> (дата обращения: 17.06.2026).

Главная стратегическая цель — обеспечить безусловное технологическое и экономическое доминирование США в мире. За счет осуществления масштабных инвестиций в интеграцию ИИ в реальные сектора экономики происходит быстрая трансформация целых отраслей — от медицины и производства до экологии и образования. Многие корпорации перекраивают свои производства, делая ИИ главным вектором своих инвестиций.

В КНР приоритетом высшего уровня выступает развитие воплощенного искусственного интеллекта (embodied AI) и антропоморфной робототехники. Главным стратегическим документом в этой области стали Мнения Государственного совета КНР об углубленной реализации инициативы «Искусственный интеллект+». Документ определяет AI+ как ключевой механизм формирования «новых качественных производительных сил» и ставит задачу обеспечить широкомасштабную интеграцию искусственного интеллекта с реальной экономикой, особенно в промышленном секторе⁷.

В рамках этой стратегии Китай активно стимулирует разработку и внедрение человекоподобных (humanoid) роботов, рассматривая их как ключевой элемент будущей интеллектуальной производственной системы. Основной целью является глубокая интеграция ИИ с шестью приоритетными отраслями. Согласно официальному документу, уровень интеграции ИИ должен превысить 70 % к 2027 г., 90 % к 2030 г., а к 2035 г. — завершиться полным формированием «интеллектуальной экономики и общества»⁸.

В России государственная повестка сфокусирована на системном внедрении генеративного ИИ и автономных платформ в промышленность, сельское хозяйство, энергетику и логистику. Данный процесс демонстрирует значительную динамику и охватывает как ведущие технологические компании, так и крупные промышленные предприятия, способствуя цифровой трансформации реального сектора экономики.

Как подчеркнул Президент России В. В. Путин, «искусственный интеллект наряду с цифровыми платформами и автономными системами формирует принципиально иной облик экономики, общественных отношений, социальной сферы, образования, здравоохранения, логистики и промышленности, обороны и безопасности»⁹. Он отметил необходимость «фронтального внедрения» ИИ во всех ключевых отраслях, включая производство, логистику, энергетику, управление и образование, поставив задачу сформировать национальный план внедрения генеративного искусственного интеллекта на уровне всей страны к 2030 г.¹⁰

⁷ Государственный совет КНР. (2025). Постановление № 11 «Об углубленной реализации инициативы “Искусственный интеллект+”» // Официальный сайт Центрального народного правительства КНР. URL: <http://www.gov.cn> (дата обращения: 20.06.2026).

⁸ Министерство промышленности и информационных технологий КНР (MIIT). (2026). Action Plan for Deep Integration of Artificial Intelligence with Key Industries.

⁹ Путин В. В. Выступление на заседании Совета по развитию искусственного интеллекта при Президенте Российской Федерации (2025—2026) // Официальный сайт Президента России. URL: <http://kremlin.ru/events/president/news> (дата обращения: 20.06.2026).

¹⁰ Путин В. В. Поручения и выступления по национальным целям развития искусственного интеллекта (2025—2026) // Официальный сайт Президента Российской Федерации. URL: <http://kremlin.ru>.

Такие установки задают стратегический вектор цифровой трансформации российской экономики и подчеркивают приоритетность широкого внедрения ИИ в реальном секторе.

Ключевыми игроками на этом направлении выступают «Сбер» и «Яндекс», которые разрабатывают и внедряют промышленные ИИ-решения в партнерстве с крупными предприятиями. «Сбер» активно продвигает GigaChat и платформу ZIIoT (совместно с ГК «Цифра»), создавая ИИ-агентов для оптимизации производства, предиктивного обслуживания оборудования и управления технологическими процессами¹¹.

«Яндекс» развивает YandexGPT и платформу AI Studio, позволяющие создавать промышленных агентов. Эти решения уже применяются в компаниях «Норникель», «Газпром нефть» и других для анализа данных, прогнозирования и оптимизации технологических режимов¹².

Значительный вклад вносит компания Cognitive Pilot («Когнитив Роботикс»), разрабатывающая системы автономного управления на базе ИИ для сельскохозяйственной и промышленной техники, включая беспилотные роботы-тягачи и обходчики¹³.

Крупные промышленные холдинги, такие как «Русал», «Норникель», «ЕвроХим» и «Северсталь», активно внедряют машинное зрение, предиктивную аналитику и генеративный ИИ для повышения эффективности производства и снижения издержек¹⁴.

Реализация этих инициатив осуществляется в рамках Национальной стратегии развития искусственного интеллекта на период до 2030 года, утвержденной Указом Президента РФ от 10.10.2019 № 490¹⁵. Стратегия направлена на достижение устойчивой конкурентоспособности российской экономики, обеспечение лидирующих позиций в мире по отдельным направлениям ИИ, укрепление национальной безопасности и рост благосостояния населения¹⁶.

Ключевыми целевыми показателями Стратегии к 2030 г. являются: рост совокупной производительности отечественных ИИ-суперкомпьютеров до 1 эксафлопса, совокупный прирост ВВП за счет ИИ — не менее 11,2 трлн рублей

¹¹ Промышленная платформа ZIIoT на базе GigaChat (2026) // Официальный сайт Сбера. URL: <https://www.sber.ru> (дата обращения: 20.06.2026).

¹² YandexGPT и AI Studio для промышленности. Корпоративные кейсы («Норникель», «Газпром нефть») (2026) // URL: yandex.ru/company/ai.

¹³ Cognitive Pilot. (2026). Автономные системы управления на базе ИИ // URL: cognitivepilot.com.

¹⁴ «Русал», «Норникель», «ЕвроХим», «Северсталь». Корпоративные отчеты по цифровизации и внедрению ИИ (машинное зрение, предиктивная аналитика). (2025—2026). Разделы Sustainability (Digital Transformation на официальных сайтах компаний).

¹⁵ Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (ред. от 15.02.2024) // Официальный интернет-портал правовой информации. URL: <http://publication.pravo.gov.ru/document/0001201910100035> (дата обращения: 17.06.2026).

¹⁶ Национальная стратегия развития искусственного интеллекта на период до 2030 года (обновленная редакция) // URL: government.ru или ai.gov.ru.

(накопленным итогом), а также увеличение объема рынка услуг в сфере ИИ до 60 млрд рублей в год. Стратегия акцентирует внимание на развитии отечественной инфраструктуры, подготовке кадров, создании доверенных ИИ-решений и стимулировании внедрения технологий в приоритетных отраслях, включая промышленность и энергетику¹⁷.

Таким образом, глобальная трансформация производства на базе ИИ кардинально меняет мировую промышленность, вовлекая в этот процесс как лидеров мирового рынка, так и российские предприятия, что в конечном итоге укрепляет конкурентные позиции отечественного производства.

Стремительное развитие технологий искусственного интеллекта обнажает серьезные проблемы правового регулирования. Законодательная база во многих странах, включая Россию, существенно отстает от реальной скорости технологического прогресса. Ключевыми вызовами остаются вопросы ответственности за действия ИИ, определение правового статуса генерируемого контента, защита авторских прав при обучении моделей на больших массивах данных, а также борьба с deepfake, дискриминацией и иными рисками. В условиях, когда ИИ все чаще принимает решения с минимальным участием человека, отсутствие четких правовых механизмов создает значительную правовую неопределенность и повышает риски как для бизнеса, так и для общества в целом.

На глобальном уровне основными вопросами остаются ответственность за действия ИИ-систем, защита интеллектуальной собственности, кибербезопасность и предотвращение дискриминации.

Одним из первых в мире всеобъемлющих и системных нормативных актов, регулирующих сферу искусственного интеллекта, стал AI Act (Regulation (EU) 2024/1689) Европейского союза. Закон был принят в 2024 г. и полностью вступил в силу в 2026 г. Европейский AI Act вводит первый в мире комплексный риск-ориентированный подход к регулированию искусственного интеллекта. В зависимости от уровня потенциального риска все ИИ-системы разделены на несколько категорий: от минимальных требований для низкорисковых приложений (например, спам-фильтры) до строгих обязательных норм для высокорисковых систем. Особо жесткое регулирование применяется к ИИ, используемому в критически важных областях — промышленности, энергетике, транспорте, медицине и сфере занятости.

Для таких систем предусмотрены обязательные процедуры: независимый аудит, обеспечение прозрачности алгоритмов, ведение подробной технической документации, проведение оценки влияния на права человека, а также сохранение значимого человеческого контроля над принятием решений. Нарушение требований AI Act влечет серьезные штрафы — до 35 млн евро или 7 % от глобального годового оборота компании¹⁸.

¹⁷ Минэкономразвития РФ, Минцифры РФ (2026). Доклады о ходе реализации Национальной стратегии ИИ.

¹⁸ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. L series. 2024. № 1689. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата обращения: 17.06.2026).

В отличие от жесткого и комплексного AI Act в ЕС, в США федеральное регулирование ИИ остается минимальным и носит фрагментарный характер.

Нынешняя администрация США сознательно выбрала стратегию максимального ускорения развития ИИ при минимальном государственном вмешательстве. При этом ярко выраженный либерально-ускоряющий подход к регулированию ИИ в США принципиально отличается от риск-ориентированной модели Европейского союза. Государство сознательно минимизирует регуляторную нагрузку, рассматривая искусственный интеллект в первую очередь как инструмент геополитической и экономической конкуренции с Китаем.

На федеральном уровне в США отсутствует единый комплексный закон об искусственном интеллекте. Регулирование искусственного интеллекта в США на федеральном уровне осуществляется преимущественно в секторальном формате. Оно реализуется через отдельные нормативные акты и отраслевые стандарты в ключевых сферах, таких как здравоохранение, транспорт, национальная оборона и финансовый сектор. При этом вопросы ответственности за действия ИИ-систем регулируются в основном общими нормами гражданского и уголовного права. Компании-разработчики и операторы несут ответственность за предсказуемый вред, причиненный использованием их технологий.

Китай также одним из первых в мире внедрил специализированное нормативное регулирование генеративного искусственного интеллекта. Основные нормативные акты в данной сфере устанавливают строгие требования к содержанию и обязательной маркировке материалов, созданных с помощью генеративного ИИ.

Согласно утвержденным в 2023 г. правовым актам — Временным мерам по управлению услугами генеративного искусственного интеллекта (Interim Measures for the Management of Generative Artificial Intelligence Services)¹⁹ и Положению об управлении технологиями глубинного синтеза (Regulation on the Management of Deep Synthesis Technology)²⁰ — провайдеры сервисов обязаны не только осуществлять обязательную маркировку всего генерируемого контента, применяя при этом различные «водяные знаки», но и внедрять системы обнаружения и блокирования генерации запрещенного контента, включая политически чувствительную информацию, а также вести учет данных обучения и пользовательских запросов для целей последующего государственного контроля. При этом особое внимание в регулировании уделяется обеспечению соответствия контента социалистическим ценностям и предотвращению распространения информации, представляющей угрозу национальной безопасности и общественной стабильности.

Таким образом, китайская модель правового регулирования искусственного интеллекта носит ярко выраженный контент-ориентированный и государственно-контролирующий характер, существенно отличающийся как от риск-ориентированного

¹⁹ Interim Measures for the Management of Generative Artificial Intelligence Services (2023) // Cyberspace Administration of China. URL: http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm (дата обращения: 17.06.2026).

²⁰ Regulation on the Management of Deep Synthesis Technology (互联网信息服务深度合成管理规定), 2022 // Cyberspace Administration of China. URL: http://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm (дата обращения: 17.06.2026).

подхода Европейского союза, так и от либерального, инновационно-ориентированного подхода США.

В России правовое регулирование искусственного интеллекта носит фрагментарный развивающийся характер. Основным стратегическим документом остается Национальная стратегия развития искусственного интеллекта на период до 2030 года.

На законодательном уровне в настоящее время действуют:

- Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (так называемых регуляторных песочницах)²¹;
- Федеральный закон от 2024 г. № 498-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам искусственного интеллекта», который вводит отдельные нормы об ответственности и обязательной маркировке ИИ-генерируемого контента²².

В 2026 г. находится в стадии активной разработки и общественного обсуждения проект федерального закона «Об искусственном интеллекте». В нем предполагается урегулировать ключевые вопросы, включая ответственность за вред, причиненный ИИ, правовой статус результатов генерации ИИ, а также защиту авторских прав при использовании произведений для обучения моделей²³.

Указом Президента РФ от 26.02.2026 № 116 создана Комиссия при Президенте Российской Федерации по вопросам развития технологий искусственного интеллекта. Ее цель — координация деятельности федеральных органов государственной власти, Банка России, органов государственной власти субъектов РФ, иных государственных органов и заинтересованных организаций по вопросам разработки согласованных подходов к формированию и реализации государственной политики в области создания, развития и внедрения технологий искусственного интеллекта.

Что касается позиции ведущих российских правоведов, то они демонстрируют высокую степень единства по фундаментальному вопросу правового статуса результатов искусственного интеллекта. Большинство экспертов²⁴ сходятся во мнении, что цифровые объекты, включая результаты работы ИИ, должны обладать особым правовым режимом в системе гражданского права, сопоставимым с уже существующими категориями объектов — вещными, обязательственными,

²¹ СПС «КонсультантПлюс».

²² СПС «КонсультантПлюс».

²³ Проект федерального закона «Об искусственном интеллекте» (по состоянию на 2026 г.).

²⁴ См., например: *Близнец И. А.* Интеллектуальная собственность и искусственный интеллект: проблемы и перспективы правового регулирования // Интеллектуальная собственность. Авторское право и смежные права. 2025. № 4. С. 12—18; *Бевзенко Р. С.* Цифровые объекты гражданских прав: проблемы квалификации и правового режима // Вестник гражданского права. 2025. № 2. С. 45—67; *Серго А. Г.* Искусственный интеллект и гражданское право: перспективы развития законодательства // Журнал российского права. 2025. № 4. С. 78—92; *Новоселова Л. А.* Конфликт интересов авторов и разработчиков ИИ: где выход? // Журнал Суда по интеллектуальным правам. 2025. № 4 (50). С. 41—49.

корпоративными или интеллектуальными правами²⁵. На сегодняшний день полноценный правовой режим для таких объектов в российском законодательстве отсутствует.

Таким образом, в российской правовой доктрине преобладает подход, направленный не на создание новых субъектов права, а на формирование полноценного специального правового режима для цифровых объектов в рамках действующей системы гражданского законодательства²⁶.

Может ли Евразия стать единой цифровой экосистемой? На сегодняшний день санкционная политика, которую проводит коллективный Запад, вызывает геоэкономическое расслоение и ослабляет связность евразийского пространства. Одним из вариантов ответа на этот вызов может быть объединение «Цифровой шелковый путь» с цифровыми инициативами ЕАЭС, что позволит повысить технологическую устойчивость Евразии.

Идея формирования общей цифровой экосистемы Большой Евразии действительно имеет широкий размах, но на практике это не один готовый проект, а набор разрозненных инициатив и процессов, которые по мере развития постепенно объединяются в единую систему.

По мнению авторов, в условиях мировой цифровой трансформации, ускоренного внедрения ИИ-технологий во все сферы жизни требуется формирование особых правовых инструментов. Это объективно приобретает стратегическое значение для технологической независимости страны и ее устойчивого развития. Частично эти вопросы нашли отражение в Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года, утвержденных решением Высшего Евразийского экономического совета от 11.10.2017 № 12.

Формирование глобального цифрового управления, в том числе регулирование развития искусственного интеллекта в странах Большой Евразии, будет определяться не только темпами технологического прогресса и объемом инвестиций, но и способностью правовых систем каждого государства региона эффективно адаптироваться к новым вызовам. При этом важно обеспечивать баланс между защитой прав человека, экономической стабильностью и повышением национальной конкурентоспособности.

БИБЛИОГРАФИЯ

1. Бевзенко Р. С. Цифровые объекты гражданских прав: проблемы квалификации и правового режима // Вестник гражданского права. — 2025. — № 2. — С. 45—67.
2. Блинец И. А. Интеллектуальная собственность и искусственный интеллект: проблемы и перспективы правового регулирования // Интеллектуальная собственность. Авторское право и смежные права. — 2025. — № 4. — С. 12—18.

²⁵ Новоселова Л. А. Правовые проблемы использования искусственного интеллекта // Материалы круглого стола. М. : МГУ имени М.В.Ломоносова, 2025.

²⁶ Серго А. Г. Указ. соч.

3. Новоселова Л. А. Правовые проблемы использования искусственного интеллекта // Материалы круглого стола. — М. : МГУ имени М.В.Ломоносова, 2025.
4. Панцеров К. А. Технологии искусственного интеллекта как основа обеспечения технологического суверенитета: вызовы и угрозы для стран ЕАЭС // Евразийская интеграция: экономика, право, политика. — 2026. — Т. 20. — № 2.
5. Серго А. Г. Искусственный интеллект и гражданское право: перспективы развития законодательства // Журнал российского права. — 2025. — № 4. — С. 78—92.

Семейные ценности в цифровой среде: проблемы и гарантии правовой защиты

Аннотация. Статья посвящена актуальным проблемам правовой защиты традиционных семейных ценностей в условиях трансформации цифровой среды под воздействием алгоритмов. Традиционный подход, основанный на ограничении доступа к противоправному контенту, недостаточен в ситуации гиперперсонализации, «информационных пузырей» и «эхо-камер».

В работе выявляются концептуальные противоречия между требованием прозрачности алгоритмов и охраной коммерческой тайны, а также недостатки процедурного подхода к регулированию рекомендательных технологий. Критическому осмыслению подвергается доктрина ценностно-нейтральности алгоритмов.

На основе изучения зарубежных концепций (Value Sensitive Design, «позитивные вычисления», RecSoGood) и анализа существующих технических решений (Tournesol.app, YouChoose.ai) сформулированы предложение по формированию комплексного правового института регулирования рекомендательных технологий. В качестве перспективного механизма предлагается внедрение созидательных рекомендательных технологий, включая инструменты алгоритмического перехвата и эмуляции контента, что позволит сместить акцент с ограничения доступа на ценностно ориентированное управление алгоритмическими потоками.

Ключевые слова: семейные ценности, традиционные ценности, рекомендательные технологии, рекомендательные системы, цифровая среда, правовое регулирование рекомендательных технологий, информационный пузырь, эхо-камера, созидательные технологии, ценностно ориентированное проектирование, национальная безопасность, персонализация контента, искусственный интеллект, цифровое профилирование



**Анастасия
Вячеславовна
НИКИШИНА,**

аспирант кафедры
информационного права
и цифровых технологий
Университета имени
О.Е. Кутафина (МГЮА)
s2043051@edu.msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2026.142.6.181-189

Anastasia V. NIKISHINA,

Postgraduate student, Department of Information Law and Digital Technologies
of the Kutafin Moscow State Law University (MSAL)

s2043051@edu.msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Family Values in the Digital Environment: Problems and Guarantees of Legal Protection

Abstract. This article addresses the current challenges of legally protecting traditional family values amidst the transformation of the digital environment driven by algorithms. It substantiates the thesis that the traditional approach — based solely on restricting access to illegal content — is insufficient

© Никишина А. В., 2026

when confronted with such digital reality phenomena as hyper-personalization, «filter bubbles», and «echo chambers», which are shaped by recommender technologies.

Drawing on foreign concepts (Value Sensitive Design, «positive computing», RecSoGood) and an analysis of existing technical solutions (Tournesol.app, YouChoose.ai), this article formulates proposals for developing a comprehensive legal framework for the regulation of recommender technologies. As a promising mechanism, it suggests the implementation of «constructive recommender technologies», including tools for «algorithmic interception» and content emulation. This would shift the focus from access restriction to value-oriented management of algorithmic streams.

Keywords: family values, traditional values, recommender technologies, recommender systems, digital environment, legal regulation of recommender technologies, filter bubble, echo chamber, constructive technologies, value-sensitive design, national security, content personalization, artificial intelligence, digital profiling

В настоящее время к информации, отрицающей традиционные ценности, можно отнести информацию, формирующую неуважение к родителям и (или) другим членам семьи (п. 4 ч. 1 ст. 5 Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»), информацию, пропагандирующую нетрадиционные сексуальные отношения и (или) предпочтения, педофилию, смену пола, отказ от деторождения (п. «л» ч. 5 ст. 15.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации)).

Семья, будучи первичной и фундаментальной ячейкой общества, представляет собой один из ключевых объектов нормативного регулирования. Современный этап развития правовой системы характеризуется переосмыслением роли семьи: из института частной жизни она трансформировалась в стратегический ресурс национальной безопасности.

Правовое закрепление защиты семейных ценностей отражает не только текущие социальные запросы, но и долгосрочные цели государства по сбережению нации и обеспечению суверенитета. В последние годы наблюдается интенсивное развитие законодательства, направленного на защиту и продвижение традиционных семейных ценностей в Российской Федерации.

Несмотря на признание важности традиционных семейных ценностей в Указе Президента РФ от 09.11.2022 № 809¹, в законодательстве остается нерешенным ряд проблем. Ограничение доступа к информации помогает устранить противоправный контент в информационном поле. Однако динамика распространения информации и ее алгоритмическая персонализация создают ситуацию, при

¹ Указ Президента РФ от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» // СЗ РФ. 2022. № 46. Ст. 7977.

которой традиционные методы блокировки становятся недостаточно эффективными. В научном сообществе все чаще встречаются дискуссии о необходимости замещения удаленного контента «позитивным»².

Современные цифровые платформы являются не просто сервисами развлечения и коммуникации, а инструментами управления, конструирования социальной реальности и коммерциализации человеческого внимания. Их коммерческая модель, основанная на экономике внимания, привела к тому, что большинство рекомендательных систем (РС) оптимизированы исключительно для удержания внимания пользователя. При этом механизмы работы этих систем, как правило, остаются закрытыми³. За последние десятилетия рекомендательные системы эволюционировали к гиперперсонализированным моделям на базе ИИ, нейросетей и гибридных методов фильтрации, обрабатывая в реальном времени большие данные, включая информацию с устройств IoT. Сегодня явно наблюдается тенденция трансформации публичного пространства под влиянием алгоритмов. С правовой точки зрения феномены «эхо-камер» и «информационных пузырей» остаются не до конца изученными.

«Информационный пузырь», на наш взгляд, следует рассматривать как ограничение прав субъекта на доступ к информации. Данное состояние характеризуется пассивной неполнотой информации. С. Нгуен разграничивает «эхо-камеры» и «информационные пузыри»: последние — это эпистемические структуры, ограничивающие доступ к информации через «упущение» (пользователь видит только узкий круг источников, формируемый как его действиями, так и алгоритмами)⁴. Вместе с тем «информационный пузырь» может быть разрушен при условии, что пользователь тем или иным способом все же сталкивается с иной информацией. «Эхо-камеры» же представляют собой «эпистемическое сообщество», члены которого не только разделяют единые убеждения на основе усеченного массива данных, но и занимают антагонистическую позицию по отношению к внешним носителям иных взглядов, систематически дискредитируя⁵.

Следовательно, юридически значимым признаком является наличие или отсутствие внешненаправленного действия. Неосведомленность субъекта об

² См.: Друкер М. М. Создание положительного контента социальных медиа как инструмент формирования ценностных ориентиров современных подростков // Вестник Волжского университета имени В. Н. Татищева. 2020. № 2. Т. 2. С. 145—151 ; Шагина Е. С. Формирование позитивного контента в социальных сетях как форма профилактики экстремизма, проводимая учреждениями дополнительного образования // Государственная молодежная политика: вызовы и современные технологии работы с молодежью. Дискуссионная площадка «Социальные девиации молодежи: проявления, динамика, профилактика». 2021. С. 332—337.

³ Naudts L., Helberger N., Veale M., Sax M. A Right to Constructive Optimization: A Public Interest Approach to Recommender Systems in the Digital Services Act // Journal of Consumer Policy. 2025. № 48. P. 269—296.

⁴ Nguyen C. T. (2020). Echo Chambers and Epistemic Bubbles // Episteme. 17(2). 2018. P. 145.

⁵ Нумяев Э. А. Роль цифровых рекомендательных алгоритмов в распространении религиозных фундаменталистских нарративов // Вестник русской христианской гуманитарной академии. 2025. Т. 26. № 3. С. 120—125.



альтернативных точках зрения ставит вопрос о повышении уровня цифровой гигиены в процессе употребления контента. Если алгоритмы платформ создают ситуацию, при которой взгляды, не соответствующие данному сообществу, активно противопоставляются как «свой — чужой», необходимо вырабатывать публично-правовые механизмы регулирования. Согласно Закону об информации противодействие распространению противоправного контента в сети Интернет осуществляется преимущественно посредством ограничения доступа к такой информации.

Таким образом, в настоящее время возрастает необходимость формирования правового инструментария, направленного на минимизацию сопутствующих цифровизации рисков.

По итогам заседания Совета по реализации государственной демографической и семейной политики Президент России поручил представить предложения по внесению в нормативные правовые акты изменений, направленных на популяризацию традиционных семейных ценностей и позитивного образа многодетной семьи в рекламе (п. 5 перечня поручений от 10.02.2026 № Пр-282)⁶. В рамках настоящего исследования предлагается рассмотреть в качестве механизма реализации этой задачи внедрение созидательных рекомендательных технологий, относящихся к мягкой силе регулирования, не прибегая к методам ограничения контента.

При рассмотрении подходов к определению рекомендательных технологий в первую очередь следует обратиться к положениям Закона об информации. В статье 10.2-2 данного Закона под рекомендательными технологиями понимаются информационные технологии, обеспечивающие предоставление информации на основе сбора, систематизации и анализа сведений, отражающих предпочтения пользователей сети Интернет, место нахождения которых ограничено территорией России.

Данное определение акцентирует внимание на процессе обращения с данными, их сборе, систематизации и анализе, упуская прогностическую природу алгоритмов.

Фундаментом для выработки любых рекомендаций выступает интегрированная совокупность знаний системы: о самом пользователе, о поведенческих паттернах других пользователей, а также о структуре всего доступного информационного пространства⁷. Большинство современных рекомендательных систем используют эту накопленную информацию, которую часто называют профилем пользователя, цифровой пользовательской моделью или массивом пользовательских настроек, для формирования итоговой выдачи⁸. Рекомендательные техно-

⁶ Перечень поручений по итогам заседания Совета по реализации государственной демографической и семейной политики // URL: <http://www.kremlin.ru/acts/assignments/orders/79141> (дата обращения: 11.02.2026).

⁷ *Ананьева М. Е.* Разработка подходов к улучшению качества контекстных рекомендательных систем и алгоритмов : дис. ... канд. техн. наук. М., 2025. С. 30—78.

⁸ *Мамай И. Б., Ильин Д. А., Лимонова Е. Е., Путинцев Д. Н.* Системы научных рекомендаций // Международный журнал прикладных и фундаментальных исследований. 2017. № 7. С. 181—184.

логии, являясь набором алгоритмов для принятия решений, осуществляющих предиктивную аналитику пользовательских интересов, позволяют отбирать для пользователей наиболее релевантный контент⁹.

То есть рекомендательные технологии — это модульные программные комплексы, предназначенные для интеграции различных источников данных и методов обработки с целью формирования персонализированных рекомендаций.

Статья 29 Конституции РФ, закрепляющая право свободно искать, получать, передавать, производить и распространять информацию, задает парадигму деятельности цифровых платформ. Рекомендательные алгоритмы фактически совершают все перечисленные действия. Однако с точки зрения реализации конституционных прав субъектом этих действий остается человек (владелец ресурса, разработчик), использующий алгоритм как инструмент. Конституция РФ провозглашает право каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ст. 23), при этом сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ст. 24). Техническая функция алгоритмов напрямую связана со сбором, хранением и использованием информации о пользователях цифровой платформы, применяющей рекомендательные алгоритмы. Таким образом, ограничение на уровне Конституции РФ сбора, хранения, использования и распространения информации о гражданах является правовой основой для ограничения использования рекомендательных технологий.

На отраслевом уровне основополагающим нормативным правовым актом, регламентирующим использование рекомендательных технологий, выступает Закон об информации. Положения ст. 10.2-2 данного Закона закрепляют для владельцев информационных ресурсов, применяющих рекомендательные технологии, комплекс обязанностей. В числе прочего предусматривается обязанность по раскрытию не только видов используемых сведений, касающихся предпочтений пользователей, но также описаний процессов и методов, посредством которых осуществляются сбор, систематизация, анализ и предоставление информации. Данная обязанность противопоставляется правовой охране коммерческой тайны и защите алгоритмов как объектов интеллектуальной собственности, что порождает конфликт между необходимостью обеспечения прозрачности алгоритмов и защиты охраняемой законом информации (ограниченного доступа и (или) охраноспособных результатов интеллектуальной деятельности).

Ключевой особенностью текущего правового регулирования рекомендательных технологий является ориентация на процедурную прозрачность путем формального раскрытия информации об их работе и создания механизмов принуждения. Однако сущность алгоритмического воздействия — динамическое профилирование, эксплуатация когнитивных искажений, адаптация моделей под поведение пользователя — остается за пределами правового регулирования.

Отсутствие законодательно закрепленных критериев алгоритмической безопасности, механизмов независимого аудита, дифференцированных требований к

⁹ Парыгин Д. С., Стрекалова А. С., Гуртяков А. С., Аданья С. Г., Пивоваров В. В. Применение рекомендательных технологий в системах с пространственной информацией // Прикаспийский журнал: управление и высокие технологии. 2019. № 1 (45). С. 97—100.



рекомендательным технологиям в зависимости от сферы применения (например, для разных категорий субъектов, включая несовершеннолетних пользователей) ограничивает эффективность текущего правового регулирования, а использование алгоритмического ранжирования исключительно в коммерческих интересах несет в себе риски для национальной безопасности.

Защита системы ценностей представляет собой не только отражение национальных приоритетов государства, но и ставит задачи по укреплению национальной безопасности страны. Внесенные Законом о поправке к Конституции РФ от 14.03.2020 № 1-ФКЗ¹⁰ положения, возлагающие на Правительство РФ полномочия по сохранению и укреплению традиционных семейных ценностей, определили вектор дальнейшего развития российского законодательства в части укрепления и защиты института семьи.

С точки зрения обеспечения национальной безопасности защита традиционных семейных ценностей согласно Указу Президента РФ от 02.06.2021 № 400¹¹ обеспечивается в том числе путем реализации государственной информационной политики, направленной на усиление в массовом сознании роли традиционных российских духовно-нравственных и культурно-исторических ценностей, неприятие гражданами навязываемых извне деструктивных идей, стереотипов и моделей поведения.

Целесообразно пересмотреть текущее правовое регулирование рекомендательных технологий с точки зрения обеспечения национальной безопасности государства, сместить акцент правового регулирования с постфактумной блокировки контента на превентивное управление алгоритмическими потоками, что требует разработки отечественных подходов к целеполаганию рекомендательных технологий. В этом контексте концепция созидательных технологий обретает не только технологическое, но и публично-правовое измерение.

В международной практике уже существуют примеры созидательной работы алгоритмов. Например, Google при запросе на суицидальную тематику предлагает позвонить по телефону психологической помощи лицам, оказавшимся в трудной жизненной ситуации. Данный механизм можно применять не только в рамках появления сообщений-рекомендаций.

Созидательное использование алгоритмов видится перспективным при поисковом запросе на потенциально деструктивные темы, например, при запросе «Совершение абортов. Срочно!» алгоритмы могут не только предложить психологическую помощь, но и выдавать позитивный контент о материнстве и господдержке.

Важным аспектом персонализации является ИИ-анализ цифровых следов пользователя с целевым подбором в рекомендательной ленте информации о мерах государственной поддержки в той или иной ситуации и текущем семейном статусе (выплаты, льготы, гарантии, государственные услуги и сервисы, меры жилищной и социальной поддержки и др.).

¹⁰ Закон РФ о поправке к Конституции Российской Федерации от 14.03.2020 № 1-ФКЗ // СЗ РФ. 2020. № 11. Ст. 1416.

¹¹ Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (ч. II). Ст. 5351.

Представляется целесообразным рассмотреть на законодательном уровне и в рамках технического регулирования возможность использования инструментов алгоритмического перехвата. Речь идет об отечественных программных решениях (эмуляторах, браузерных расширениях), которые, как промежуточный слой, фильтруют и переранжируют контент зарубежных платформ по отечественным методикам.

Примеры релевантности такого подхода — *Tournesol.app*¹² или *YouChoose.ai*¹³. Практически это означает фильтрацию деструктивного контента и продвижение созидательного на основе государственных методологий.

Анализ современной научной литературы позволяет выделить несколько парадигм использования созидательных рекомендательных технологий.

Концепция проектирования с учетом ценностей (*Value Sensitive Design, VSD*), методологию которой разработали Б. Фридман и П. Кан в конце XX в.¹⁴, требует воплощения ценностей (неприкосновенность частной жизни, честь, достоинство) в архитектуру системы с помощью триединой структуры: концептуальные, эмпирические и технологические исследования (например, как алгоритм искажает восприятие института семьи).

С точки зрения данной концепции конфликт между правом пользователя на защиту конфиденциальной информации о себе и потребностью платформы в коммерциализации контента решается через разработку стандартов. Например, стандарт IEEE 7000-2021¹⁵ устанавливает набор процессов, с помощью которых организации могут включать рассмотрение этических ценностей на всех этапах разработки системы, обеспечивая прослеживаемость этических ценностей через концепцию операций.

Концепция «позитивных вычислений» Р. Кальво и Д. Питерса требует проектировать рекомендательные системы с учетом таких психологических факторов, как: развитие навыков, саморегуляция, просоциальные установки (взаимопомощь, эмпатия)¹⁶.

В контексте рекомендательных алгоритмов исследователи вводят важное различие: переход от гедонического (сиюминутное получение удовольствия, часто низменного) к эвдемоническому (глубоко значимый, развивающий опыт) эффекту рекомендаций. Разработка метрик цифрового благополучия позволяет установить обязанность владельцев информационных ресурсов проводить аудит алгоритмов на предмет их соответствия основополагающим принципам.

¹² Рекомендации по совместному контенту // URL: <https://tournesol.app/> (дата обращения: 14.03.2026).

¹³ Проект *Youchoose* // URL: <https://youchoose.ai/> (дата обращения: 14.03.2026).

¹⁴ См.: *Friedman B., Hendry D. G. Value Sensitive Design: Shaping Technology with Moral Imagination*. MIT Press, 2026.

¹⁵ 7000-2021 — Стандартная модель процесса IEEE для решения этических проблем при проектировании систем // URL: <https://ieeexplore.ieee.org/document/9536679/footnotes#footnotes> (дата обращения: 14.03.2026).

¹⁶ См.: *Rafael A. Calvo, Dorian Peters. Positive Computing: Technology for Wellbeing and Human Potential*. The MIT Press, 2014.



Рассмотренные подходы, несмотря на их различную дисциплинарную принадлежность, формируют единый вектор движения от ценностно нейтрального к ценностно ориентированному развитию технологий, в том числе технологий искусственного интеллекта.

На основе проведенного анализа полагаем целесообразным обозначить следующие перспективы развития информационного законодательства. Закрепленная в Законе об информации модель регулирования прозрачности алгоритмов путем представления отчетности, на наш взгляд, концептуально не охватывает всю сущность нейросетевых алгоритмов, работающих по принципу «черного ящика».

Глобальный тренд перехода от суверенитета над территорией к суверенитету над потоками данных ставит перед государством задачу по совершенствованию мер реагирования на угрозы, порождаемые процессом цифровизации. Алгоритмическая природа распространения контента, характеризующаяся закрытостью метаданных, использованием нейросетевых моделей и эффектами создания «эхо-камер» и «информационных пузырей», нивелирует эффективность традиционных методов ограничения доступа к распространяемому контенту.

Таким образом, гарантии защиты традиционных семейных ценностей в цифровой среде не могут быть обеспечены исключительно мерами по ограничению информации, запрещенной к распространению на территории Российской Федерации.

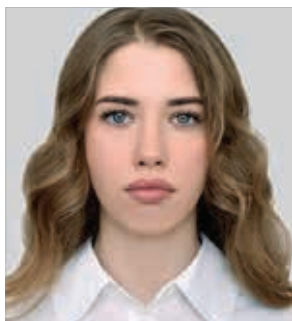
Эффективная защита возможна лишь при условии формирования комплексного правового института регулирования рекомендательных технологий, который обеспечивает не только удаление противоправного контента, но и ценностно ориентированное формирование информационной среды с использованием созидательных рекомендательных технологий, функционирующих в интересах личности, общества и государства.

БИБЛИОГРАФИЯ

1. *Ананьева М. Е.* Разработка подходов к улучшению качества контекстных рекомендательных систем и алгоритмов : дис. ... канд. техн. наук. — М., 2025.
2. *Друкер М. М.* Создание положительного контента социальных медиа как инструмент формирования ценностных ориентиров современных подростков // Вестник Волжского университета имени В. Н. Татищева. — 2020. — № 2. — Т. 2. — С. 145—151.
3. *Мамай И. Б., Ильин Д. А., Лимонова Е. Е., Путинцев Д. Н.* Системы научных рекомендаций // Международный журнал прикладных и фундаментальных исследований. — 2017. — № 7. — С. 181—184.
4. *Парыгин Д. С., Стрекалова А. С., Гуртяков А. С., Адання С. Г., Пивоваров В. В.* Применение рекомендательных технологий в системах с пространственной информацией // Прикаспийский журнал: управление и высокие технологии. — 2019. — № 1 (45). — С. 97—100.
5. *Шагина Е. С.* Формирование позитивного контента в социальных сетях как форма профилактики экстремизма, проводимая учреждениями дополнительного образования // Государственная молодежная политика: вызовы и современ-

- менные технологии работы с молодежью. Дискуссионная площадка «Социальные девиации молодежи: проявления, динамика, профилактика». — М., 2021. — С. 332—337.
6. *Friedman B., Hendry D. G.* Value Sensitive Design: Shaping Technology with Moral Imagination. — MIT Press, 2026. — 500 p.
7. *Naudts L., Helberger N., Veale M., Sax M.* A Right to Constructive Optimization: A Public Interest Approach to Recommender Systems in the Digital Services Act // *Journal of Consumer Policy*. — 2025. — № 48. — P. 269—296.
8. *Nguyen C. T.* (2020). Echo Chambers and Epistemic Bubbles // *Episteme*. — 17 (2). — 2018.
9. *Rafael A. Calvo, Dorian Peters.* Positive Computing: Technology for Wellbeing and Human Potential. — The MIT Press, 2014. — 288 p.





**Вероника
Александровна
НОСОВА,**

аспирант Университета
имени О.Е. Кутафина
(МГЮА)

veron.nosova17@yandex.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

Публично-правовое стимулирование развития отрасли информационных технологий как инструмент обеспечения технологического суверенитета

Аннотация. В статье исследуется публично-правовой механизм стимулирования развития ИТ-отрасли в Российской Федерации как инструмент обеспечения технологического суверенитета и достижения технологического лидерства. На основе анализа нормативных актов и эмпирических данных за 2022—2025 гг. выявлено противоречие между формальными индикаторами импортозамещения и фактическим уровнем технологической независимости. Исследована трансформация механизма стимулирования развития ИТ-отрасли, осуществляемого посредством принятия новых федеральных законов, ужесточения правил ИТ-аккредитации и переориентации грантовой политики. Проведен сравнительный анализ российского механизма с моделями КНР и Индии. Предложена трехуровневая модель оценки отечественности ПО (формальный, функциональный и структурный). **Ключевые слова:** информационные технологии, технологический суверенитет, технологическое лидерство, публично-правовой механизм, стимулирование развития, отрасль информационных технологий

DOI: 10.17803/2311-5998.2026.142.6.190-196

Veronika A. NOSOVA,

Postgraduate student of the Kutafin Moscow State Law University (MSAL)

veron.nosova17@yandex.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Public Law Incentives for the Development of the Information Technology Industry as Instrument for Ensuring Technological Sovereignty

Abstract. The article examines the public law mechanism for stimulating the development of the IT industry in Russia as an instrument for ensuring technological sovereignty and achieving technological leadership. Based on the analysis of normative legal acts and empirical data for 2022—2025, a contradiction is identified between formal indicators of import substitution and the actual level of technological independence. The legal nature of the transformation on the public law mechanism for incentivizing IT industry development is examined, carried out through the adoption of new federal laws, the tightening of IT accreditation rules, and reorientation of grant policy. A comparative analysis of the Russian mechanism with the models of China and India is conducted. A three-tier model for assessing software domesticity (formal, functional, and structural) is proposed.

Keywords: *information technology, technological sovereignty, technological leadership, software import substitution, critical information infrastructure, state support*

Национальная цель «Технологическое лидерство»¹ предполагает способность государства обеспечивать устойчивое функционирование значимых цифровых систем преимущественно на основе отечественных решений. Санкционное давление, сопровождавшееся уходом ведущих иностранных технологических компаний с российского рынка, показало уязвимость отечественной цифровой инфраструктуры и актуализировало вопрос о соотношении между декларируемыми результатами импортозамещения и действительным уровнем технологической независимости.

Сформированный в 2022 г. публично-правовой механизм стимулирования развития ИТ-отрасли, нормативной основой которого стал Указ Президента РФ от 02.03.2022 № 83², закрепил совокупность регулятивных и фискальных инструментов поддержки. Эти меры обеспечили значительный количественный рост — к 2024 г. число программных продуктов в Реестре отечественного ПО превысило 24,3 тыс. при плановых 11,1 тыс.³, а доля закупаемого государственными компаниями российского ПО достигла 84,6 %⁴. Вместе с тем перевыполнение количественных индикаторов не обеспечило реальной технологической независимости. Правовой режим Единого реестра российских программ для ЭВМ⁵ (далее — Реестр) основан на критериях принадлежности исключительных прав и не предусматривает верификации технологической независимости продукта. Данное явление обозначается как «формальная локализация» — ситуация, при которой юрисдикционная отечественность (российское происхождение) продукта не тождественна его технологической независимости.

Целью статьи является анализ публично-правового механизма стимулирования развития ИТ-отрасли в условиях перехода от формальной локализации

¹ Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // СЗ РФ. 2024. № 20. Ст. 2584.

² Указ Президента РФ от 02.03.2022 № 83 «О мерах по обеспечению ускоренного развития отрасли информационных технологий в Российской Федерации» // СЗ РФ. 2022. № 10. Ст. 1468.

³ Леднева О. В., Сидорова О. Е. Анализ результатов выполнения национального проекта «Цифровая экономика» в Российской Федерации // Информатизация в цифровой экономике. 2025. Т. 6. № 2. С. 197—214.

⁴ Белая книга цифровой экономики за 2019—2024 годы : аналитический сборник // URL: <https://d-economy.ru/analytic/belaja-kniga-cifrovoj-jekonomiki-2019-2024>.

⁵ Постановление Правительства РФ от 16.11.2015 № 1236 «Об утверждении Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств — членов Евразийского экономического союза, за исключением Российской Федерации» // СЗ РФ. 2015. № 47. Ст. 6600.



к обеспечению технологического суверенитета и технологического лидерства. Методологическую основу исследования составляют сравнительный анализ российского законодательства, сравнительный анализ российской модели стимулирования и иностранных моделей, а также анализ эмпирических данных Минцифры России, новостных порталов.

Разрыв между номинальными и фактическими результатами проявляется при сопоставлении данных Реестра отечественного ПО с результатами опросов бизнеса. По данным Forbes, 75 % ИТ-инфраструктуры российских компаний по-прежнему составляют иностранные решения, при этом около 77 % организаций сталкиваются с техническими и интеграционными барьерами при попытках перехода на отечественные аналоги⁶. Внутренние затраты на развитие цифровой экономики в доле ВВП, при плановом значении свыше 5,1 % к 2024 г., фактически оставались на уровне 2,1—2,5 %, что во многом обусловлено снижением инвестиций в НИОКР в секторе ИКТ, наблюдающимся с 2017 г.⁷

Особенно острой проблема становится в инфраструктурном секторе. В телекоммуникационной отрасли уровень импортозависимости к 2022 г. достигал 80 %⁸, а в ряде сегментов вместо импортозамещения произошла замена одного иностранного поставщика другим — доля китайских производителей оптического волокна выросла с 6 % до 75 % при одновременном сокращении доли единственного отечественного производителя⁹. Данный процесс может быть квалифицирован как замещение без суверенитета.

Описанный разрыв повлек последовательное изменение правового регулирования ИТ-отрасли. Федеральный закон «Об информации, информационных технологиях и о защите информации»¹⁰ (далее — Закон № 149-ФЗ) ориентирует государственное управление преимущественно на применение ИТ, не формируя самостоятельного правового механизма стимулирования развития ИТ-отрасли как сектора экономики¹¹. Правовое обеспечение ИТ-отрасли традиционно рассматривалось через призму отдельных институтов налогового¹² и бюджетного

⁶ ИТ-инфраструктура российских компаний на 75 % все еще состоит из зарубежных решений // URL: <https://habr.com/ru/companies/k2tech/news/841892/> (дата обращения: 05.03.2026).

⁷ Леднева О. В., Сидорова О. Е. Анализ результатов выполнения национального проекта «Цифровая экономика» в Российской Федерации // Информатизация в цифровой экономике. 2025. Т. 6. № 2. С. 197—214.

⁸ Соколов А. Б. Государственная поддержка отрасли телекоммуникаций в целях достижения технологического суверенитета // Вестник Института экономики Российской академии наук. 2025. № 4.

⁹ Соколов А. Б. Указ. соч.

¹⁰ Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

¹¹ Южаков В. Н., Ефремов А. А. Направления совершенствования правового регулирования в сфере стимулирования развития информационных технологий // Российское право: образование, практика, наука. 2017. № 5. С. 62—69.

¹² Грачева Е. Ю. К вопросу о сущности финансового права // Вестник Университета имени О.Е. Кутафина (МГЮА). 2020. № 9 (73). С. 26—32.

права¹³, без формирования единого публично-правового механизма, увязанного с целями технологического суверенитета и технологического лидерства.

Проявлениями перехода стали окончание моратория на плановые выездные налоговые проверки ИТ-компаний и принятие Федеральных законов № 58-ФЗ¹⁴ и № 325-ФЗ¹⁵, наделивших Правительство РФ полномочиями по переходу объектов КИИ на российские ПО и установивших требования национального контроля¹⁶.

Формируемая модель устанавливает прямую юридическую связь между правом на льготный режим и достижением верифицируемых показателей технологической независимости.

С 01.01.2026 вступили в силу изменения в Положение о государственной аккредитации российских ИТ-организаций¹⁷, формирующие механизм верификации встречных обязательств. Ужесточены финансовые критерии (профильная доля от выручки), введен критерий национального контроля¹⁸, а также образовательный ценз. Государство этими мерами корректирует налоговые льготы, задействуя инструмент целевого софинансирования государственных задач.

Действующая одноуровневая модель оценки отечественности ПО сводится к факту включения в Реестр, привязывания преференции к корпоративной принадлежности правообладателя, а не к технологической независимости продукта. В этой связи предлагается переход к трехуровневой функционально-структурной модели оценки.

Формальный уровень сохраняет критерий регистрации в Реестре — как необходимое, но недостаточное условие. Второй уровень, функциональный, связан с подтверждением достижения девятого (высшего) уровня готовности технологий по ГОСТ Р 58048-2017. Так, постановления Правительства РФ № 598¹⁹ и № 550²⁰ установили требование девятого уровня готовности технологии для получения

¹³ Карасева М. В. Наука финансового права и новые институциональные структуры // Российский журнал правовых исследований. 2023. Т. 10. № 2. С. 7—12.

¹⁴ Федеральный закон от 07.04.2025 № 58-ФЗ «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры» // СЗ РФ. 2025. № 15. Ст. 1784.

¹⁵ Федеральный закон от 31.07.2025 № 325-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2025. № 31. Ст. 4679.

¹⁶ Обзор основных изменений в области безопасности критической информационной инфраструктуры (КИИ) 2025—2026 гг. // URL: <https://www.lidings.com/ru/media/legalupdates/cii2025-2026/> (дата обращения: 25.04.2026).

¹⁷ Постановление Правительства РФ от 28.11.2025 № 1949 «О внесении изменений в некоторые акты Правительства Российской Федерации» // СЗ РФ. 2025. № 48 (ч. IV). Ст. 7391.

¹⁸ Козырева Е. В., Чернова Л. Г. Меры поддержки российских ИТ-компаний в современных условиях // Электронный научный журнал «Вектор экономики». 2024. № 12.

¹⁹ Постановление Правительства РФ от 06.04.2022 № 598 «О внесении изменений в правила предоставления субсидий из федерального бюджета Российскому фонду развития информационных технологий» // СЗ РФ. 2022. № 15. Ст. 2515.

²⁰ Постановление Правительства РФ от 03.05.2019 № 550 «Об утверждении Правил предоставления субсидий из федерального бюджета Российскому фонду развития информационных технологий» // СЗ РФ. 2019. № 19. Ст. 2306.



субсидий на особо значимые проекты. Третий уровень, структурный, предполагает зависимость объема льгот от доли использования доверенной отечественной электронной компонентной базы, что корреспондирует с требованиями Закона № 325-ФЗ о доверенных программно-аппаратных комплексах²¹. Переход к трехуровневой системе не требует принятия нового федерального закона, достаточно внесения изменений в подзаконные акты, регулирующие условия включения в Реестр и предоставления субсидий.

Действующие нормы распылены по различным отраслям законодательства, что порождает правовую неопределенность и регуляторный арбитраж. В научной литературе обосновывается, что цифровая трансформация требует правового ответа, выходящего за рамки точечного регулирования²². В этой связи заслуживает внимания идея о разработке единого кодифицированного акта, объединяющего нормы о правовом режиме ИТ, государственной поддержке ИТ-отрасли и критической информационной инфраструктуре.

Сопоставление российского механизма с моделями КНР и Индии позволяет оценить обоснованность перехода. Например, КНР сочетает умеренное снижение налоговой нагрузки (ставка 15 % вместо 25 %) с императивом отказа от зарубежных компонентов в ряде секторов²³ — инструмент, аналогов которому в российском законодательстве не существовало до принятия Законов № 58-ФЗ и № 325-ФЗ.

Индия опирается на экспортно ориентированную модель, в которой налоговые каникулы привязаны к доходам от экспорта ИТ-услуг, формируют прямую юридическую связь между предоставлением преференции и достижением измеримого результата²⁴.

Исходя из этого, можно предположить, что действующий в Российской Федерации фискальный механизм является одним из наиболее привлекательных по совокупному уровню налоговой нагрузки²⁵, однако стимулировал преимущественно экстенсивный рост. Опыт КНР и Индии подтверждает необходимость

²¹ Федеральный закон от 31.07.2025 № 325-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2025. № 31. Ст. 4679.

²² Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 85—102.

²³ Отчет McKinsey Global Institute о стратегии цифровой экономики Китая: Digital China: Powering the economy to global competitiveness. McKinsey Global Institute. McKinsey, December 2017 // URL: https://www.mckinsey.com/~media/mckinsey/industries/technology%20media%20and%20telecommunications/high%20tech/our%20insights/digital%20china%20powering%20the%20economy%20to%20global%20competitiveness/mgi_digital-china_report_dec-2017.pdf (дата обращения: 25.04.2026).

²⁴ Mehta B. S. Inter-industry linkages of ICT sector in India // Indian Journal of Human Development. 2020. # 14 (1). P. 42—61. URL: <https://journals.sagepub.com/doi/10.1177/0973703020919835> (дата обращения: 25.04.2026).

²⁵ Ефремов А. А. Оценка результативности и эффективности стимулирования развития отрасли информационных технологий в России: состояние и перспективы // Вопросы государственного и муниципального управления. 2023. № 4. С. 71—99.

дополнения налогового режима механизмом встречных обязательств, к формированию которого Россия приступила в 2025—2026 гг.

Практическая достижимость перехода от формальной к реальной локализации подтверждается ситуацией на рынке сложного инженерного ПО. По данным J'son & Partners Consulting, по итогам 2024 г. доля российских разработчиков здесь занимает 91 % внутреннего рынка с прогнозом роста до 95 % к 2030 г.²⁶ Данный сегмент демонстрирует фактическое вытеснение зарубежных решений, что доказывает достижимость технологического суверенитета при условии концентрации ресурсов и проработанном публично-правовом механизме стимулирования.

Национальный проект «Экономика данных» (2025—2030 гг.) устанавливает целевые ориентиры, корреспондирующие с функциональной моделью оценки. Например, не менее 80 % организаций ключевых отраслей должны перейти на использование российского ПО, а его доля в государственных органах должна достичь 95 %²⁷.

Проведенное исследование позволяет квалифицировать формальную локализацию как институциональный дефект публично-правового механизма стимулирования развития ИТ-отрасли, при котором количественное перевыполнение реестровых показателей сопровождается сохранением структурной технологической зависимости от иностранных решений. Дефект обусловлен одноуровневой моделью оценки отечественности ПО и правовой дисперсностью регулирования, не обеспечивающей связь между объемом предпочтений и уровнем технологической независимости.

Нормативные положения 2025—2026 гг. свидетельствуют о переходе от модели безусловных предпочтений к модели встречных обязательств. Для преодоления формальной локализации обосновано внедрение трехуровневой модели оценки отечественности ПО (формальный, функциональный и структурный критерии) как юридически значимых условий предоставления мер государственной поддержки.

Описанная трансформация отражает переход от компенсаторной к целеориентированной функции публично-правового стимулирования, в рамках которой инструменты государственной поддержки выступают механизмом достижения национальных целей технологического лидерства.

БИБЛИОГРАФИЯ

1. *Грачева Е. Ю.* К вопросу о сущности финансового права // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2020. — № 9 (73). — С. 26—32.

²⁶ J'Son & Partners Consulting. Стратегический обзор рынка инженерного ПО // URL: <https://ict.moscow/analytics/strategicheskii-obzor-rynka-inzhenernogo-po-perekhod-k-ai-native-i-oblachnym-ekosistemam/> (дата обращения: 25.04.2026).

²⁷ Основные показатели и мероприятия национального проекта «Экономика данных и цифровая трансформация государства» // URL: <http://government.ru/info/54314/> (дата обращения: 25.04.2026).



2. *Ефремов А. А.* Оценка результативности и эффективности стимулирования отрасли информационных технологий в России: состояние и перспективы // Вопросы государственного и муниципального управления. — 2023. — № 4. — С. 71—99.
3. *Карасева М. В.* Наука финансового права и новые институциональные структуры // Российский журнал правовых исследований. — 2023. — Т. 10. — № 2. — С. 7—12.
4. *Козырева Е. В., Чернова Л. Г.* Меры поддержки российских IT-компаний в современных условиях // Электронный научный журнал «Вектор экономики». — 2024. — № 12. — URL: https://vectoreconomy.ru/images/publications/2024/12/regionaleconomy/Kozyreva_Chernova.pdf (дата обращения: 05.03.2026).
5. *Леднева О. В., Сидорова О. Е.* Анализ результатов выполнения национального проекта «Цифровая экономика» в Российской Федерации // Информатизация в цифровой экономике. — 2025. — Т. 6. — № 2. — С. 197—214.
6. *Соколов А. Б.* Государственная поддержка отрасли телекоммуникаций в целях достижения технологического суверенитета // Вестник Института экономики Российской академии наук. — 2025. — № 4.
7. *Хабриева Т. Я., Черногор Н. Н.* Право в условиях цифровой реальности // Журнал российского права. — 2018. — № 1. — С. 85—102.
8. *Южаков В. Н., Ефремов А. А.* Направления совершенствования правового регулирования в сфере стимулирования развития информационных технологий // Российское право: образование, практика, наука. — 2017. — № 5. — С. 62—69.

Нормативные подходы к правовому регулированию городов будущего: от умных счетчиков к умным домам

Аннотация. Статья посвящена концептуальному осмыслению нормативных подходов к регулированию технологий умных городов в России — от точечных фрагментарных нормативных правовых актов до стратегических документов системного уровня.

На основе анализа действующего законодательства автор выделяет три этапа развития правового регулирования в данной сфере: первичное точечное нормирование, ведомственную стандартизацию умных домов, а также формирование системы нормативно-правового регулирования. Выявляется центральная системная проблема действующей нормативной модели — ее ведомственно-секторальный характер, при котором каждая подсистема умного города (интеллектуальный учет, управление зданием, обработка данных, кибербезопасность) функционирует в рамках обособленного регуляторного контура без механизма межсистемного взаимодействия. Анализируются конкретные правовые пробелы: нормативная асимметрия между интеллектуальными счетчиками различных ресурсов, неопределенность гражданско-правового статуса умного дома как объекта права, правовой вакуум вокруг данных экосистем интернета вещей, а также принципиальная неурегулированность цифрового двойника города.

В качестве решения выявленных проблем предложена авторская концепция многоуровневого нормативного регулирования, структурированная по трем уровням: инфраструктурному (технологические стандарты и требования безопасности), платформенному (правовой режим данных, цифровых платформ и операторов) и сервисному (цифровые услуги, алгоритмическое управление и механизмы защиты прав граждан). Сделан вывод о том, что данная концепция может стать основой для разработки специального рамочного закона, регулирующего умные городские технологии в комплексе.

Ключевые слова: умный город, умный дом, цифровой двойник, интернет вещей, правовое регулирование цифровых технологий, информационное право, национальные стандарты, ГОСТ, персональные данные, киберфизические системы



**Дмитрий Игоревич
РЫЖКОВ,**

аспирант кафедры
информационного права
и цифровых технологий
Университета имени
О.Е. Кутафина (МГЮА)
diryzhkov@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2026.142.6.197-205

Dmitrii I. RYZHKOV,

Postgraduate student of the Department of Information Law
and Digital Technologies

Kutafin Moscow State Law University (MSAL)

diryzhkov@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

The Legal Regulation Approaches for the Cities of Future: from Smart Meters to Smart Homes

Abstract. *The article offers a conceptual analysis of regulatory approaches to smart city technologies in Russia, tracing their evolution from isolated, fragmentary legal acts to strategic system-level policy documents.*

Based on an analysis of current legislation, the author identifies three stages in the development of legal regulation in this field: initial targeted norm-setting, departmental standardization of smart homes, and the emergence of a comprehensive system of legal regulation. The central systemic problem of the existing regulatory model is identified as its sectoral, agency-based character, whereby each subsystem of the smart city (intelligent metering, building management, data processing, cybersecurity) operates within its own isolated regulatory framework without mechanisms for inter-system interaction. Specific legal gaps are examined, including: regulatory asymmetry between intelligent meters for different resources, uncertainty regarding the civil-law status of the smart home as an object of rights, the legal vacuum surrounding data in Internet of Things ecosystems, and the fundamental lack of regulation for the city's digital twin.

As a solution, the author proposes a multi-level regulatory concept structured across three tiers: the infrastructural level (technological standards and safety requirements), the platform level (legal regime for data, digital platforms, and operators), and the service level (digital services, algorithmic management, and mechanisms for protecting citizens' rights). It is concluded that this concept can serve as a basis for drafting a special framework law that would regulate smart city technologies in an integrated manner.

Keywords: *smart city, smart home, digital twin, Internet of Things, legal regulation of digital technologies, information law, national standards, GOST, personal data, cyber-physical systems*

Введение

Концепция умного города из мечты будущего последовательно превращается в нормативную реальность. Для современной правовой науки принципиально важно не просто зафиксировать появление новых технологических практик, но и разрабатывать достаточный правовой инструментарий для их освоения или даже предвидеть и обеспечить возникновение перспективных технологических

концепций будущего. Данное исследование ставит перед собой задачу концептуального осмысления нормативных подходов, складывающихся в России в сфере умных городских технологий — от точечных фрагментарных нормативных правовых актов до стратегических документов системного уровня.

Проект «Умный город» функционирует с 2018 г. в рамках национального проекта «Жилье и городская среда» и национальной программы «Цифровая экономика»¹. За период 2019—2023 гг. индекс цифровой зрелости городов (IQ городов) показывал последовательный рост: к 2023 г. его среднее значение составило 61 балл из 120². Тем не менее, по оценкам экспертов, даже в крупных городах сохраняется правовая неопределенность, выступающая значительным риском для инвесторов и разработчиков, — следствие фрагментарного и ведомственного характера действующего регулирования³.

Актуальность проблематики обусловлена, во-первых, стремительным ростом проникновения умных технологий в жилищный сектор: каждая вторая новостройка в крупных городах возводится с применением систем умного дома, в новых домах до 80 % управляющих компаний используют такие системы⁴. Во-вторых, с 01.02.2025 вступила в силу крупнейшая в России серия национальных стандартов цифровизации многоквартирных домов, разработанная при участии более 30 организаций и 150 экспертов⁵. В-третьих, в январе 2026 г. Президент России поставил задачу разработки комплексного закона, регулирующего применение автономных систем⁶. Совокупность этих факторов делает научно-правовое осмысление данной сферы в высокой степени актуальным.

¹ Проект цифровизации городского хозяйства «Умный город» // Официальный интернет-портал Министерства строительства и жилищно-коммунального хозяйства РФ. URL: <https://minstroyrf.gov.ru/trades/gorodskaya-sreda/proekt-tsifrovizatsii-gorodskogo-khozyaystva-umnyy-gorod/> (дата обращения: 25.03.2026).

² Власти потратили более 800 млн на «умные города»: IQ городов вырос в полтора раза // URL: https://www.cnews.ru/news/top/2025-02-19_vlasti_potratili_bolee_800 (дата обращения: 25.03.2026).

³ См.: Двойники, роботы и нейросети: какие «умные» технологии осваивают города России // URL: <https://www.vedomosti.ru/gorod/smartcity/articles/osvaivayut-goroda-rossii> (дата обращения: 25.03.2026).

⁴ См.: Защита данных: россиян обезопасят от утечек из «умного дома» в новостройках // Общественный совет при Минстрое России. URL: <https://osminstroy.ru/news/-zashchita-sdannykh--rossiyan-obezipasyat-ot-utechek-iz--umnogo-doma--v-novostroykakh/> (дата обращения: 25.03.2026).

⁵ См.: *Богданова Е. А.* Вступила в действие крупнейшая серия стандартов цифровизации домов. Что это такое? // URL: <https://telesputnik.ru/materials/gov/news/vstupila-v-deistvie-krupneisaya-seriya-standartov-cifrovizacii-domov-cto-eto-takoe> (дата обращения: 25.03.2026).

⁶ Совещание по вопросам развития автономных систем // URL: <http://kremlin.ru/events/president/news/79016> (дата обращения: 25.03.2026).



Интеллектуальный учет ресурсов: вопросы фрагментарного регулирования

Отправной точкой формирования нормативной базы умного города в России следует считать Федеральный закон от 27 декабря 2018 г. № 522-ФЗ⁷. Именно этот акт впервые закрепил понятие интеллектуальной системы учета электрической энергии (мощности). Вместе с тем существует принципиальное ограничение: сфера применения названного Закона — исключительно учет электроэнергии.

Примечательно, что еще в 2019 г. Н. Г. Жаворонкова и Ю. Г. Шпаковский указывали на недопустимость «отсутствия “связанности” планов, ответственности и системности многочисленных нормативных (подзаконных) актов», на основании которых функционируют федеральные и региональные информационные ресурсы в сфере энергетики⁸. Этот прогностический вывод в полной мере подтвердился: правовая асимметрия между интеллектуальными счетчиками электроэнергии и иными ресурсами оказалась именно следствием отсутствия системной правовой концепции.

Интеллектуальные счетчики на воду, газ и тепло федеральным законодательством специально не регулируются, что создает разрыв в сфере нормативного правового регулирования между технологической и правовой сторонами умного дома.

Таким образом, сбор, передача и хранение данных о потреблении всех ресурсов, осуществляемые единой автоматизированной информационной системой, сочетаются с правовой разрозненностью регулирования отдельных компонентов. Умный счетчик электроэнергии в одном доме юридически живет в ином нормативном измерении, чем умный счетчик воды, даже если физически оба устройства являются частью единой управляющей платформы.

Стандартизация умного дома

Развитие нормативно-технической базы в сфере умных домов происходило параллельно с реализацией ведомственного проекта Минстроя «Умный город» и прошло несколько качественных этапов.

В 2020 г. Росстандарт утвердил первую серию из восьми национальных стандартов в области умных городов, разработанных Техническим комитетом ТК 194 «Кибер-физические системы». В 2022 г. Министерство строительства актуализировало стандарт умного города, включив в него 18 тематических блоков, охватывающих не только коммунальную инфраструктуру, но и образование, здравоохранение и социальную сферу⁹.

⁷ Федеральный закон от 27.12.2018 № 522-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с развитием систем учета электрической энергии (мощности)» // СЗ РФ. 2018. № 53 (ч. I). Ст. 8448.

⁸ См.: Жаворонкова Н. Г., Шпаковский Ю. Г. Экологические и энергетические проблемы четвертой промышленной революции: правовые аспекты // Lex russica. 2019. № 10. С. 53—62.

⁹ Минстрой утвердил новый стандарт «Умного города» // Официальный интернет-портал Министерства строительства и жилищно-коммунального хозяйства РФ. URL: <https://>

Новый виток развития связан с принятием рядом государственных стандартов в период с 2024 по 2025 г. С 01.02.2025 вступили в силу крупнейшая в истории отечественной стандартизации серия документов в сфере цифровизации многоквартирных домов¹⁰, а также ряд иных государственных стандартов.

Помимо стандартизации, важным инструментом стал реестр умных жилых комплексов, формируемый на интернет-платформе «Единый ресурс застройщиков»: к марту 2026 г. в нем числилось 333 объекта.

Вместе с тем принятие стандартов серии «Умный дом» не решает проблему правового статуса самой системы. В гражданско-правовом смысле умный дом до сих пор не выделен в качестве самостоятельного объекта права, рассматривается как обычный объект недвижимости с дополнительным техническим оснащением. Встроенные стационарные компоненты (видеонаблюдение, СКУД, системы вентиляции) квалифицируются как недвижимость, переносные устройства — как движимое имущество. Такая дуальная квалификация порождает практические трудности при совершении сделок, установлении ответственности и разграничении полномочий управляющей организации и собственников.

Развитие от умного дома к умному городу означает переход от управления объектом к управлению средой. Как справедливо отмечает А. В. Минбалеев, цифровой двойник является новым для правовой науки явлением, нуждающимся в дифференциации от смежных понятий — цифрового профиля, цифрового персонажа и цифрового аватара, а также в самостоятельном законодательном закреплении в целях эффективной защиты прав субъектов, данные о которых они содержат¹¹.

minstroyrf.gov.ru/press/minstroy-utverdil-novyj-standart-umnogo-goroda/ (дата обращения: 25.03.2026).

¹⁰ ГОСТ Р 71865—2024 «Умный дом. Архитектура» // URL: <https://docs.cntd.ru/document/1310964251> (дата обращения: 25.03.2026) ; ГОСТ Р 71866—2024 «Умный дом. Общие технические требования к автоматизированным системам управления зданием» // URL: <https://docs.cntd.ru/document/1310964223> (дата обращения: 25.03.2026) ; ГОСТ Р 71867—2024 «Умный дом. Стадии создания автоматизированной системы управления зданием» // URL: <https://docs.cntd.ru/document/1310939637> (дата обращения: 25.03.2026) ; ГОСТ Р 71868—2024 «Умный дом. Классы многоквартирных домов Часть 1. Требования к классам» // URL: <https://docs.cntd.ru/document/1310939638/titles/65C0IR> (дата обращения: 25.03.2026) ; ГОСТ Р 71869—2025 «Умный дом. Требования к автоматизированным системам управления освещением» // URL: <http://docs.cntd.ru/document/1311150194/titles/7D80K5> (дата обращения: 25.03.2026) ; ГОСТ Р 71870—2024 «Умный дом. Требования к устройствам. Общие положения» // URL: <https://docs.cntd.ru/document/1310939630> (дата обращения: 25.03.2026).

¹¹ См.: Минбалеев А. В. Цифровые двойники и цифровые аватары как новое явление в праве // Юридический мир. 2022. № 2. С. 27—32.



Цифровой двойник города: вопросы правового статуса

Ключевым концептуальным инструментом перехода служит цифровой двойник города — «комплексная виртуальная модель, синхронизированная с реальными городскими системами в режиме реального времени»¹².

Практика функционирования проекта «Цифровой двойник Москвы» наглядно демонстрирует переход цифровых городских технологий из экспериментальной в операционную фазу. Платформа, работающая с 2019 г. и созданная на основе более чем 12 млн фотоснимков столицы, представляет собой точную трехмерную фотограмметрическую копию всей территории города, дополненную несколькими тысячами аналитических слоев, обновляемых в режиме реального времени. В нее интегрированы данные о движении более чем 8 тыс. единиц городской техники, архив панорам 13 тыс. километров городских улиц с 2013 г., а также 3D-модели 3 тыс. зданий. При этом примечательно, что платформа представляет собой собственную разработку Москвы на основе свободно распространяемого программного обеспечения¹³. Однако именно этот пример обнажает центральный правовой пробел: несмотря на масштаб и значимость платформы, правовой статус цифрового двойника города как объекта права, режим данных, которые он накапливает, и ответственность за управленческие решения, принятые на его основе, до сих пор не урегулированы специальным федеральным законодательством.

Центральной проблемой действующего регулирования является его ведомственно-секторальный характер: правовое регулирование умных городов состоит из разрозненных нормативных актов и ведомственных стандартов, создающих правовую неопределенность для инвесторов и разработчиков. По существу, каждая подсистема умного города в правовом аспекте функционирует самостоятельно, вне взаимосвязи с иными системами: интеллектуальный учет электроэнергии регулируется Законом об электроэнергетике и нормативными актами Правительства; умный дом как объект строительства — техническими регламентами и жилищным законодательством; обработка данных — законодательством о персональных данных; кибербезопасность систем — законодательством о критической информационной инфраструктуре.

Анализ правовых пробелов

Одной из ключевых проблем действующего регулирования является его фрагментарный характер: правовое регулирование умных городов состоит из разрозненных нормативных правовых актов и ведомственных стандартов.

¹² См.: Елисеева А. Стандартизация цифровых двойников городов: проект ГОСТ Р «Смарт-Сити» // URL: <https://gostassistant.ru/article/standartizaciya-cifrovyyh-dvoynikov-gorodov-proekt-gost-r-smart-siti> (дата обращения: 25.03.2026).

¹³ См.: Цифровой двойник Москвы: как 3D-моделирование и искусственный интеллект изменили управление городом // URL: <https://www.mos.ru/news/item/126225073/> (дата обращения: 25.03.2026).

Это явление точно охарактеризовано К. С. Евсиковым как дисбаланс, при котором «правотворческая деятельность в области цифрового права ориентирована на “доцифровые” методы государственного управления», что применительно к умным городским технологиям означает неспособность нормативных правовых актов, фрагментарно регулирующих функционирование умных домов, в достаточной мере охватить межсистемное взаимодействие киберфизических комплексов¹⁴.

Отсутствие рамочного закона, который устанавливал бы общие принципы, понятийный аппарат и разграничение полномочий, ведет к нескольким практическим последствиям.

Во-первых, возникают пробелы в регулировании межсистемного взаимодействия: нормы жилищного законодательства не определяют порядок сопряжения информационных систем различных уровней единой системы публичной власти в Российской Федерации.

Во-вторых, появляются коллизии между отраслевыми нормами: требования к защите персональных данных устройств интернета вещей, установленные Федеральным законом «О персональных данных»¹⁵, разрабатывались без учета технологической архитектуры распределенных киберфизических систем.

В-третьих, остаются не в полной мере ясными критерии привлечения к публично-правовой ответственности: достоверно неизвестно, какой орган осуществляет надзор за соблюдением требований к умному дому в комплексе, а не по отдельным подсистемам.

Особую остроту приобретает проблема правового регулирования данных, генерируемых системами умного дома. Общественный совет при Министерстве строительства и ЖКХ ранее констатировал: несмотря на то, что фактически все данные, собираемые системой умного дома (маршруты перемещений, паттерны потребления ресурсов, биометрические идентификаторы), могут быть отнесены к персональным, на практике эти системы не подпадают под действие правового режима персональных данных, не защищены от утечек и уязвимы для кибератак¹⁶.

На основании проведенного анализа полагаем целесообразным предложить концепцию многоуровневого нормативно-правового регулирования технологий умных городов.

Первым уровнем должно охватываться правовое регулирование физической и цифровой инфраструктуры умного города: интеллектуальных систем учета, технической архитектуры автоматических систем управления, инженерных коммуникаций, а также сетей связи, обеспечивающих работу устройств интернета вещей. Задача данного уровня — посредством технологических стандартов установить минимальные требования безопасности, обязательные для всех субъектов, вводящих объекты городской инфраструктуры в эксплуатацию.

¹⁴ См.: *Евсиков К. С.* Государственно-правовые концепции использования информационных технологий в государственном управлении // *Lex russica*. 2022. Т. 81. № 1. С. 74—86.

¹⁵ Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.

¹⁶ См.: Защита сданных: россияне обезопасят от утечек из «умного дома» в новостройках // URL: <https://osminstroy.ru/news/-zashchita-sdannyykh--rossiyan-obezipasyat-ot-utechek-iz-umnogo-doma--v-novostroykakh/> (дата обращения: 25.03.2026).



Второй уровень регулирует данные, платформы и управленческие системы: правовой режим данных умного города (включая собранные устройствами интернета вещей данные, агрегированные данные об инфраструктуре и данные цифровых двойников), права доступа к данным и их монетизация, статус муниципальных и региональных цифровых платформ, а также интеграция с государственными информационными системами. На данном уровне важно ввести понятие «данные городского хозяйства» как особую категорию информации, обладающей публично-правовым измерением наряду с частноправовым. Применительно к умным домам необходимо законодательно закрепить иерархию субъектов — операторов данных: жилец (как первичный субъект данных), управляющая организация (как технический оператор), застройщик (как первичный создатель инфраструктуры) — и разграничить их права и ответственность.

Третий уровень должен охватывать правовое регулирование цифровых услуг в умном городе: алгоритмического управления городскими системами (транспортом, энергетикой, ЖКХ), ответственности за вред, причиненный автономными системами, доступа граждан к данным, касающимся их жилища и городской среды, а также механизмов обжалования автоматических решений.

С точки зрения предложенной концепции каскадного регулирования компоненты инфраструктурного уровня умного города могут быть квалифицированы как ИТ-активы в смысле, предложенном А. В. Минбалеевым: это инфраструктурные объекты, «предназначенные для совершения тех или иных действий с информацией» и имеющие публично-правовое измерение как инструменты цифровой трансформации системы государственного и муниципального управления¹⁷. Такое понимание позволяет отделить правовой режим физической инфраструктуры умного города (системы управления, сети интернета вещей, платформы учета ресурсов) от правового режима данных, в ней циркулирующих.

Выводы

Проведенное исследование позволяет сформулировать ряд обобщающих выводов теоретического и прикладного характера.

Правовое регулирование технологий умных городов в России прошло три этапа: от первичного точечного нормирования через ведомственную стандартизацию умных домов к формирующейся системе нормативно-правового регулирования. Тем не менее даже в совокупности существующие нормативные правовые акты не образуют единого нормативного массива, способного обеспечить последовательное и непротиворечивое регулирование умной городской среды.

Центральной системной проблемой действующей нормативной модели выступает ее ведомственно-секторальный характер: каждая подсистема умного города — интеллектуальный учет, управление зданием, обработка данных, кибербезопасность — функционирует в рамках обособленного регуляторного контура, без правового механизма межсистемного взаимодействия. Следствием этого

¹⁷ См.: Минбалеев А. В. Правовой режим ИТ-активов как объекта публично-правовых и частноправовых отношений // Lex russica. 2025. Т. 78. № 11. С. 143—153.

являются нормативная асимметрия между интеллектуальными счетчиками различных ресурсов, правовая неопределенность статуса умного дома как объекта гражданских прав, правовой вакуум вокруг данных экосистем интернета вещей и принципиальная неурегулированность цифрового двойника города как нового объекта публичных и частноправовых отношений.

Для преодоления выявленных пробелов в статье предложена авторская концепция многоуровневого нормативного регулирования, структурированного по трем юридическим уровням: инфраструктурному (технологические стандарты и требования безопасности), платформенному (правовой режим данных, цифровых платформ и операторов) и сервисному (цифровые услуги, алгоритмическое управление и механизмы защиты прав граждан). Данная концепция может стать концептуальной основой для подготовки специального нормативно-правового регулирования.

БИБЛИОГРАФИЯ

1. *Евсиков К. С.* Государственно-правовые концепции использования информационных технологий в государственном управлении // *Lex russica*. — 2022. — Т. 81. — № 1. — С. 74—86.
2. *Минбалева А. В.* Правовой режим ИТ-активов как объекта публично-правовых и частноправовых отношений // *Lex russica*. — 2025. — Т. 78. — № 11. — С. 143—153.
3. *Минбалева А. В.* Цифровые двойники и цифровые аватары как новое явление в праве // *Юридический мир*. — 2022. — № 2. — С. 27—32.

НАУЧНОЕ НАСЛЕДИЕ



Алан Тьюринг,
1951 г.

Алан Тьюринг — первый философ искусственного интеллекта. Когда Алан Тьюринг обратил свое внимание на искусственный интеллект, пожалуй, в мире не было никого, кто был бы лучше подготовлен для изучения этой сферы. Его статья «Вычислительная техника и интеллект» (1950) до сих пор является одной из наиболее часто цитируемых в этой области. Хотя Тьюринг и умер молодым, долгое время большая часть его работ оставалась либо засекреченной, либо иным образом недоступной.

Сегодня мы публикуем отрывок из его оригинальной статьи «Вычислительная техника и интеллект»¹.

A. M. Turing

Computing Machinery and Intelligence

1. The Imitation Game

I propose to consider the question, “Can machines think?” This should begin with definitions of the meaning of the terms “machine” and “think”. The definitions might be framed so as to reflect so far as possible the normal use of the words, but this attitude is dangerous. If the meaning of the words “machine” and “think” are to be found by examining how they are commonly used it is difficult to escape the conclusion that the meaning and the answer to the question, “Can machines think?” is to be sought in a statistical survey such as a Gallup poll. But this is absurd. Instead of attempting such a definition I shall replace the question by another, which is closely related to it and is expressed in relatively unambiguous words.

The new form of the problem can be described in terms of a game which we call the “imitation game”. It is played with three people, a man (A), a woman (B), and an interrogator (C) who may be of either sex. The interrogator stays in a room apart from the other two. The object of the game for the interrogator is to determine which of the other two is the man and which is the woman. He knows them by labels X and Y, and at the end of the game he says either “X is A and Y is B” or “X is B and Y is A”. The interrogator is allowed to put questions to A and B thus:

C: Will X please tell me the length of his or her hair?

Now suppose X is actually A, then A must answer. It is A's object in the game to try and cause C to make the wrong identification. His answer might therefore be:

“My hair is shingled, and the longest strands are about nine inches long”.

In order that tones of voice may not help the interrogator the answers should be written, or better still, typewritten. The ideal arrangement is to have a teleprinter communicating between the two rooms. Alternatively the question and answers can be repeated by an intermediary. The object of the game for the third player (B) is to help the interrogator. The best strategy for her is probably to give truthful answers.

¹ Turing A. M. (1950) Computing Machinery and Intelligence. Mind 49: 433—460.

She can add such things as "I am the woman, don't listen to him!" to her answers, but it will avail nothing as the man can make similar remarks.

We now ask the question, "What will happen when a machine takes the part of A in this game?" Will the interrogator decide wrongly as often when the game is played like this as he does when the game is played between a man and a woman? These questions replace our original, "Can machines think?"

2. Critique of the New Problem

As well as asking, "What is the answer to this new form of the question", one may ask, "Is this new question a worthy one to investigate?" This latter question we investigate without further ado, thereby cutting short an infinite regress.

The new problem has the advantage of drawing a fairly sharp line between the physical and the intellectual capacities of a man. No engineer or chemist claims to be able to produce a material which is indistinguishable from the human skin. It is possible that at some time this might be done, but even supposing this invention available we should feel there was little point in trying to make a "thinking machine" more human by dressing it up in such artificial flesh. The form in which we have set the problem reflects this fact in the condition which prevents the interrogator from seeing or touching the other competitors, or hearing — their voices. Some other advantages of the proposed criterion may be shown up by specimen questions and answers. Thus:

Q: Please write me a sonnet on the subject of the Forth Bridge.

A: Count me out on this one. I never could write poetry.

Q: Add 34957 to 70764.

A: (Pause about 30 seconds and then give as answer) 105621.

Q: Do you play chess?

A: Yes.

Q: I have K at my K1, and no other pieces. You have only K at K6 and R at R1. It is your move. What do you play?

A: (After a pause of 15 seconds) R-R8 mate.

The question and answer method seems to be suitable for introducing almost any one of the fields of human endeavour that we wish to include. We do not wish to penalise the machine for its inability to shine in beauty competitions, nor to penalise a man for losing in a race against an aeroplane. The conditions of our game make these disabilities irrelevant. The "witnesses" can brag, if they consider it advisable, as much as they please about their charms, strength or heroism, but the interrogator cannot demand practical demonstrations.

The game may perhaps be criticised on the ground that the odds are weighted too heavily against the machine. If the man were to try and pretend to be the machine he would clearly make a very poor showing. He would be given away at once by slowness and inaccuracy in arithmetic. May not machines carry out something which ought to be described as thinking but which is very different from what a man does? This objection is a very strong one, but at least we can say that if, nevertheless, a machine can be constructed to play the imitation game satisfactorily, we need not be troubled by this objection.

It might be urged that when playing the "imitation game" the best strategy for the machine may possibly be something other than imitation of the behaviour of a man.



This may be, but I think it is unlikely that there is any great effect of this kind. In any case there is no intention to investigate here the theory of the game, and it will be assumed that the best strategy is to try to provide answers that would naturally be given by a man.

3. The Machines Concerned in the Game

The question which we put in 1 will not be quite definite until we have specified what we mean by the word “machine”. It is natural that we should wish to permit every kind of engineering technique to be used in our machines. We also wish to allow the possibility that an engineer or team of engineers may construct a machine which works, but whose manner of operation cannot be satisfactorily described by its constructors because they have applied a method which is largely experimental. Finally, we wish to exclude from the machines men born in the usual manner. It is difficult to frame the definitions so as to satisfy these three conditions. One might for instance insist that the team of engineers should be all of one sex, but this would not really be satisfactory, for it is probably possible to rear a complete individual from a single cell of the skin (say) of a man. To do so would be a feat of biological technique deserving of the very highest praise, but we would not be inclined to regard it as a case of “constructing a thinking machine”. This prompts us to abandon the requirement that every kind of technique should be permitted. We are the more ready to do so in view of the fact that the present interest in “thinking machines” has been aroused by a particular kind of machine, usually called an “electronic computer” or “digital computer”. Following this suggestion we only permit digital computers to take part in our game.

This restriction appears at first sight to be a very drastic one. I shall attempt to show that it is not so in reality. To do this necessitates a short account of the nature and properties of these computers.

It may also be said that this identification of machines with digital computers, like our criterion for “thinking”, will only be unsatisfactory if (contrary to my belief), it turns out that digital computers are unable to give a good showing in the game.

There are already a number of digital computers in working order, and it may be asked, “Why not try the experiment straight away? It would be easy to satisfy the conditions of the game. A number of interrogators could be used, and statistics compiled to show how often the right identification was given”. The short answer is that we are not asking whether all digital computers would do well in the game nor whether the computers at present available would do well, but whether there are imaginable computers which would do well. But this is only the short answer. We shall see this question in a different light later.

4. Digital Computers

The idea behind digital computers may be explained by saying that these machines are intended to carry out any operations which could be done by a human computer. The human computer is supposed to be following fixed rules; he has no authority to deviate from them in any detail. We may suppose that these rules are supplied in a book, which is altered whenever he is put on to a new job. He has also an unlimited

supply of paper on which he does his calculations. He may also do his multiplications and additions on a “desk machine”. but this is not important.

If we use the above explanation as a definition we shall be in danger of circularity of argument. We avoid this by giving an outline. of the means by which the desired effect is achieved. A digital computer can usually be regarded as consisting of three parts:

- (i) Store.
- (ii) Executive unit.
- (iii) Control.

The store is a store of information, and corresponds to the human computer’s paper, whether this is the paper on which he does his calculations or that on which his book of rules is printed. In so far as the human computer does calculations in his bead a part of the store will correspond to his memory.

The executive unit is the part which carries out the various individual operations involved in a calculation. What these individual operations are will vary from machine to machine. Usually fairly lengthy operations can be done such as “Multiply 3540675445 by 7076345687” but in some machines only very simple ones such as «Write down 0» are possible.

We have mentioned that the “book of rules” supplied to the computer is replaced in the machine by a part of the store. It is then called the “table of instructions”. It is the duty of the control to see that these instructions are obeyed correctly and in the right order. The control is so constructed that this necessarily happens.

The information in the store is usually broken up into packets of moderately small size. In one machine, for instance, a packet might consist of ten decimal digits. Numbers are assigned to the parts of the store in which the various packets of information are stored, in some systematic manner. A typical instruction might say:

“Add the number stored in position 6809 to that in 4302 and put the result back into the latter storage position”.

Needless to say it would not occur in the machine expressed in English. It would more likely be coded in a form such as 6809430217. Here 17 says which of various possible operations is to be performed on the two numbers. In this case the operation is that described above, viz., “Add the number”. It will be noticed that the instruction takes up 10 digits and so forms one packet of information, very conveniently. The control will normally take the instructions to be obeyed in the order of the positions in which they are stored, but occasionally an instruction such as.

“Now obey the instruction stored in position 5606, and continue from there” may be encountered, or again

“If position 4505 contains 0 obey next the instruction stored in 6707, otherwise continue straight on”.

Instructions of these latter types are very important because they make it possible for a sequence of operations to be replaced over and over again until some condition is fulfilled, but in doing so to obey, not fresh instructions on each repetition, but the same ones over and over again. To take a domestic analogy. Suppose Mother wants Tommy to call at the cobbler’s every morning on his way to school to see if her shoes are done, she can ask him afresh every morning. Alternatively she can stick up a notice once and for all in the hall which he will see when he leaves for school and which tells

him to call for the shoes, and also to destroy the notice when he comes back if he has the shoes with him.

The reader must accept it as a fact that digital computers can be constructed, and indeed have been constructed, according to the principles we have described, and that they can in fact mimic the actions of a human computer very closely.

The book of rules which we have described our human computer as using is of course a convenient fiction. Actual human computers really remember what they have got to do. If one wants to make a machine mimic the behaviour of the human computer in some complex operation one has to ask him how it is done, and then translate the answer into the form of an instruction table. Constructing instruction tables is usually described as "programming". To "programme a machine to carry out the operation A" means to put the appropriate instruction table into the machine so that it will do A.

An interesting variant on the idea of a digital computer is a "digital computer with a random element". These have instructions involving the throwing of a die or some equivalent electronic process; one such instruction might for instance be, "Throw the die and put the-resulting number into store 1000". Sometimes such a machine is described as having free will (though I would not use this phrase myself). It is not normally possible to determine from observing a machine whether it has a random element, for a similar effect can be produced by such devices as making the choices depend on the digits of the decimal for.

Most actual digital computers have only a finite store. There is no theoretical difficulty in the idea of a computer with an unlimited store. Of course only a finite part can have been used at any one time. Likewise only a finite amount can have been constructed, but we can imagine more and more being added as required. Such computers have special theoretical interest and will be called infinitive capacity computers.

The idea of a digital computer is an old one. Charles Babbage, Lucasian Professor of Mathematics at Cambridge from 1828 to 1839, planned such a machine, called the Analytical Engine, but it was never completed. Although Babbage had all the essential ideas, his machine was not at that time such a very attractive prospect. The speed which would have been available would be definitely faster than a human computer but something like 1 00 times slower than the Manchester machine, itself one of the slower of the modern machines, the storage was to be purely mechanical, using wheels and cards.

The fact that Babbage's Analytical Engine was to be entirely mechanical will help us to rid ourselves of a superstition. Importance is often attached to the fact that modern digital computers are electrical, and that the nervous system also is electrical. Since Babbage's machine was not electrical, and since all digital computers are in a sense equivalent, we see that this use of electricity cannot be of theoretical importance. Of course electricity usually comes in where fast signalling is concerned, so that it is not surprising that we find it in both these connections. In the nervous system chemical phenomena are at least as important as electrical. In certain computers the storage system is mainly acoustic. The feature of using electricity is thus seen to be only a very superficial similarity. If we wish to find such similarities we should look rather for mathematical analogies of function.

5. Universality of Digital Computers

The digital computers considered in the last section may be classified amongst the “discrete-state machines”. These are the machines which move by sudden jumps or clicks from one quite definite state to another. These states are sufficiently different for the possibility of confusion between them to be ignored. Strictly speaking there, are no such machines. Everything really moves continuously. But there are many kinds of machine which can profitably be thought of as being discrete-state machines. For instance, in considering the switches for a lighting system it is a convenient fiction that each switch must be definitely on or definitely off. There must be intermediate positions, but for most purposes we can forget about them. As an example of a discrete-state machine we might consider a wheel which clicks round through 120 once a second, but may be stopped by a lever which can be operated from outside; in addition a lamp is to light in one of the positions of the wheel. This machine could be described abstractly as follows. The internal state of the machine (which is described by the position of the wheel) may be q_1 , q_2 or q_3 . There is an input signal i_0 . or i_1 (position of lever). The internal state at any moment is determined by the last state and input signal according to the table.

Юрий Григорьевич

ШПАКОВСКИЙ,

главный редактор

журнала «Вестник

Университета имени

О.Е. Кутафина (МГЮА)»,

доктор юридических наук,

профессор

Познавательное о разном¹

1. Интересные исторические факты

Царский развод по-грузински!

Жениться по любви не может ни один король? Слова нехитрой советской песенки как нельзя лучше свидетельствовали о негласной традиции, которую нельзя было нарушать 200, 300 или 500 лет назад.

И если в интересах страны требовалось монархам заключить брак с нелюбимым человеком, то глава государства шел на это, понимая, что возможности просто так развестись не будет. Крепость семейных уз в Средние века была обусловлена сильным религиозным влиянием.

Однако королевские разводы были всегда. Причем стоящим во главе государства расторгнуть узы брака было сложнее всего: ведь они были примером для тех, кто жил в государстве.

А теперь мысленно перенесемся в 1187 год, в тронный зал в Тбилиси. Грузинская царица Тамара стоит перед церковным собором и произносит слова, от которых у вельмож холодеет внутри: «Я не должна отдыхать под тенью оскверненного дерева». Она требует развода. И не просто развода — она публично обвиняет своего мужа, русского князя Юрия, сына Андрея Боголюбского, в пьянстве и разврате. Скандал грандиозный.

Тамаре 21 год. Она правительница Грузии, «царь царей», которую народ боготворит. Ее называют мудрой, справедливой, почти святой. А ее муж — красивый, но порочный князь, которого грузины прозвали «Георгий Руси».

В XII в. женщины не разводились. Тем более царицы. Что заставило Тамару пойти на этот шаг?



Тамара родилась около 1166 г. Ее династия — Багратионы, древнейшая царская семья Грузии, которая, по преданию, вела род от самого библейского царя Давида. Отец — царь Георгий III. Мать — красавица Бурдухан, дочь осетинского царя.

У Георгия III не было сыновей. И он вместо того, чтобы менять жен в попытках добиться рождения наследника, принимает простое решение: короновать 12-летнюю дочь как соправительницу. Мало кто верил, что девочка сможет удержать власть. Но царь был непреклонен.

Чтобы закрепить ее статус, он приказывает чеканить новую монету. Впервые в истории Грузии на монете появляется женское имя — Тамара.

В 1184 г. Георгий III умер. Восемнадцатилетняя Тамара стала единоличной правительницей.

¹ Материал подготовлен с использованием интернет-ресурсов.

Долго править в одиночестве ей не дали. Придворный совет — Дарбази — немедленно стал требовать: царица должна выйти замуж. Стране нужен наследник и политический союз. Нужен мужчина рядом, иначе соседи не будут воспринимать Грузию всерьез.

Выбор пал на Юрия — младшего сына владимирского князя Андрея Боголюбского. Вскоре Юрий прибыл в Грузию. Тамара попросила дать ей время присмотреться к жениху. Но совет настаивал: свадьба должна состояться немедленно.

Юрий оказался порочным до предела — предавался пьянству, разврату... Тамара терпела, уговаривала, посылала к нему монахов, лично, при свидетелях просила исправиться. Грузинские летописи сохранили подробности этих разговоров: она была настойчива, терпелива и дипломатична. Но Юрий не менялся.

В конце концов все средства истощились. По преданию, объявляя о разводе, царица бросила бывшему мужу: «И я не в силах выпрямить тень кривого дерева... отряхиваю пыль, которая пристала ко мне через тебя».

Юрия щедро одарили и выслали в Константинополь. Развод по тем временам был шагом крайним. Но Юрий не смирился. Через четыре года Юрий вернулся. Он собрал армию из недовольных грузинских феодалов — тех, кого Тамара лишила привычных кормушек, — и попытался силой вернуть себе трон и жену. Тамара немедленно мобилизовала верные войска и разбила его. Через два года Юрий предпринял вторую попытку, но его уже никто не поддержал. Он исчез из истории. Никто не знает, где и когда он умер.

Крайне важно, что Ватикан не играл никакой роли в разводе царицы Тамары. Это важный исторический момент: решение о расторжении брака с Юрием (Георгием) было принято исключительно внутри Грузинского царства.

В 1187 г. Тамара убедила государственный совет одобрить развод. Но непростой в этой истории была роль церкви. В ту эпоху развод в православном мире был крайне редким и сложным явлением, поскольку брак считался священным союзом. Однако Грузинская православная церковь в итоге дала согласие на расторжение брака. Историки предполагают, что это могло быть связано с реформами, которые Тамара провела в церковной среде в начале своего правления: она поставила на ключевые посты лояльных ей людей и укрепила материальное положение церковных учреждений.

Таким образом, решение было внутренним делом Грузии и ее церковной иерархии, а не результатом какого-либо вмешательства со стороны Рима.

А Тамара вскоре счастливо вышла замуж за друга детства, осетинского князя Давида Сослана.

Ее имя прочно вошло в историю Грузии. За годы правления Тамары строились храмы, распространялось православие. Она отменила смертную казнь и потребовала судить строго всех — начиная с себя.

Сами грузины не зовут ее «царицей». Титул «мепе» (царь) не имел женской формы, так подчеркивали, что Тамара правила сама, как государь, а не как жена царя. Поэтому по-грузински она буквально — Царь Тамар.

Село или деревня?



Сегодня вряд ли кто-то с уверенностью может сказать, чем отличается деревня от села. Тем более, что в обиходе жителей деревень, сел, хуторов, станиц и других небольших населенных пунктов называют одинаково — сельский житель.

Село и деревня — небольшие населенные пункты. Иногда люди путают эти понятия, хотя исторически между деревней и селом были большие различия. Село было центром приходской жизни, а деревня — маленьким поселением на несколько дворов. Однако в современной России можно встретить небольшие тихие села и крупные развитые деревни. Так в чем же различие между деревней и селом и как статус этих населенных

пунктов регулировался законом?

С конца XVII в. деревня представляла собой крестьянское селение. Причем тогда деревней мог считаться даже один дом с двором. Но так как крестьяне часто селились рядом друг с другом, то деревнями называли несколько дворов с огородом и пашнями. Основным видом деятельности было сельское хозяйство.

Село — это населенный пункт крупнее деревни как по территории, так и по количеству жителей. Еще в царское время говорили «село с деревнями», описывая земли около села. Сейчас село считается хозяйственным и административным центром для близлежащих деревень.

До Революции 1917 г. в селе, в отличие от деревни, обязательно присутствовала церковь. Признак этот закрепился рано — уже к XIV в. наличие церкви становится ключевой приметой села. И дело было не столько в вере, сколько в бюрократии. Церковь работала как местное МФЦ: там регистрировали рождения, браки и смерти, там же собирались жители для решения важных вопросов, при храме держали церковно-приходскую школу. Появлялся храм — появлялась и вся административная жизнь. Статус можно было и потерять. Если, например, деревянная церковь ветшала, разрушалась или сгорела в грозу, прихожан приписывали к соседнему храму, и село превращалось в деревню.

Также в селах была развита легкая промышленность — функционировали мельницы и кузницы, в то время как в деревнях большая часть жителей занималась ручным трудом в поле или в огороде, обучала хозяйству детей.

Уже после появления земств в 1864 г. младших членов семьи отправляли из деревень на обучение в более крупные села. В ходу была народная медицина: жители собирали целебные травы и обращались к знахарям.

Так что, если едете по России и видите старую церковь посреди «деревни» — знайте: когда-то это было село.

После Революции 1917 г. различия начали стираться. При советской власти селом могли назвать крупные деревни и бывшие приходские центры, наличие церкви, мельниц и кузниц перестали считать определяющим для статуса поселения. Но в целом деревня была не так хорошо обустроена, как село. В селе были школа, фельдшерский пункт, а иногда больница, дом культуры или клуб, сельсовет.

А в деревнях даже магазины были не везде. Исключение составляли деревни с развитой инфраструктурой, которые относились к зажиточным колхозам.

Сегодня и село, и деревня относятся к сельским населенным пунктам. Этот термин упоминается в Федеральном законе от 20.03.2025 № 33-ФЗ «Об общих принципах организации местного самоуправления в единой системе публичной власти». При этом четкая разница между селом и деревней в Законе не проведена.

Региональные власти интерпретируют федеральные нормы с учетом местной специфики и учитывают исторически сложившиеся топонимы. Например, сибирские и другие отдаленные регионы иногда присваивают статус села поселениям с меньшей численностью населения, чем центральные области страны. В северных территориях учитывают фактор сезонной доступности населенных пунктов. Южные регионы традиционно различают станицы, хутора и села, опираясь на казачьи традиции землепользования.

Следует заметить, что в советское время в обиход прочно вошло понятие «периферия». Во многом негативный смысл этого понятия был связан с распределением выпускников столичных вузов, когда после окончания учебы в вузе специалиста могли отправить на несколько лет куда угодно, например в затерянный горный аул или плохо обустроенное дальневосточное поселение. Правда, в основном распределение любимых чад было проблемой для столичных семей.

Распределение после вуза затрагивало каждого молодого специалиста. Имея связи, можно было остаться в родном городе, конечно, если были подходящие места. Жителей маленьких населенных пунктов распределение не особо пугало, к тому же они могли еще и получить жилье на новом месте. А вот из крупных городов, особенно из Москвы, уезжать не хотелось никому. Часто такое распределение становилось трагедией для всей семьи.



Ахмет Китаев. «Родное дитя на периферию?!» (1954)

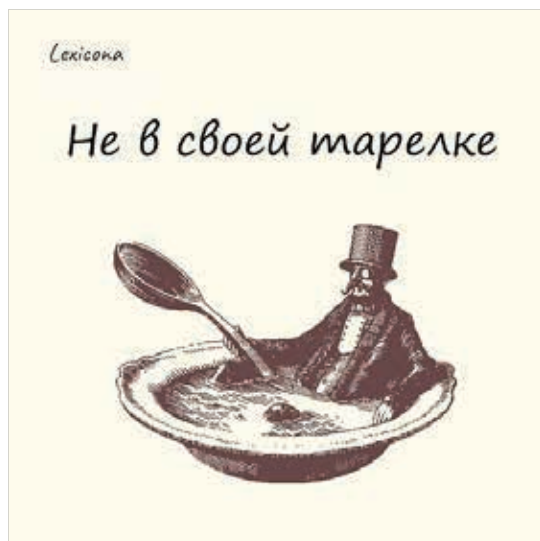
2. Почему мы так говорим?

Не в своей тарелке

Выражение «не в своей тарелке» означает, что человек чувствует себя некомфортно, неудобно, стесненно. Это выражение стало таким привычным и понятным, что его странноватый смысл совершенно не ощущается теми, кто его произносит. Но в свое время, примерно 150 лет назад, оно наделало немало шума.

Переводчик, который, взявшись переложить на родную речь модный французский романчик, допустил кучу ошибок. Даже в таком распространенном выражении, как *n'être pas dans son assiette* (не в свойственном ему положении), он умудрился перепутать похожие слова — «положение» и «тарелка» — и, особо не раздумывая над тем, что получилось, решил, что сойдет и так.

В результате же это выражение прочно вошло не только в наш лексикон, но и в классическую литературу. Александр Грибоедов, бывший заядлым театралом,



разумеется, не мог пройти мимо столь блистательного ляпа и вложил безграмотную фразу в уста Фамусова: «Любезнейший! Ты не в своей тарелке. С дороги нужен сон. Дай пульс. Ты не здоров». Слова эти должны были характеризовать то самое смешение языков, франко-нижегородский диалект, над которым издевался Грибоедов. Однако с легкой руки Александра Сергеевича бездумная фраза обрела смысл и прижилась в русском языке в новом значении, о котором и не подозревают французы. Воистину, «нам не дано предугадать, как наше слово отзовется».

Лермонтов писал в эпиграмме на Булгакова:

*На вздор и шалости ты хват
И мастер на безделки.
И, шутовской надев наряд,
Ты был в своей тарелке.*

А у Тургенева в комедии «Где тонко, там и рвется» мы можем встретить: «...да здравствуют насмешливость, веселость и злость! Вот я опять в своей тарелке!»

Ксива

Наверное, слово «ксива» прочно вошло в наш лексикон. И связано оно прежде всего со служебным удостоверением сотрудников спецслужб. Без удостоверения сотрудник любого силового ведомства — это обычный гражданин, не имеющий особых прав и полномочий при осуществлении своих действий. Многие не раз слышали фразы «У него крутая ксива», «Живи красиво, если у папы ксива» и т.д.



Однако этому жаргонному словечку самое меньшее три тысячи лет. Именно ксивы спрашивали иерусалимские стражники у Христа и его апостолов, потому что на арамейском это слово означает бумаги, документы. А в русский жаргон оно пришло через образованных еврейских бандитов и мошенников, которые в начале XX в. составляли немалую часть криминального мира Одессы и Киева.

Слово «ксива» заимствовано из идиша. В идише существительное «ксива» означает нечто написанное, запись, в том числе письмо или документ.

Еврейское происхождение (из идиша и иврита) вообще имеют около 10 % слов криминального жаргона, например:

«пацан», «шмон», «шухер», «малина», «блат», «параша».

На иврите «балат» означало «тихо» — это слово использовалось еще в Ветхом завете. На идише, в зависимости от произношения, оно могло означать «близкий» или «ладонь». Когда криминальные деятели теневой экономики приходили к согласию, они били по рукам — это и был блат.

Слово «ништак» тоже пришло к нам из иврита. Там оно звучит «ништак» и переводится как «мы успокоимся».

«Шмон» — читается как «шмонэ» и переводится с иврита как «8». В жаргоне «шмон» означает обыск. При чем тут 8? Считается, что в царских тюрьмах

ежедневно в 8 часов вечера, когда заключенных уводили на ужин, охранники проходили с обыском по камерам.

Всем известное слово «халява» переводится с иврита как «молоко». В еврейских общинах издревле существовал обычай по пятницам раздавать молоко неимущим. И, соответственно, это молоко они называли «халяв».

Слово «шара», или «на шару», происходит от ивритского «шеар» — остатки. Шеаром называли то, что остается у продавца, а именно непригодное для продажи.

Остаться с носом

Почему остаться с носом плохо?

Просто 300 лет назад, когда это выражение появилось, слово «нос» имело еще одно значение, по важности почти не уступавшее основному. Означало оно «взятка» или «подношение», «приношение». Если человек, понесший взятку, не сумел договориться с чиновником, он, соответственно, оставался со своим «носом».

По другой версии, здесь имеется в виду тот «нос», который жених по древнему обычаю подносил родителям невесты (т.е. приношение, подарок, выкуп). Если жениху отказывали, подарок отвергали, то жених оставался «с носом».



Конь педальный

Выражение «конь педальный» знакомо многим как ироничное или оскорбительное замечание, адресованное человеку, которого считают недостаточно сообразительным. Однако не все знают, что эта фраза родилась благодаря детской игрушке, выпущенной в СССР в 1950-х гг.

В послевоенные годы советские производители старались радовать детей доступными и оригинальными игрушками. Одной из таких попыток стал «конь педальный» — гибрид трехколесного велосипеда и лошадки-качалки.

Самые блестящие умы нашей промышленности были брошены на то, чтобы создать идеальный гибрид лошадки на колесиках с велосипедом. Мутант получил официальное наименование «конь педальный» и в конце 1950-х гг. был запущен в массовое производство.

Однако игрушка была крайне неудобной и сложной в использовании. Педали находились так далеко от седла, что ребенку приходилось буквально тянуться, чтобы ими пользоваться. Вместо привычного руля конь оснащался поводьями, которые никак не способствовали маневренности. При этом металлическая конструкция издавала громкие звуки, а само устройство было тяжелым и неповоротливым.

Несмотря на эти недостатки, конь педальный был желанным объектом для советских детей, а обладатели этой игрушки вызывали зависть у сверстников.

С течением времени конь педальный исчез с прилавков магазинов. Однако выражение вошло в обиход как символ чего-то нелепого или неудачного.





ISSN 2311-5998



9 772311 599771 >