

№ 2 (101)  
2023

# ВЕСТНИК

## УНИВЕРСИТЕТА

имени О.Е. Кутафина (МГЮА)

Право есть  
искусство добра  
и справедливости

*Jus est ars  
boni et aequi*

В номере

### Выпуск КИБЕРПРАВО

#### ВЕКТОР ЮРИДИЧЕСКОЙ НАУКИ

- 25** Полякова Т. А., Троян Н. А.  
Актуальные проблемы систематизации законодательства России под влиянием цифровых технологий в период цифровой трансформации
- 42** Добробаба М. Б.  
Понятие персональных данных: проблема правовой определенности
- 62** Яковлева А. В.  
Проблемы правового обеспечения в становлении института кибергиены
- 71** Минбалеев А. В., Сторожакова Е. Э.  
Проблемы правовой охраны персональных данных в процессе использования нейронных сетей

#### ЗАРУБЕЖНЫЙ ОПЫТ

- 162** Королев С. В., Лялина И. С.  
Интернет-право и кибербезопасность КНР

№ 2 (101)  
2023

# ВЕСТНИК УНИВЕРСИТЕТА имени О.Е. Кутафина (МГЮА)

Выпуск  
КИБЕРПРАВО

Издается с 2014 года  
Выходит один раз в месяц

## Председатель редакционного совета:

*БЛАЖЕЕВ Виктор Владимирович* — ректор Университета имени О.Е. Кутафина (МГЮА), профессор кафедры гражданского и административного судопроизводства, кандидат юридических наук, доцент, г. Москва, Россия

## Заместитель председателя редакционного совета:

*ГРАЧЕВА Елена Юрьевна* — заведующий кафедрой финансового права, 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:

*СЕВРЮГИНА Ольга Александровна* — эксперт 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 Саратовской государственной юридической академии, доктор юридических наук, профессор, г. Саратов, Россия

*БЕЗВЕРХОВ Артур Геннадьевич* — декан юридического факультета Самарского национального исследовательского университета имени академика С. П. Королева, доктор юридических наук, профессор, г. Самара, Россия

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

*БУКАЛЕРОВА Людмила Александровна* — заведующий кафедрой уголовного права, уголовного процесса и криминалистики Российского государственного университета дружбы народов, 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

*ВОСКОБИТОВА Лидия Алексеевна* — заведующий кафедрой уголовно-процессуального права Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, 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* — заведующий кафедрой экологического и природоресурсного права Университета имени О.Е. Кутафина (МГЮА), 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 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 РФ, профессор Института международных отношений и социально-политических наук Московского государственного лингвистического университета, доктор философских наук, профессор, г. Москва, Росси



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), 2023

2/2023

**КОМАРОВА Валентина Викторовна** — заведующий кафедрой 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 РФ, доктор юридических наук, г. Москва, Россия

**ЛЮТОВ Никита Леонидович** — профессор кафедры трудового права и права социального обеспечения Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, 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, 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

**РОМАНОВА Виктория Валерьевна** — заведующий кафедрой энергетического права Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, г. Москва, Россия

**РОССИНСКАЯ Елена Рафаиловна** — директор Института судебных экспертиз, заведующий кафедрой судебных экспертиз Уни-

верситета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

**РЫЛЬСКАЯ Марина Александровна** — директор Института проблем эффективного государства и гражданского общества Финансового 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 теории государства и права (МГЮА), доктор юридических наук, доцент, 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

<b>В журнале публикуются статьи по научным специальностям группы 5.1 «Право» (юридические науки)</b>	5.1.1. Теоретико-исторические правовые науки. 5.1.2. Публично-правовые (государственно-правовые) науки. 5.1.3. Частноправовые (цивилистические) науки. 5.1.4. Уголовно-правовые науки. 5.1.5. Международно-правовые науки.
<b>РЕГИСТРАЦИЯ СМИ</b>	Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) ПИ № ФС77-67361 от 5 октября 2016 г.
<b>ISSN</b>	2311-5998 (Print), 2782-6163 (Online)
<b>ПЕРИОДИЧНОСТЬ</b>	12 раз в год
<b>УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ</b>	Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)» Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
<b>АДРЕС РЕДАКЦИИ</b>	Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993 Тел.: 8 (499) 244-88-88 (доб. 687). E-mail: vestnik@msal.ru
<b>ПОДПИСКА И РАСПРОСТРАНЕНИЕ</b>	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
<b>ТИПОГРАФИЯ</b>	Отпечатано в Издательском центре Университета имени О.Е. Кутафина (МГЮА) Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
<b>ВЫПУСКНЫЕ ДАННЫЕ</b>	Дата выхода в свет: 29.03.2023 Объем 23,62 усл. печ. л. (14,42 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 А. Б. Рыбакова

Компьютерная верстка Д. А. Беляков

# COURIER

## OF THE KUTAFIN MOSCOW STATE LAW UNIVERSITY (MSAL)

№ 2 (101)  
2023

Edition  
**CYBER LAW**

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), Professor of the Department of Civil and Administrative Court Proceedings, Cand. Sci. (Law), Associate Professor, Moscow, Russia

### Vice-Chairperson of the Council of Editors:

*GRACHEVA Elena Yurievna* — Head of the Department of Financial Law, 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:

*SEVRYUGINA Olga Alexandrovna* — Expert 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 of Saratov State Academy of Law, Dr. Sci. (Law), Professor, Saratov, Russia

*BEZVERKHOV Arthur Gennadevich* — Dean of the Law Faculty of the National Research University named after Academician Sergey P. Korolev, Dr. Sci. (Law), Professor, Samara, 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* — Head of the Department of Criminal Law, Criminal Procedure and Criminology of the Peoples' Friendship University of Russia, 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

*VOSKOBITOVA Lidia Alekseevna* — Head of the Department of Criminal Procedure Law of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, 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 of Kutafin Moscow State Law University (MSAL), 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* — Head of the Department of Environmental and Natural Resources Law of Kutafin Moscow State Law University (MSAL), 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 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, RANEPА University; Professor, Institute of International Relations and Socio-Political Sciences, Moscow State Linguistic University, Dr. Sci. (Philosophy), 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), 2023

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

*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

*LYUTOV Nikita Leonidovich* — Head of the Department of Labor and Social Security Law of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, 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 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

*ROMANOVA Victoria Valeryevna* — Head of the Department of Energy Law of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Moscow, Russia

*ROSSINSKAYA Elena Rafailovna* — Director of the Forensic Examination Institute, 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), Associate 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 Aleksey Vladimirovich* — Head of the Department of information law and digital technologies of the Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor

<b>The Journal publishes research papers written on scientific specialties of Group 5.1 «Law» (Legal Sciences)</b>	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.	
<b>THE CERTIFICATE OF MASS MEDIA REGISTRATION</b>	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	
<b>ISSN</b>	2311-5998 (Print), 2782-6163 (Online)	
<b>PUBLICATION FREQUENCY</b>	12 issues per year	
<b>FOUNDER AND PUBLISHER</b>	Federal State Budgetary Educational Institution of Higher Education "Kutafin Moscow State Law University (MSAL)", 9 Sadovaya-Kudrinskaya ul., Moscow, Russia, 125993	
<b>EDITORIAL OFFICE. POSTAL ADDRESS</b>	9 Sadovaya-Kudrinskaya ul., Moscow, Russia, 125993 Tel.: +7 (499) 244-88-88 (ext. 687) E-mail: <a href="mailto:vestnik@msal.ru">vestnik@msal.ru</a>	
<b>SUBSCRIPTION AND DISTRIBUTION</b>	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	
<b>PRINTING HOUSE</b>	Printed in Publishing Center of Kutafin Moscow State Law University (MSAL) 9 Sadovaya-Kudrinskaya ul., Moscow, Russia, 125993	
<b>SIGNED FOR PRINTING</b>	29.03.2023 Volume: 23,62 conventional printer's sheets (14,42 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>		
<b>Editor L. A. Munkueva</b>	<b>Proof-reader A. B. Rybakova</b>	<b>Computer layout D. A. Belyakov</b>

# СОДЕРЖАНИЕ

СЛОВО К ЧИТАТЕЛЮ .....	8
УНИВЕРСИТЕТСКАЯ ХРОНИКА .....	11
ВЕКТОР ЮРИДИЧЕСКОЙ НАУКИ	
Развитие законодательства в период цифровой трансформации общества	
<b>Полякова Т. А., Троян Н. А.</b> Актуальные проблемы систематизации законодательства России под влиянием цифровых технологий в период цифровой трансформации .....	25
<b>Абдусаламов Р. А.</b> Правовое регулирование использования информационных технологий в сфере высшего образования в Российской Федерации .....	34
<b>Добробаба М. Б.</b> Понятие персональных данных: проблема правовой определенности .....	42
<b>Чубукова С. Г.</b> Квасисубъекты в киберправе .....	53
<b>Яковлева А. В.</b> Проблемы правового обеспечения в становлении института кибергигиены .....	62
Искусственный интеллект	
<b>Минбалеев А. В., Сторожакова Е. Э.</b> Проблемы правовой охраны персональных данных в процессе использования нейронных сетей .....	71
<b>Таран К. К.</b> Формирование в ЕС нормативно-правовой базы, регулирующей отношения по использованию искусственного интеллекта .....	80
Информационная безопасность гражданского общества	
<b>Соловкин С. В.</b> Автоматизированный сбор данных о человеке: неявные принципы правового регулирования .....	90
<b>Химченко А. И.</b> Формирование цифровой среды доверия: динамика развития инфраструктуры идентификации при реализации цифровых услуг .....	101
<b>Селюк А. С.</b> Защита персональных данных в цифровом пространстве .....	110
<b>Евсиков К. С.</b> К вопросу о правовом регулировании интернет-голосования .....	120

Правоотношения в цифровой сфере

**Сушкова О. В.**

Правовые характеристики качества патентов  
в сфере информационных технологий: постановка проблемы ..... 129

**Пашнина Т. В.**

О целесообразности совершенствования системы  
правового регулирования информационных отношений  
в сфере библиотечного дела в контексте киберправа ..... 137

**Шельменков В. Н.**

Основные принципы обработки правовой информации  
в информационных правовых системах ..... 146

**Холодная Е. В.**

О некоторых юридически значимых  
особенностях технологий облачных вычислений ..... 153

ЗАРУБЕЖНЫЙ ОПЫТ

**Королев С. В., Лялина И. С.**

Интернет-право и кибербезопасность КНР ..... 162

Трибуна молодого ученого

**Байгарин Р. Т.**

Правовые проблемы обеспечения кибербезопасности  
генетических данных в Российской Федерации ..... 168

**Журков А. А.**

Актуальные вопросы правового регулирования  
искусственного интеллекта в условиях необходимости  
обеспечения национального цифрового суверенитета  
в период санкционного давления ..... 177

**Ткаченко А. А.**

Институт личной информации религиозного характера:  
определение и структура. Особенности оборота  
такой информации в киберпространстве ..... 187

Право в историческом преломлении

**Шпаковский Ю. Г.**

Кибернетика в СССР ..... 196  
Кому служит кибернетика ..... 198

Памятники права

Постановление ЦК КПСС и Совета министров СССР  
от 8 октября 1970 г. № 849-291 ..... 210

ПОСТСКРИПТУМ

**Шпаковский Ю. Г.**

«Безбожники» ..... 218

# CONTENTS

NOTE TO THE READERS .....	8
UNIVERSITY CHRONICLE .....	11
VECTOR OF LEGAL SCIENCE	
Development of legislation in the period of digital transformation of society P	
<b><i>Polyakova T. A., Troyan N. A.</i></b> Current Problems of Russian Legislation Systematization under the Influence of Digital Technologies in the Conditions of Digital Transformation .....	25
<b><i>Abdusalamov R. A.</i></b> Legal Regulation of the Use of Information Technologies in Higher Education in the Russian Federation .....	34
<b><i>Dobrobaba M. B.</i></b> Concept of personal data: the Problem of Legal Certainty .....	42
<b><i>Chubukova S. G.</i></b> Quasi-subjects in cyber law .....	53
<b><i>Iakovleva A. V.</i></b> Problems of Legal Support of the Cyber Hygiene Institute .....	62
Artificial intelligence P	
<b><i>Minbaleev A. V., Storozhakova E. E.</i></b> Problems of legal protection of personal data in the process of using neural networks .....	71
<b><i>Taran K. K.</i></b> Constituting a regulatory framework in the EU that regulates relations on the using artificial intelligence .....	80
Information security of civil society P	
<b><i>Solovkin S. V.</i></b> Automated Collection of Data on a Person: Implicit Principles of Legal Regulation .....	90
<b><i>Khimchenko A. I.</i></b> Formation of a digital environment of trust: dynamics of development of identification infrastructure in the implementation of digital services .....	101
<b><i>Selyuk A. S.</i></b> Protection of Personal Data in the Digital Space .....	110
<b><i>Evsikov K. S.</i></b> On the Issue of Legal Regulation of I-Voting .....	120

Legal relations in the digital sphere P

**Sushkova O. V.**

- Legal Characteristics of the Quality of Patents  
in the Sphere of Information Technologies:  
Statement of the Problem ..... 129

**Pashnina T. V.**

- On the Expediency of Improving the System  
of Legal Regulation of Information Relations  
in the Field of Librarianship in the Context of Cyber Law ..... 137

**Shelmenkov V. N.**

- Basic principles of processing legal information  
in information legal systems ..... 146

**Kholodnaya E. V.**

- About some Legally Significant Features  
of Cloud Computing Technologies ..... 153

FOREIGN EXPERIENCE

**Korolev S. V., Lyalina I. S.**

- Internet law and cybersecurity of the PRC ..... 162

YOUNG RESEARCHERS' PERSPECTIVE

**Baygarin Ruslan T.**

- Legal challenges in ensuring the cybersecurity  
of genetic data in the Russian Federation ..... 168

**Zhurkov A. A.**

- Topical issues of legal regulation of artificial intelligence  
in the context of the need to ensure national digital  
sovereignty during the period of sanctions pressure ..... 177

**Tkachenko A. A.**

- The Institution of Personal Information  
of Religious Nature: Definition, Structure,  
the Specificities of the Circulation in Cyberspace ..... 187

LAW IN HISTORICAL REFRACTION

Some Pages of the Past Periodicals p

**Shpakovsky Yu. G.**

- Cybernetics in the USSR ..... 196  
Who Serves Cybernetics ..... 198

Legal Monuments p

- Resolution of the Central Committee  
of the CPSU and the Council of Ministers  
of the USSR of October 8, 1970 No. 849-291 ..... 210

POSTSCRIPT

**Shpakovsky Yu. G.**

- “Atheists” ..... 218

## Слово к читателю



### Уважаемые читатели!

Вашему вниманию представлен очередной тематический выпуск журнала «Вестник Университета имени О.Е. Кутафина (МГЮА)», посвященный проблемам киберправа. Развитие этого направления в современной юридической науке актуализировалось во многом в связи с реализацией в Университете имени О.Е. Кутафина (МГЮА) проекта «Киберправо», реализуемого по программе стратегического академического лидерства «Приоритет-2030».

В настоящее время совершенствование законодательной базы России должно строиться на решении качественно новых проблем, вызванных существующим технологическим прогрессом, появлением новых вызовов и угроз в цифровой среде, активным использованием различных цифровых технологий и качественно новым развитием информационного общества в России.

Сегодня в связи с повышением общественной значимости отношений в киберсреде существует потребность развития отдельной подотрасли информационного права — киберправа. Правовое регулирование отношений в сфере обеспечения кибербезопасности, правовое обеспечение развития цифровой экономики в киберпространстве, развитие правового регулирования цифрового профилирования, отношений в сфере использования искусственного интеллекта в сети Интернет активно развивается, но во многих сферах и направлениях отсутствуют концептуальные подходы и модели правового регулирования.

Специфика киберпространства во многом выражается в системе специальных субъектов и формирующихся квазисубъектов, которые приобретают особый правовой статус. Системы искусственного интеллекта, киберфизические системы, роботы, цифровые платформы все чаще обозначаются как субъекты права или квазисубъекты, что требует особого осмысления юридической наукой.

Исследования по данным вопросам нашли отражение в настоящем номере. Так, исследуются актуальные проблемы систематизации законодательства России в условиях цифровой трансформации, поднимается вопрос о формировании отдельного института «кибергиены» в системе правового обеспечения информационной безопасности.

Значительное место в номере уделяется актуальным вопросам правовой охраны персональных данных. Активное развитие законодательства и правоприменительной практики в сфере персональных данных порождает много вопросов о правовой природе персональных данных, требованиях к ним. На практике все больше проблем возникает в связи с использованием персональных данных в рамках функционирования нейронных сетей и искусственного интеллекта. Очень много нареканий вызывает рост случаев использования автоматизированного сбора данных о человеке, что предполагает выработку государствами новых механизмов их защиты. Все эти вопросы также нашли свое отражение в специальной рубрике журнала.

В представленном выпуске публикуются научные статьи, посвященные актуальным проблемам современного цифрового государства, анализу проблем правового регулирования интернет-голосования, дистанционного электронного государства.

Отдельно необходимо упомянуть вопросы правового регулирования использования информационных технологий в сфере высшего образования в Российской Федерации в условиях цифровой трансформации.

В статьях молодых исследователей поднимаются актуальные сегодня проблемы обеспечения кибербезопасности генетических данных, формирования института личной информации религиозного характера и особенностей ее обращения в киберпространстве. Данные вопросы будут интересны не только начинающим ученым.

Полагаем, что публикуемые в настоящем выпуске журнала труды и информационные материалы вызовут интерес у широкого круга как представителей юридической науки и практики, так и специалистов, занимающихся современными вопросами правового обеспечения отношений в цифровой среде.

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

### Конференции, круглые столы, семинары

#### IX Зимняя школа молодых ученых — 2023 «Киберправо и кибербезопасность»



В Университете имени О.Е. Кутафина (МГЮА) с 30 января по 3 февраля 2023 г. проходила IX Зимняя школа молодых ученых «Киберправо и кибербезопасность». Пятидневная программа школы предусматривала проведение лекций, мастер-классов, круглых столов и неформальных бесед с ведущими российскими учеными и практиками, анализ результатов «мозговых штурмов».

Мероприятия проводились в загородном досуговом комплексе Университета «Малюшина дача».

Первый день работы школы открыл ее руководитель — проректор по научно-исследовательской деятельности, доктор юридических наук, профессор, заслуженный деятель науки РФ Владимир Синюков.

В приветственной речи Владимир Николаевич рассказал о программе школы, обозначил ее основные цели: актуализация исследовательской деятельности молодых ученых и подготовка научных публикаций по актуальным проблемам развития теории и практики юридической науки в контексте исследования проблем развития киберправа и обеспечения кибербезопасности.

Занятия в Зимней школе — 2023 начались с лекции заведующего кафедрой информационного права и цифровых технологий Университета имени О.Е. Кутафина (МГЮА), научного консультанта программы школы, доктора юридических наук, эксперта РАН Алексея Минбалеева на тему «Основные направления развития киберправа».

31 января 2023 г. состоялось торжественное открытие IX Зимней школы молодых ученых, на котором с приветствиями и напутственными словами к участникам обратились Инна Ершова, первый проректор Университета имени О.Е. Кутафина (МГЮА), заслуженный юрист России, доктор юридических наук, профессор; Владимир Синюков, проректор по научно-исследовательской деятельности, доктор юридических наук, профессор; Наталья Софийчук, проректор по образовательной деятельности, кандидат юридических наук, доцент; Наталья Соколова, научный руководитель НИИ, доктор юридических наук, доцент.



тельской деятельности, доктор юридических наук, профессор; Наталья Софийчук, проректор по образовательной деятельности, кандидат юридических наук, доцент; Наталья Соколова, научный руководитель НИИ, доктор юридических наук, доцент.

<sup>1</sup> URL: <https://msal.ru/news/>

В рамках Зимней школы прошла лекция-дискуссия Людмилы Терентьевой, доктора юридических наук, профессора кафедры международного частного права Университета имени О.Е. Кутафина (МГЮА), на тему «Правовое регулирование отношений в киберпространстве: вопросы управления и юрисдикции».

В закрытии Зимней школы молодых ученых принял участие ректор Университета имени О.Е. Кутафина (МГЮА), сопредседатель Ассоциации юристов России, заслуженный юрист России, профессор Виктор Блажеев, который сказал о важности проекта школы для Университета, поблагодарил участников, пожелал им успехов и пригласил к сотрудничеству по приоритетным научным направлениям.

Проректор по научно-исследовательской деятельности Владимир Синюков подвел итоги работы IX Зимней школы молодых ученых «Киберправо и кибербезопасность». Задачи школы были выполнены в полном объеме, тема раскрыта, залогом успеха стало как высочайшая квалификация преподавателей школы, так и активность, вовлеченность в дискуссии и заинтересованность участников, многие из которых занимаются проблемами в области киберправа и кибербезопасности в рамках диссертационных исследований. По итогам работы участникам школы были вручены сертификаты и удостоверения о повышении квалификации.



### Проектная сессия в рамках программы стратегического академического лидерства «Приоритет-2030»

3 и 4 февраля 2023 г. на площадке загородного досугового комплекса «Малюшина дача» состоялась проектная сессия в рамках программы стратегического академического лидерства «Приоритет-2030», в ходе которой были сформулированы и обсуждены предложения к стратегическому проекту «Инновационная юриспруденция», реализуемому Университетом имени О.Е. Кутафина (МГЮА).

В первый день работы проектная сессия носила прогностический характер: участники обсудили переход Университета к целевой модели развития, влияние мировых трендов на развитие юридической науки, образования и профессии. Обсуждение проходило в тематических группах, каждая из которых фокусировалась на развитии конкретной политики или кластерного проекта.

Во второй день проектная сессия была посвящена стратегическому планированию: спикеры тематических групп докладывали о разрабатываемых в рамках центров компетенций инновационных юридических продуктах, которые впоследствии будут транслированы в научное, профессиональное и образовательное





сообщество. Кроме того, участники обсудили проект локального нормативного акта, регулирующего основы инновационной проектной деятельности в рамках программы, стадии реализации проектов, распределение компетенции между участниками проектной деятельности.

В ходе коллективного обсуждения были представлены идеи по коммерциализации университетской науки, внедрению инноваций в образовательный процесс, совершенствованию молодежной, инфраструктурной и кампусной политики, определены перспективы участия членов консорциума «Инновационная юриспруденция» в реализации стратегического проекта.

В работе проектной сессии приняли участие ректор Университета имени О.Е. Кутафина (МГЮА), сопредседатель Ассоциации юристов России, заслуженный юрист Российской Федерации Виктор Блажеев, первый проректор Инна Ершова, проректор по стратегическому и международному развитию Мария Мажорина, проректор по научно-исследовательской деятельности Владимир Синоков, проректор по образовательной деятельности Наталья Софийчук, проректор по административной работе и информационным технологиям Сергей Игитханян, представители Центра управления изменениями Университета имени О.Е. Кутафина (МГЮА), центров компетенций и научно-педагогического сообщества.

## **XI Международный юридический форум «Правовая защита интеллектуальной собственности: проблемы теории и практики»**

В Университете имени О.Е. Кутафина (МГЮА) 17-18 февраля 2023 г. состоялся XI Международный юридический форум «Правовая защита интеллектуальной собственности: проблемы теории и практики» (IP Форум).

Форум был организован кафедрой интеллектуальных прав при поддержке Министерства высшего образования и науки РФ, Суда по интеллектуальным правам, Научно-образовательного центра права и биоэтики в сфере геномных исследований и применения генетических технологий.

К участию в XI IP Форуме были приглашены ученые российских и зарубежных юридических вузов и факультетов, сотрудники научных организаций,



представители государственных органов, практикующие юристы, а также другие специалисты в сфере права интеллектуальной собственности, эксперты в области экологии, средства массовой информации, освещающие вопросы IT-технологий, студенты и аспиранты.

В приветственном слове первый проректор Университета имени О.Е. Кутафина (МГЮА) Инна Ершова подчеркнула уникальность IP Форума и актуальность выбранной в этом году темы — «Генетические исследования и интеллектуальные права», отметив разнообразии составленной программы и неизменно высокий уровень организации мероприятия.

Гостей поприветствовали также председатель оргкомитета IP Форума, доцент, кандидат юридических наук Елена Гринь, руководитель Роспатента Юрий Зубов и депутат Государственной Думы Наталья Костенко.

Председатель Суда по интеллектуальным правам Людмила Новоселова отметила особый вклад, который вносит IP Форум в развитие отечественного права интеллектуальной собственности: *«По результатам предыдущих форумов были разработаны законодательные инициативы в области интеллектуальных прав и в области патентования. Поэтому IP Форум — это не просто наука, но и правоприменение и законодательство, то есть все направления, которые необходимы юристу».*

Открыл пленарное заседание проректор по научно-исследовательской деятельности Университета, доктор юридических наук, профессор, заслуженный деятель науки РФ Владимир Синюков.



*«Форум стал интеллектуальным центром по апробации юридических инструментов, продуктов в серии стимулирования инноваций, в которых так нуждается наша промышленность, социальная сфера. Практика показывает, что в России творческих людей очень много, но правовая составляющая создания творческих продуктов не всегда эффективна», — отметил Владимир Синюков.*

В рамках IP Форума состоялись также круглый стол «Интеллектуальные права в цифровой среде», дискуссионная площадка «Будущее IP-юристов в постцифровую эпоху. Есть ли жизнь после цифры?», круглый стол «Медиация в IP-спорах: практика и перспективы», дискуссионная площадка «Интеллектуальные права в электронной коммерции», а также круглый стол «Курс на успех: экспертные блоги юристов в социальных сетях».

### **Первый Международный юридический форум «Современные проблемы развития права и цифровой экономики в России и за рубежом»**



15 февраля 2023 г. в Университете имени О.Е. Кутафина (МГЮА) состоялся Первый Международный юридический форум «Современные проблемы развития права и цифровой экономики в России и за рубежом». Форум посвящен актуальным вопросам развития права в период коренных социально-экономических преобразований, обусловленных процессами цифровизации.

Пленарное заседание открыла первый проректор Университета имени О.Е. Кутафина (МГЮА) Инна Ершова. *«Форум призван внести свой вклад в осмысление очень многого из того, что происходит сегодня в цифровой экономике», — отметила она.*

Основной целью форума является создание площадки для общения и обмена опытом, обсуждения современных кейсов по цифровизации государственного управления и бизнес-процессов в сферах права и экономики.

Заместитель председателя Комитета по экономической политике Государственной Думы Федерального Собрания РФ, председатель Российского союза налогоплательщиков Артем Кириянов подчеркнул, что требования, которые сейчас россияне предъявляют к государственным цифровым услугам, достаточно высокие.

Председатель Ассоциации российских дипломатов МИД России Игорь Халевинский в своей приветственной речи отметил роль журнала «Право и цифровая экономика» в становлении и развитии цифровизации, а также в работе исследовательских центров ведущих организаций высшего образования страны.

В рамках форума гости обсудили юридические вопросы становления цифровой экономики: правовое обеспечение внедрения цифровых технологий в

различных отраслях; цифровые технологии в государственном управлении и юридической профессии; интеллектуальную собственность на цифровые технологии, цифровую личность; цифровые права и юридические технологии; правовое регулирование рисков и угроз цифровизации — технологических (информационная безопасность) и социальных (безработица, кибербуллинг и т.д.).

## **XVI Международная научно-практическая конференция «Наука административного права в системе публично-правовых наук»**

16 февраля 2023 г. в Университете состоялась XVI Международная научно-практическая конференция, посвященная памяти Юрия Марковича Козлова (1925-2002), которому в этом году исполнилось бы 98 лет, на тему: «Наука административного права в системе публично-правовых наук». Мероприятие проводится ежегодно Национальной ассоциацией административистов и кафедрой административного права и процесса Университета имени О.Е. Кутафина (МГЮА) при содействии руководства Университета.

Открыл конференцию Лев Леонидович Попов, президент Национальной ассоциации административистов, профессор кафедры административного права и процесса Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, заслуженный деятель науки РФ, заслуженный юрист РСФСР. Обратившись с приветственным словом к участникам, он поделился воспоминаниями о трудном научном пути Юрия Марковича Козлова и рассказал о его месте в науке административного права.

## **В МГЮА обсудили конституционные основы защиты национальной безопасности и интересов России**

2 февраля 2023 г. в Университете имени О.Е. Кутафина (МГЮА) прошел круглый стол «Конституционные основы защиты национальной безопасности и интересов России», посвященный 80-летней годовщине разгрома советскими войсками немецко-фашистских захватчиков в Сталинградской битве. В центре внимания участников были вопросы конституционно-правового обеспечения национальной безопасности, сохранения исторической правды, гражданско-патриотического воспитания молодого поколения.

Мероприятие, организованное кафедрой конституционного и муниципального права, прошло при поддержке Комитета Государственной Думы по науке и высшему образованию. Партнерами выступили АНО «Поколение уверенного будущего» и Общероссийская общественная организация «Ассоциация историков права».

Инна Владимировна Ершова вручила партнерам мероприятия благодарственные письма и памятные книги об истории Университета имени О.Е. Кутафина





(МГЮА). Активное участие в подготовке и проведении мероприятия приняли студенты Студенческого научного общества Университета.

С приветственным словом к участникам круглого стола обратилась первый проректор Университета имени О.Е. Кутафина (МГЮА), заслуженный юрист РФ, почетный работник высшего профессионального образования РФ, доктор юридических наук, профессор Инна Владимировна Ершова. Передав приветственное слово ректора Университета имени О.Е. Кутафина (МГЮА) Виктора Владимировича Блажеева, Инна Владимировна отметила значимость проводимого мероприятия с учетом исторической важности Сталинградской битвы, напомнив участникам о символе этой победы — Мамаевом кургане, открытие которого состоялось 55 лет назад. Она подчеркнула: *«Если сама Сталинградская битва явилась переломом в Великой Отечественной войне, то Мамаев курган — это конечная точка нашей победы в ней, которая ее знаменует»*.

В своем приветственном обращении к участникам мероприятия председатель Комитета Государственной Думы по науке и высшему образованию, профессор кафедры конституционного и муниципального права Университета имени О.Е. Кутафина (МГЮА) Сергей Владимирович Кабышев поделился воспоминаниями о своей работе в Волгограде, о том, как принимал присягу на верность Родине на Мамаевом кургане, и отметил важность сохранения исторической памяти. *«Наша задача, — сказал он, — мобилизовать наши силы, чтобы обеспечить неповторение такой трагедии, как Великая Отечественная война. Необходимо объединиться и доказать свою правоту и историческую правду»*. Также Сергей Владимирович напомнил о важности внесенных поправок в Конституцию России в части защиты исторической правды.

Мероприятие прошло в смешанном формате, объединило более 150 человек — ученых (юристов и историков), представителей органов власти и общественных организаций, молодых исследователей и студентов вузов.

## Круглый стол «Новые традиции юридической науки»



8 февраля 2023 г. в Университете имени О.Е. Кутафина (МГЮА) прошел круглый стол, посвященный Дню российской науки.

Мероприятие открыл проректор по научно-исследовательской деятельности Университета, доктор юридических наук, профессор, заслуженный деятель науки РФ Владимир Синюков.

В ходе круглого стола обсуждались актуальные вопросы, имеющие стратегическое значение для развития юридической науки, а также были отмечены научные достижения преподавательского состава Университета. Ректор Виктор Блажеев поздравил деятелей науки МГЮА и подчеркнул социальную значимость исследований в эпоху технологических изменений. Только за 2022 г. были реализованы 64 инициативы в рамках государственных проектов, а научный состав МГЮА сыграл существенную роль в становлении российской науки.

За вклад в развитие юридической науки были награждены благодарностями работники Университета: заведующий кафедрой истории государства и права, доктор юридических наук, профессор Игорь Исаев, профессор кафедры уголовного права, доктор юридических наук Алексей Рарог, профессор кафедры трудового права и права социального обеспечения, доктор юридических наук Эльвира Тучкова, профессор кафедры гражданского права, доктор юридических наук Людмила Василевская, заведующий кафедрой административного права и процесса, доктор юридических наук, профессор Сергей Зубарев, заведующий кафедрой философии и социологии, доктор юридических наук, доктор философских наук, профессор Олег Рыбаков, профессор кафедры конституционного и муниципального права, доктор юридических наук Галина Садовникова,





проректор по международному и стратегическому развитию, кандидат юридических наук Мария Мажорина, профессор кафедры международного права, доктор юридических наук, доцент Владислав Толстых, профессор кафедры финансового права, доктор юридических наук, доцент Лана Арзуманова, профессор кафедры предпринимательского и корпоративного права, доктор юридических наук Ольга Тарасенко, профессор кафедры философии и социологии, доктор философских наук, доцент Александр Огородников, доцент кафедры криминалистики, кандидат юридических наук Ярослава Комиссарова, доцент кафедры уголовно-процессуального права, доктор юридических наук Сергей Насонов, помощник проректора по научно-исследовательской деятельности, доктор юридических наук, профессор Мария Егорова, доцент кафедры гражданского права, кандидат юридических наук Ирина Аюшеева, доцент кафедры интеграционного и европейского права, кандидат юридических наук Мария Некотенева, доцент кафедры правового моделирования, доцент кафедры международного частного права, кандидат юридических наук Олеся Засемкова, директор Центра управления изменениями, кандидат юридических наук Владимир Никишин, директор Содружества выпускников МГЮА, кандидат юридических наук Вахтанг Федоров и специалист по маркетингу отдела научных мероприятий и молодежной научной деятельности Научно-исследовательского института Маргарита Милева.

### **I Всероссийский научный симпозиум «Рясенцевские чтения»**

16-17 февраля 2023 г. в Университете прошел I Всероссийский научный симпозиум «Рясенцевские чтения». Мероприятие было организовано кафедрой гражданского права в память о выдающемся ученом, педагоге, основателе цивилистической школы ВЮЗИ.



В рамках научного симпозиума состоялись пленарное заседание и круглые столы по актуальным проблемам гражданского права, а также была организована культурная программа: экскурсия по Большому академическому театру, экскурсия по Российской академии художеств и концерт.

С приветственными словами к участникам научного симпозиума обратилась первый проректор Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, заслуженный юрист РФ Инна Ершова. Инна Владимировна поделилась своими воспоминаниями о Владимире Александровиче как об ученом, педагоге и человеке.

На мероприятии был показан документальный фильм о В. А. Рясенцеве, специально снятый к открытию научного симпозиума.

## Развитие университета

### Договор о практической подготовке обучающихся между МГЮА и Департаментом военного имущества Министерства обороны России

Состоялась процедура подписания договора Университета имени О.Е. Кутафина (МГЮА) с Департаментом военного имущества Министерства обороны Российской Федерации. В мероприятии приняли участие ректор МГЮА Виктор Блажеев, директор Департамента военного имущества Министерства обороны РФ Михаил Сапунов, проректор по административной работе и информационным технологиям Сергей Игитханян, проректор по молодежной политике Александр Чанышев, директор Центра карьеры и развития компетенций МГЮА Рубен Овсепян.

Ректор Виктор Блажеев подчеркнул, что Университет плотно работает с Министерством обороны РФ:



*«Я очень благодарен вам за вклад в патриотическое воспитание наших студентов, которому вы активно содействуете. Надеюсь на дальнейшее плодотворное сотрудничество».*

### Церемония подписания соглашения с ООО «Российские студенческие отряды»



Накануне Дня российских студенческих отрядов в Университете имени О.Е. Кутафина (МГЮА) прошла торжественная церемония подписания соглашения с молодежной общероссийской общественной организацией «Российские студенческие отряды».



К гостям обратилась первый проректор Университета имени О.Е. Кутафина (МГЮА) Инна Ершова: *«Для меня студенческие отряды — это моя молодость. Днем работаем, а вечером поем песни под гитару у костра. Это душа и навыки. Я уверена, что и вы в студенческих отрядах научились многому. Желаю вам успехов, а Университет продолжит поддерживать ваши инициативы».*

Участников встречи также поприветствовал проректор по молодежной политике Университета имени О.Е. Кутафина (МГЮА) Александр Чанышев.

В Университете имени О.Е. Кутафина (МГЮА) работает один студенческий педагогический отряд

«Оригами». Бойцы этого отряда получили благодарности ректора Университета имени О.Е. Кутафина (МГЮА) за весомый вклад в развитие студенческого педагогического отряда и активное участие в его деятельности.

## Студенты МГЮА прошли подготовку в проекте «Зима в спецназе»

29 января — 12 февраля 2023 г. студенты Военного учебного центра Университета имени О.Е. Кутафина (МГЮА) приняли участие в проекте Российского технологического университета (РТУ) МИРЭА и Министерства обороны России «Зима в спецназе».

Обучающиеся Центра достойно прошли испытания и овладели практическими навыками в области тактической подготовки, огневой подготовки, химической и биологической защиты.

11 февраля 2023 г. ректор МГЮА Виктор Блажеев посетил военные сборы, он высоко оценил успехи студентов в боевой подготовке. Были награждены учащиеся МГЮА Рем Цеков, Константин Ребров, Александр Романко, Никита Самойлов, Федор Смирнов, Казбек Ханикаев, Зелимхан Хутиев, Богдан Янин, Магомедали Мустафаев, Ислам Джалалов, отличившиеся за время участия в проекте.



## В МГЮА обсудили сотрудничество с АО «Новая мода» в рамках консорциума «Инновационная юриспруденция»

8 февраля 2023 г. состоялась встреча представителей Университета имени О.Е. Кутафина (МГЮА) с руководством юридической и GR служб АО «Новая мода».

В мероприятии приняли участие проректор по стратегическому и международному развитию, руководитель Центра компетенций «Право устойчивого развития. ESG-стандарты» Мария Мажорина, директор Центра управления изменениями Владимир Никишин, руководитель проекта «Консорциум «Инновационная юриспруденция»» Центра управления изменениями Ольга Бендицкая, заведующий кафедрой информационного права и цифровых технологий, руководитель Центра компетенций «Киберправо» Алексей Минбалева, и.о. директора Института бизнес-права Андрей Петраков, директор Научно-исследовательского института Олег Кудряшов, доктор юридических наук, профессор кафедры международного частного права Бениамин Шахназаров.



## Встреча представителей МГЮА с руководством ФГКУ «Росгеолэкспертиза»

13 февраля 2023 г. состоялась встреча представителей Университета имени О.Е. Кутафина (МГЮА) с руководством ФГКУ «Росгеолэкспертиза».

В мероприятии приняли участие проректор по стратегическому и международному развитию, руководитель Центра компетенций «Право устойчивого развития. ESG-стандарты» Мария Мажорина, руководитель Центра компетенций «Экоправо» Вячеслав Агафонов, руководитель Центра компетенций «Геоправо» Эльвин Теймуров, руководитель проекта «Консорциум «Инновационная юриспруденция»» Центра управления изменениями Ольга Бендицкая.

ФГКУ «Росгеолэкспертиза» на встрече представляли директор Гудков Сергей, начальник управления нормативно-методического обеспечения недропользования Нармин Миркеримова и ведущий юрисконсульт отдела проверок закупочной деятельности управления контрактной службы Даниил Игнатьев.

Участники обсудили способы взаимовыгодного сотрудничества в рамках Консорциума «Инновационная юриспруденция», в частности, были затронуты возможные формы взаимодействия в рамках центров компетенций «Геоправо» и «Экоправо», а также в рамках Высшей школы права.

## Мероприятия ректората

### Заседание Ученого совета



27 февраля 2023 г. прошло заседание Ученого совета, в рамках которого были приняты решения по актуальным вопросам кадровой политики, а также заслушаны отчеты по научно-исследовательской деятельности внутренних подразделений.

После приветственного слова ректора Виктора Блажеева и традиционной церемонии награждения директор Научно-исследовательского института Олег Кудряшов представил отчет о научно-исследовательской деятельности Института в 2022 г. В презентации были отражены структура исследовательских проектов за предыдущий год и их основные направления. Также были отмечены изменения в структуре финансирования Института в связи с завершением работы над

одним из проектов Российского центра научной информации, проведен общий анализ бюджета за предыдущий год. Кроме того, выступавшим была затронута тема финансовых и научно-исследовательских перспектив текущих заказов.

Научный руководитель Научно-исследовательского института, заведующий кафедрой международного права, доктор юридических наук Наталья Соколова выступила со второй частью отчета о научно-исследовательской деятельности

Института в 2022 г. В своей презентации она затронула структуру организации научно-исследовательской деятельности, а также актуальные проблемы, существующие в научной деятельности Института.

С докладом о ходе реализации программы стратегического академического лидерства «Приоритет-2030» выступила проректор по стратегическому и международному развитию МГЮА, доцент кафедры международного частного права, кандидат юридических наук Мария Мажорина.

Аспирант кафедры адвокатуры Алексей Деньгин представил отчет об успешном прохождении учебной программы и подготовке к защите диссертационной работы.

Докторант кафедры криминологии и уголовно-исполнительного права Себила Саламова и докторант кафедры конституционного и муниципального права Андрей Будаев также отчитались о проделанной работе и рассказали о дальнейших планах.



## Премии, награждения

### Награждение молодых ученых в Государственной Думе Федерального Собрания РФ

По случаю Дня российской науки в Государственной Думе Федерального Собрания РФ, отмечаемого 8 февраля, состоялась торжественная церемония награждения молодых ученых.

Благодарности «За вклад в развитие современной российской науки и активную научно-исследовательскую деятельность» удостоен директор Высшей школы права, доцент кафедры международного права Университета имени О.Е. Кутафина (МГЮА) Эльвин Сахаватович Теймуров.

### Премии Правительства Москвы

Состоялась также торжественная церемония награждения молодых ученых Москвы, чьи разработки отмечены на уровне Правительства. Лауреатами премии стали 90 молодых людей, среди которых руководитель Центра управления изменениями Университета имени



О.Е. Кутафина (МГЮА), доцент кафедры криминалистики, кандидат юридических наук Владимир Никишин.

### Стипендии имени А. А. Собчака



В Университете на торжественной церемонии назвали имена обладателей стипендии имени А. А. Собчака. В список лауреатов вошли обучающиеся МГЮА — студентки 4-го курса МПИ Елена Борулева и Софья Петрова.

Обладателей стипендии поздравила член Совета Федерации Людмила Нарусова. В ходе мероприятия собравшиеся посмотрели фильм о жизни Анатолия Собчака.

## Развитие законодательства в период цифровой трансформации общества

### Актуальные проблемы систематизации законодательства России под влиянием цифровых технологий в период цифровой трансформации<sup>1</sup>

**Аннотация.** В статье рассматриваются актуальные вопросы систематизации законодательства РФ, обозначены проблемы и концептуальные пути их решения. Обращено внимание на необходимость систематизации российского информационного законодательства, упорядочение действующих законов, нормативных правовых актов и приведение всех юридических норм в единую правовую систему. Особое внимание уделено вопросам, связанным с осмыслением концептуального подхода к разработке Информационного кодекса, использованием юридических конструкций, терминов, исследованием различных взглядов на правовое регулирование информационных отношений, состояние правового регулирования, его противоречия и пробелы.

В работе использовались методы анализа и синтеза. Проведенное исследование позволило сделать вывод о том, что в условиях цифровой трансформации необходимо проработать и укрепить научно-правовые методы в различных направлениях информационного общества, законодательно закрепить понятия, связанные с оборотом информации, разработать требования к государственным информационным системам. Обосновано, что новые научно-теоретические подходы будут соответствовать фундаментальной системе различных правовых конструкций, а также позволят систематизировать правовые отношения в информационной сфере.

**Ключевые слова:** информационное общество, система правовой информации, цифровая трансформация, прорывные технологии, цифровая платформа, информационно-телекоммуникационные технологии, искусственный интеллект, Информационный кодекс, угрозы, правовое регулирование.

DOI: 10.17803/2311-5998.2023.102.2.025-033

<sup>1</sup> Статья выполнена по государственному заданию № FMUZ-2021-0042 «Правовое регулирование цифровой экономики, искусственного интеллекта, информационной безопасности».



**Татьяна Анатольевна ПОЛЯКОВА,**

главный научный сотрудник, и.о. заведующего сектором информационного права и международной информационной безопасности Института государства и права

Российской академии наук, доктор юридических наук, профессор, заслуженный юрист РФ  
[polyakov\\_ta@mail.ru](mailto:polyakov_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-fadeeva@yandex.ru](mailto:n-fadeeva@yandex.ru)  
119019, Россия, г. Москва, ул. Знаменка, д. 10

© Полякова Т. А.,  
Троян Н. А., 2023

**TATYANA A. POLYAKOVA,**

Chief researcher,  
acting head of the Sector  
of information law and international information security  
of the Institute of State and Law  
of the Russian Academy of Sciences  
Dr. Sci. (Law), Professor,  
honored lawyer of Russian Federation  
**polyakov\_ta@mail.ru**  
10, ul. Znamenka, Moscow, Russia, 119019

**NATALIA A. TROYAN,**

Senior researcher of the Sector  
of information law and international information security  
of the Institute of State and Law  
of the Russian Academy of Sciences,  
Cand. Sci. (Law)  
**n-fadeeva@yandex.ru**  
10, ul. Znamenka, Moscow, Russia, 119019

### **Current Problems of Russian Legislation Systematization under the Influence of Digital Technologies in the Conditions of Digital Transformation**

**Abstract.** *The article deals with topical issues on the systematization of the legislation of the Russian Federation. The study outlines the problems and conceptual ways to solve them. Attention is drawn to the need to systematize the Russian information legislation, streamline existing laws, regulatory legal acts and bring all legal norms into a single legal system. Particular attention is paid to issues related to understanding the conceptual approach to the development of the Information Code, the use of legal structures, terms, the study of different views on the legal regulation of information relations, the state of legal regulation, the disclosure of contradictions and gaps. In the study, methods of analysis and synthesis were used. The study made it possible to draw a number of conclusions: that in the context of digital transformation it is necessary to develop and strengthen scientific and legal methods in various areas of the information society. It is necessary to legislate the concepts related to the circulation of information, as well as develop requirements for state information systems. It is substantiated that in real time, new scientific and theoretical approaches will contribute to the fundamental system of various legal structures, as well as systematize legal relations in the information sphere.*

**Keywords:** *information society, legal information system, digital transformation, breakthrough technologies, digital platform, information and telecommunication technologies, artificial intelligence, Information Code, threats, legal regulation.*

**В** условиях цифровизации развитие общества связано с новыми технологиями, являющимися определяющим фактором цифровой экономики и цифровой экосистемы, что позволяет выделить новый вектор развития права, новые правоотношения, формирующиеся под влиянием цифровых технологий<sup>2</sup>. Современные технологии оказывают эффективное влияние на развитие системы законодательства в России. Поэтому вопросы, связанные с систематизацией законодательства и цифровых технологий, обозначены в задачах, которые ставятся в рамках развития системы цифровой экономики<sup>3</sup>.

Так, в соответствии с Указом Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»<sup>4</sup>, определены национальные цели развития России на указанный период, ключевые направления, с учетом которых должны быть разработаны национальные проекты (программы). Одной из ключевых задач «является создание системы правового регулирования цифровой экономики, основанной на гибком подходе в каждой сфере»<sup>5</sup>.

Реализации этой задачи посвящен федеральный проект «Нормативное регулирование цифровой среды», который предусматривает разработку и принятие ряда нормативных правовых актов, направленных на снятие первоочередных барьеров, которые препятствуют развитию цифровой экономики. Планируется также урегулировать для различных отраслей законодательства вопросы, связанные с идентификацией субъектов правоотношений в цифровой среде, электронным документооборотом, оборотом данных, в том числе персональных данных<sup>6</sup>.

Сегодня достаточно активно решаются задачи систематизации современного законодательства России, регулирующего цифровые отношения. Безусловно, создание ряда автоматизированных информационно-правовых систем в государственном и частном секторе значительно упростило процесс поиска и применения нормативного материала.

Цифровые технологии имеют сегодня ключевое значение для деятельности органов государственной власти, организаций и учреждений в системе межведомственного взаимодействия и документооборота и являются гарантом качественного уровня жизни граждан, а также реализации их конституционных прав и свобод.

Как следствие, в нынешних реалиях появилась острая необходимость систематизации российского законодательства, упорядочения действующих законов, иных нормативных правовых актов и приведения всех юридических норм в

<sup>2</sup> Карцхия А. А. Гражданский оборот и цифровые технологии : монография. М. : Филинь, 2019.

<sup>3</sup> Минбалеев А. В. Проблемы цифрового права : учебное пособие. Саратов : Амирит, 2022. С. 45.

<sup>4</sup> Указ Президента РФ от 7 мая 2018 г. «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // СПС «КонсультантПлюс».

<sup>5</sup> Нормативное регулирование цифровой среды / Министерство экономического развития РФ // URL: [https://www.economy.gov.ru/material/directions/gosudarstvennoe\\_upravlenie/normativnoe\\_regulirovanie\\_cifrovoy\\_sredy/](https://www.economy.gov.ru/material/directions/gosudarstvennoe_upravlenie/normativnoe_regulirovanie_cifrovoy_sredy/) (дата обращения: 21.01.2023).

<sup>6</sup> Нормативное регулирование цифровой среды.



единую систему<sup>7</sup>, чтобы обеспечить формирование единой системы правовых актов и доступ к достоверной, актуальной правовой информации, ликвидацию устаревших и неэффективных норм права, юридических коллизий и пробелов в законодательстве.

В правовом государстве правовая система представляет собой достаточно сложную конструкцию из-за множественности органов, принимающих правовые акты, а также достаточно большого массива правовых актов, созданных правотворческими органами. В режиме реального времени в период цифровизации очень важна согласованность правотворческой деятельности. Безусловно, решение поставленных задач имеет как теоретическое, так и практическое значение не только для нормотворческой деятельности, но и для правоприменительной практики, так как под воздействием цифровых технологий система нормативных актов подвергается быстрым изменениям.

Надо признать, что сегодня накопился достаточно большой массив правовых актов, которые регулируют отношения в информационной сфере, при этом ключевое значение имеют достоверность, полнота, своевременность предоставления, актуальность, а следовательно, и систематизация информационных ресурсов. В развитии законодательства немаловажную роль играют институты систематизации и мониторинга, которые призваны упорядочить и совершенствовать законодательный массив.

Необходимо также констатировать, что накопилось достаточно много проблем, связанных с процессами систематизации, возникли различные точки зрения на понимание информационно-правового обеспечения правового мониторинга, на определение правового мониторинга, его видов, на критерии полноты и достоверности правовых данных, единые процессы их обработки и предоставления, на модернизацию информационных систем под воздействием цифровых технологий. Ключевой задачей правового мониторинга является реализация одного из приоритетных направлений государственной политики — повышения качества и эффективности законодательства как важного фактора развития государства. Все эти процессы требуют теоретических и организационно-правовых разработок для решения проблем в области правового мониторинга.

Прежде всего необходимо уделить особое внимание исторически сложившемуся практическому опыту работы в области систематизации законодательства Министерства юстиции России, которое более 220 лет уполномочено реализовывать государственную правовую политику государства. Изначально на Министерство было возложено решение ответственных задач по разработке и совершенствованию законодательства<sup>8</sup>.

Министерство юстиции РФ одним из первых применило новейшие технологии в области правового информирования. Среди приоритетных направлений его деятельности экспертиза нормативных правовых актов на наличие коррупциогенных

<sup>7</sup> Алексеев С. С. Государство и право : начальный курс. 2-е изд., перераб. и доп. М. : Юрид. лит., 1994. С. 125.

<sup>8</sup> Выступление Владимира Путина на торжественном заседании, посвященном 220-летию со дня образования Министерства юстиции России // Мониторинг правоприменения. 2022. № 3 (44) С. 83—87

факторов, мониторинг правоприменения, инкорпорация правовых актов СССР и РСФСР в законодательство Российской Федерации.

К полномочиям Министерства юстиции РФ также относится обеспечение единства правового пространства Российской Федерации, что включает разработку общей стратегии государственной политики в установленной сфере деятельности и систематизацию законодательства<sup>9</sup>, обеспечение верховенства Конституции РФ и федеральных законов и реализацию конституционных прав граждан на получение достоверной информации.

Минюстом России создан федеральный банк нормативных правовых актов субъектов Российской Федерации и ведется регистр нормативных правовых актов субъектов Российской Федерации. К федеральному регистру обеспечен свободный доступ в электронном виде по каналам сети Интернет (<http://pravominjust.ru>, <http://право-минюст.рф>)<sup>10</sup>. Минюст России проводит системный мониторинг законодательства субъектов РФ, организован доступ к муниципальному регистру в сети Интернет.

Нельзя недооценивать роль первых баз данных правовой информации, созданных в Минюсте России, исторически сложившийся опыт работы в России органов юстиции в области систематизации законодательства, правового мониторинга и государственного учета нормативных правовых актов федеральных органов исполнительной власти.

О. А. Иванюк справедливо считает, что «систематизацию законодательства в современных условиях невозможно представить без использования различных автоматизированных технологий и справочно-информационных систем законодательства»<sup>11</sup>. В России в настоящее время действуют 20 кодексов, которые создавались по различным конструкциям. М. Н. Марченко считает, что «кодексы рассматриваются юристами лишь как отправная точка, а не завершение пути. Этим они четко отличаются от компиляций (консолидации, кодексов американского права), которые встречаются в странах общего права, а также от «отредактированных» обычаев или кодексов периода до Французской революции»<sup>12</sup>.

Существуют разные точки зрения относительно систематизации законодательства. Так, например, А. Ф. Шебанов высказал глубокую мысль о наличии определенных закономерностей в процессе систематизации законодательства, утверждая, в частности, что «этот процесс должен последовательно пройти те или иные этапы»<sup>13</sup>.

А. В. Минбалеев отмечает, что «сегодня государством ставится задача не просто развития законодательства, а осуществление процессов на основе системного подхода, что, в свою очередь, предполагает осуществление процессов

<sup>9</sup> Указ Президента РФ от 10 августа 2000 г. № 1486 «О дополнительных мерах по обеспечению единства правового пространства Российской Федерации» // СЗ РФ. 2000. № 33. Ст. 3356.

<sup>10</sup> URL: <https://minjust.gov.ru/ru/activity/directions/978/> (дата обращения: 12.10.2022).

<sup>11</sup> Минбалеев А. В. Указ. соч. С. 47.

<sup>12</sup> Марченко М. Н. Источники права. М. : Проспект ; Велби, 2005. С. 475.

<sup>13</sup> Шебанов А. Ф. Подготовка Свода законов Советского государства // Сов. государство и право. 1977. № 5. С. 58.

систематизации законодательства в сфере цифровой экономики. Важно выделить несколько направлений: вопросы систематизации современного законодательства Российской Федерации, регулирующего цифровые отношения, затем вопросы кодификации и разработки Цифрового кодекса Российской Федерации, а также направление, использование технологий, в том числе искусственного интеллекта, в процессах систематизации законодательства»<sup>14</sup>.

И. Л. Бачило считала, что «систематизация и возможная кодификация информационного законодательства требуют особого внимания, в части трех блоков вопросов: структуры законодательства отрасли информационного права, упорядочения терминологии, особенно правовых дефиниций, также ряда вопросов касательно процессуального обеспечения форм и видов отношений субъектов в процессе работы с ресурсами информации и технологий и взаимодействия с участниками конкретных отношений»<sup>15</sup>.

Создание единого Информационного кодекса РФ предлагали такие ученые, как Ю. А. Нисневич, В. А. Копылов, И. В. Бондарь, И. Л. Бачило, Е. С. Лисицина, П. У. Кузнецов<sup>16</sup>. Прогрессивным шагом в изучении поставленного вопроса является проект концепции Информационного кодекса РФ, подготовленный группой ученых Института государства и права РАН под руководством И. Л. Бачило.

В исследовании правовой базы регулирования информационных отношений рассматривались вопросы обеспечения преемственности, приведения к единому толкованию систем правовых дефиниций, которые востребованы законодателем, также была разработана архитектура базовых областей для информационного законодательства России<sup>17</sup>. Основной целью Информационного кодекса РФ разработчики считали прежде всего сбалансированность правовых источников по различным направлениям, выявление несогласованности понятий, норм во взаимосвязанных законах. Информационный кодекс позволит обеспечить необходимое правовое регулирование по направлениям развития информационных технологий<sup>18</sup>.

Для России исключительно важно решение научных вопросов по улучшению информационного законодательства в условиях цифровизации информационного общества и цифровой трансформации. Необходимы новые научно-теоретические подходы, которые позволят создать рациональную систему правовых механизмов, рационализировать не только информационные процессы, но и правовые отношения в рамках информационного пространства. Это обеспечит взаимодействие информационного законодательства с различными отраслями права.

<sup>14</sup> Минбалеев А. В. Указ. соч. С. 46.

<sup>15</sup> Бачило И. Л. О подходах к систематизации и кодификации информационного законодательства // Систематизация и кодификация информационного законодательства : сборник научных работ / отв. ред. И. Л. Бачило. М. : ИГП РАН ; Канон+, 2015. С. 43.

<sup>16</sup> Нисневич Ю. А. Информация и власть. М. : Мысль, 2000. С. 131, 161 ; Копылов В. А. О структуре и составе информационного законодательства // Государство и право. 1996. № 6. С. 101—110.

<sup>17</sup> Концепция Информационного кодекса Российской Федерации / под ред. И. Л. Бачило. М. : ИГП РАН ; Канон+ ; Реабилитация, 2014. С. 9.

<sup>18</sup> Концепция Информационного кодекса Российской Федерации. С. 25.

В целях более эффективного государственного управления и доступа к достоверной правовой информации граждан, бизнеса и органов государственной власти Президентом РФ В. В. Путиным подписано распоряжение от 1 июля 2022 г. № 202-рп<sup>19</sup> о создании межведомственной рабочей группы для подготовки проекта государственной программы по систематизации правовых актов органов публичной власти всех уровней.

Председатель Конституционного Суда РФ В. Д. Зорькин в выступлении на Петербургском международном юридическом форуме также высказал мнение о необходимости принятия в России Информационного кодекса. Он отметил, что «в условиях, когда существующее цифровое законодательство не в полной мере отвечает потребностям времени, систематизировать его возможно введением Информационного кодекса Российской Федерации»<sup>20</sup>. Также он считает, что «в контексте ныне действующей Конституции России необходима разработка конституционно-правовой концепции информационного права, основу которой должно составлять конституционное право граждан на информацию. Важно законодательно определить основные формы оборота информации, установив права и обязанности его участников, определить правовой режим информации в публично-правовой и частноправовой сферах, а также основания, формы и пределы применения информационных технологий в деятельности соответствующих субъектов права»<sup>21</sup>.

Сегодня действительно отсутствует единое использование терминологического аппарата, не согласуются научные конструкции правового регулирования как норм отдельных законов, так и законодательства. Так, понятия «информационная система», «документ» интерпретируются по-разному в различных законах. Очень важными остаются вопросы, связанные с понятием «информация», тем более, что сегодня информация значительно чаще является объектом научного познания, что, в свою очередь, ведет к различным классификациям по разным критериям.

Во всем мире идет полномасштабное внедрение современных технологий, в рамках новой промышленной революции, под влиянием современных систем управления трансформируются правовые системы. В этой связи Т. А. Полякова, А. В. Минбалева, Н. В. Кроткова считают, что «в режиме реального времени

<sup>19</sup> Распоряжение Президента РФ от 1 июля 2022 г. № 202-рп «О межведомственной рабочей группе по разработке проекта государственной программы по систематизации правовых актов органов публичной власти всех уровней» // URL: [www.http://publication.pravo.gov.ru/](http://publication.pravo.gov.ru/) (дата обращения: 12.10.2022).

Рабочую группу возглавил министр юстиции РФ Константин Чуйченко. В нее также вошли представители Минцифры России, Минфина России, региональных органов исполнительной власти и научных организаций. Данное направление в Минюсте России будет курировать Департамент систематизации законодательства (URL: <https://minjust.gov.ru/ru/ministry/departments/133/> (дата обращения: 12.10.2022)).

<sup>20</sup> Право в цифровом мире : Выступление Валерия Зорькина на Петербургском международном юридическом форуме // URL: <https://alf.ru/news/pravo-v-tsifrovom-mire-vystuplenie-valeriya-zorkina-na-ptuuf/> (дата обращения: 12.10.2022).

<sup>21</sup> Право в цифровом мире. Выступление Валерия Зорькина на Петербургском международном юридическом форуме.

необходима модернизация правовых подходов к урегулированию новых общественных отношений, связанных с инновационными, эволюционными и синергическими процессами, обусловленными внедрением цифровых технологий, а также рядом новых вызовов и угроз. Новый этап развития глобального информационного общества, связанный со становлением “цифровой цивилизации”, требует юридического осмысления общественных отношений, субъектов и объектов, проблем их взаимодействия в цифровой среде, аутентификации и идентификации, информационной инфраструктуры и т.д.»<sup>22</sup>.

Безусловно, кодификация информационного законодательства важна и требует не только общественного обсуждения. Возможна оценка интеграции с другими отраслями законодательства, так как информационные правовые нормы присутствуют практически во всех его отраслях (конституционном, уголовном, гражданском, административном законодательстве и др.). Поэтому неслучайно вопросы правовой системы в условиях цифровизации и формирования единого информационно-правового пространства — это ключевая задача органов государственной власти России, требующая формирования и развития национальной системы правовой информации, в которую должно быть включено информационное законодательство. Это позволит предоставлять оперативно достоверную правовую информацию о нормативных правовых актах не только органам власти, но и гражданам, и организациям.

Для создания Информационного кодекса РФ необходимо детально исследовать весь имеющийся нормативный массив, определить его положительные стороны и выявить недостатки и проблемы, которые возникают в сфере информационных отношений.

На современном этапе в процессе цифровой трансформации еще достаточно много нерешенных вопросов, например, связанных с категориями ограниченного доступа к информации (государственная, коммерческая тайна и др.), с информационной безопасностью.

Безусловно, для решения создавшихся проблем необходима разработка теоретической модели Информационного кодекса РФ, которая обеспечила бы возможность перейти от абстрактных теоретических дискуссий к решению назревших проблем. Появилась необходимость четко определить информационные термины и понятия, создать для них четкие стандарты качества, устранить разночтения в информационном праве. Все это будет способствовать совершенствованию информационного законодательства в стране.

<sup>22</sup> Полякова Т. А., Минбалеев А. В., Кроткова Н. В. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. 2020. № 5. С. 75—87.

## БИБЛИОГРАФИЯ

1. Алексеев С. С. Государство и право : начальный курс. — 2-е изд., перераб. и доп. — М. : Юрид. лит., 1994. — 189 с.
2. Бачило И. Л. О подходах к систематизации и кодификации информационного законодательства // Систематизация и кодификация информационного законодательства : сборник научных работ / отв. ред. И. Л. Бачило. — М. : ИГП РАН ; Канон+, 2015. — С. 7—12.
3. Выступление Владимира Путина на торжественном заседании, посвященном 220-летию со дня образования Министерства юстиции России // Мониторинг правоприменения. — 2022. — № 3 (44). — С. 83—87.
4. Карцхия А. А. Гражданский оборот и цифровые технологии : монография. — М. : Филинь, 2019. — 125 с.
5. Колесова Ю. И. Органы и учреждения юстиции РФ. — Серия : Учебники и учебные пособия. — Ростов н/Д : Феникс, 2002. — 603 с.
6. Концепция Информационного кодекса Российской Федерации / под ред. И. Л. Бачило. — М. : ИГП РАН ; Канон+ ; Реабилитация, 2014. — 192 с.
7. Копылов В. А. О структуре и составе информационного законодательства // Государство и право. — 1996. — № 6. — С. 101—110.
8. Марченко М. Н. Источники права. — М. : Проспект ; Велби, 2005. — 760 с.
9. Минбалеев А. В. Проблемы цифрового права : учебное пособие. — Саратов : Амирит, 2022. — 233 с.
10. Нисневич Ю. А. Информация и власть. — М. : Мысль, 2000.
11. Полякова Т. А., Минбалеев А. В., Кроткова Н. В. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. — 2020. — № 5. — С. 75—87.
12. Шебанов А. Ф. Подготовка Свода законов Советского государства // Сов. государство и право. — 1977. — № 5. — 67с.



**Руслан Абдусаламович  
АБДУСАЛАМОВ,**  
заведующий кафедрой  
информационного права и  
информатики  
Юридического института  
Дагестанского  
государственного  
университета  
кандидат педагогических  
наук, доцент  
**abd-rus@yandex.ru**  
367000, Россия,  
Республика Дагестан,  
г. Махачкала,  
ул. Коркмасова, д. 8

## Правовое регулирование использования информационных технологий в сфере высшего образования в Российской Федерации<sup>1</sup>

**Аннотация.** В статье обозначается правовая основа использования информационных технологий в сфере высшего образования. Рассматриваются цифровые технологии, которые активно используются в практике как российских, так и зарубежных вузов. При этом отмечается, что в зарубежных странах процесс цифровизации образовательных услуг шире, чем в России. В рамках отечественного правопорядка происходит только базовое развитие как правового регулирования в данной сфере, так и практической реализации исследуемого направления. Особый акцент делается на современных проблемах использования информационных технологий в сфере высшего образования, характерных для отечественной практики и правового регулирования. Автором выявлены проблемы правового и организационного характера. В качестве выводов формулируются направления по совершенствованию правового регулирования и практического внедрения информационных технологий в сфере высшего образования в России. Автор предлагает разрешить возможные проблемы организационного, технического и правового характера, при этом во внимание должен приниматься имеющийся опыт дистанционного обучения в государстве.

**Ключевые слова:** информационное пространство, информационные технологии, высшие учебные заведения, сеть Интернет, образовательные услуги.

DOI: 10.17803/2311-5998.2023.102.2.034-041

**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**

8, ul. Korkmasova, Makhachkala, Republic of Dagestan, Russia, 367000

### Legal Regulation of the Use of Information Technologies in Higher Education in the Russian Federation

**Abstract.** The article outlines the legal basis for the use of information technology in higher education. Digital technologies are considered, which are actively used both in the practice of Russian universities and foreign ones. At the same time, it is noted that in foreign countries the process of digitalization

*of educational services is quite broader than in Russia. Within the framework of the domestic legal order, only the basic development of both legal regulation in this area and the practical implementation of the researched direction takes place. Particular emphasis is placed on modern problems of using information technologies in the field of higher education, which are typical for domestic practice and legal regulation. The author identified problems of a legal and organizational nature. As conclusions, directions for improving legal regulation and practical implementation of information technologies in the field of higher education in Russia are formulated. The author proposes to resolve possible problems of an organizational, technical and legal nature, while taking into account the existing experience of distance learning in the state.*

**Keywords:** *information space, information technologies, higher education institutions, the Internet, educational services.*

## Актуальность проблемы

Цифровые технологии получили широкое применение в сфере высшего образования. В настоящее время взят политический курс на развитие информационных технологий, которые внедряются во все сферы общественных отношений. Главным образом это связано с происходящими процессами цифровизации, которые характерны не только для нашей страны, но и для развитых стран.

Особый интерес вызывает использование информационных технологий в рамках высшего образования. Это связано с тем, что информационные технологии в сфере высшего образования являются неотъемлемым элементом его эффективности. Использование цифровых технологий в образовательной среде показывает уровень эффективности принятых решений и всего образовательного процесса.

Доктринальный интерес к данному вопросу обусловлен имеющимися проблемами в правовом регулировании, а также наличием практических проблем в данной сфере. В связи с этим в рамках настоящего исследования будут рассмотрены особенности и проблемы внедрения и использования информационных технологий в сфере высшего образования через призму правового регулирования указанных процессов.

Вопросы, связанные с правовым регулированием использования информационных технологий в Российской Федерации, являлись предметом изучения многих исследователей. Здесь можно назвать таких ученых, как Т. А. Полякова, А. В. Минбалева, Н. Н. Ковалева и др.

Несмотря на то, что многие вопросы по теме исследования достаточно изучены в научной среде, представляется, что отдельные аспекты еще остаются дискуссионными и нуждаются в более детальной проработке на уровне научной статьи. Данное обстоятельство также подтверждает актуальность проводимого исследования.



## Проекты в России и мире

Переходя непосредственно к исследованию особенностей использования информационных технологий в сфере высшего образования в России, следует определиться с историческими этапами формирования соответствующего правового регулирования в указанной сфере.

Такое явление, как цифровизация, не является новым для отечественного правопорядка. Соответствующая правовая основа начала формироваться еще в 90-е гг. XX в. Однако сам процесс практического воплощения цифровых технологий в общественные отношения происходил достаточно медленно.

В 1993 г. была утверждена Концепция правовой информатизации России<sup>2</sup>, а двумя годами позже принята президентская программа «Правовая информатизация органов государственной власти Российской Федерации». В документе отмечалось, что «в качестве основных средств тиражирования и распространения эталонных баз правовой информации должны использоваться высокоскоростные каналы и системы цифровой передачи данных, обеспечивающие конфиденциальность, безопасность, надежность и своевременность передачи информации».

В 2006 г. издается Федеральный закон «Об информации, информационных технологиях и о защите информации»<sup>3</sup>, который предусматривал свободу поиска, получения, передачи, производства и распространения информации любым законным способом.

Следует отметить, что в 2018 г. был принят Указ Президента № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»<sup>4</sup> (далее — Указ № 204). В нем ставится цель развития страны, и в первую очередь говорится о применении высоких технологий во всех сферах жизни общества и государственного управления в целом. В частности, в п. 11 Указа № 204 отмечается, что уже происходит постепенное внедрение информационных технологий в сферу высшего образования<sup>5</sup>. В высших учебных заведениях необходимо создавать условия функционирования информационной образовательной среды для освоения обучающимися образовательных программ.

Дополнительно развитие правовой регламентации указанных вопросов просматривается и в рамках таких подзаконных нормативных правовых актов, как приказ Минобрнауки России от 23.08.2017 № 816<sup>6</sup>.

<sup>2</sup> Указ Президента РФ от 28.06.1993 № 966 (ред. от 22.03.2005) «О Концепции правовой информатизации России» // Российские вести. 1993. № 132.

<sup>3</sup> Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

<sup>4</sup> Указ Президента РФ от 07.05.2018 № 204 (ред. от 21.07.2020) «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // СЗ РФ. 2018. № 20. Ст. 2817.

<sup>5</sup> Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 29.12.2022) «Об образовании в Российской Федерации» // СЗ РФ. 2012. № 53 (ч. I). Ст. 7598.

<sup>6</sup> Приказ Минобрнауки России от 23.08.2017 № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образователь-

В данной связи в России в сфере высшего образования уже активно используются информационные технологии, например, платформа Zoom, Microsoft Teams Яндекс Телемост, Sberjazz и др. Появляются и популяризируются вебинары с использованием ИТ-технологий, профессиональные тренинги и онлайн-курсы.

Следует отметить, что на международной арене также идет активный процесс внедрения цифровых технологий в сферу высшего образования.

При этом в ряде зарубежных стран реализуются проекты, которые неизвестны отечественному правопорядку. Так, «университет штата Бойсе запустил пилотную версию модели обучения на основе подписки. Паспорт на обучение стоит 425 долларов США в месяц за шесть кредитных часов или 525 долларов США за девять в любой из двух онлайн-программ бакалавриата. Это на 30 % дешевле, чем обучение по очной форме. За ежемесячную плату студенты могут выбрать свои собственные курсы для посещения и рассчитывать на долгосрочный доступ к консультациям и профессиональной помощи. Технологический институт Джорджии также рассматривает модель “Паспорт на образование” для практического использования. Это позволит студентам снизить расходы на образование и выбрать более концентрированные курсы»<sup>7</sup>.

Зарубежный опыт практики применения цифровых технологий повышает эффективность образовательного процесса, вовлеченность обучающихся в связи с использованием образовательных видеокурсов, геймификации, VR/AR-технологий, что превращает учебный процесс в захватывающую игру.

Сегодня стремительно меняются подходы к преподаванию, и нам необходимо изучать и применять международные практики, ведь для современных детей и молодежи новые цифровые технологии становятся предпочтительным средством обучения.

В зарубежных странах активно реализуется и политика в сфере смешанного образования. Речь идет о том, что в рамках такого механизма происходит и очное обучение, и онлайн-обучение. Более того, нельзя не указать и на внедрение в сферу образования технологии блокчейн.

В зарубежных странах процесс цифровизации образовательных услуг шире, чем в России. В рамках отечественного правопорядка происходит только базовое развитие правового регулирования в данной сфере и практической реализации исследуемого направления. Необходимо совершенствовать применение цифровых технологий, использовать различные способы обучения: дистанционное, интерактивное, электронное. Стоит отметить, что использование высоких технологий в обучении должно сопровождаться кибербезопасностью образовательных учреждений.

---

ных программ» // URL: [https://www.consultant.ru/document/cons\\_doc\\_law\\_278297/](https://www.consultant.ru/document/cons_doc_law_278297/) (дата обращения: 18.01.2023).

<sup>7</sup> Козлова Н. Ш., Козлов Р. С., Козлова Д. Р. Современные тенденции цифровизации образования (обзор зарубежного опыта) // Шаг в науку : сборник материалов IV Международной научно-практической конференции с участием студентов. Грозный, 15 октября 2021 г. Грозный : Чеченский государственный педагогический университет ; Алеф, 2021. С. 302.



## Вопросы правового регулирования

В 2002 г. была принята федеральная целевая программа «Электронная Россия (2002—2010)»<sup>8</sup>, а после ее завершения — государственная программа «Информационное общество»<sup>9</sup>. Обе программы предусматривали использование в экономике страны широкого спектра сетевых технологий, создание разделов «Электронное правительство» и «Электронные услуги» на официальных сайтах правительств в субъектах Российской Федерации.

Кроме того, в 2017 г. Президентом страны утверждена Стратегия развития информационного общества в Российской Федерации на 2017—2030 годы<sup>10</sup> (далее — Стратегия), которая определила цели, задачи и меры по реализации внутренней и внешней политики нашего государства в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Стоит отметить, что цифровизация уже затронула и сферу высшего образования. В частности, положения Стратегии постепенно начали реализовываться на практике. Определенным толчком к внедрению цифровых технологий в сферу высшего образования стала пандемия COVID-19, которая концептуально сказалась на реформировании процесса оказания образовательных услуг. Главным образом речь идет о дистанционном обучении.

То есть внедрение информационных технологий в высшем образовании предусматривает значительное изменение традиционного метода обучения.

Таким образом, на основании рассмотренных нормативных правовых актов можно сделать вывод о том, что использование информационных технологий в высшем образовании — это совокупность всех электронно-образовательных ресурсов, информационных ресурсов и технологий, а также средств обеспечения доступа к этим ресурсам.

## Принципы правового регулирования

На сегодняшний день основополагающие принципы использования информационных технологий заключаются в обеспечении информационной открытости для населения. Именно информационная открытость поможет снять социальную напряженность между гражданами и органами власти посредством увеличения информационных ресурсов.

<sup>8</sup> Постановление Правительства РФ от 28.01.2002 № 65 (ред. от 09.06.2010) «О федеральной целевой программе “Электронная Россия (2002—2010 годы)”» // СЗ РФ. 2002. № 5. Ст. 531.

<sup>9</sup> Постановление Правительства РФ от 15.04.2014 № 313 (ред. от 25.11.2022) «Об утверждении государственной программы Российской Федерации “Информационное общество”» // СЗ РФ. 2014. № 18 (ч. II). Ст. 2159.

<sup>10</sup> Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

Практика показывает, что использование информационных технологий в образовательной сфере находится на хорошем уровне. Об этом свидетельствуют постоянное обновление сайтов вузов, их приемных комиссий, доступ к электронным библиотечным системам и ресурсам.

Актуально это и для сферы высшего образования. Можно отметить, что в последнее время активно развиваются личные интернет-страницы высших учебных заведений, на которых публикуются важные новости.

Также специальные принципы использования информационных технологий в сфере высшего образования можно выявить непосредственно из анализа положений ст. 16 Федерального закона «Об образовании в Российской Федерации», как, например, принцип добровольности использования электронного обучения и дистанционных образовательных технологий (ч. 2 указанной статьи). Каждый вуз вправе самостоятельно разрешить вопрос о необходимости задействования в образовательном процессе информационных технологий.

В рамках использования информационных технологий в сфере высшего образования будут применяться и принципы правового регулирования, которые относятся к сфере персональных данных (что косвенно вытекает из положений ч. 3 указанной статьи). Это связано в первую очередь с обеспечением должной степени защиты и конфиденциальности персональных данных субъектов образовательного процесса.

Таким образом, правовое регулирование использования информационных технологий в сфере высшего образования строится как на общих, так и специальных принципах, которые можно вывести, например, из положений Федерального закона «Об образовании в Российской Федерации».

## Проблемы совершенствования законодательства

Цифровые технологии, улучшающие нашу жизнь, являются на сегодняшний день важнейшей и неотъемлемой частью общества и государства в целом. Правительства ведущих стран понимают необходимость развития технологических сил и ищут способы использовать их на благо граждан и организаций.

Внедрение цифровых технологий в сферу высшего образования сопряжено с различными проблемами, которые подвергаются активному обсуждению на доктринальном уровне. Исследователями неоднократно поднимались дискуссионные вопросы о слабой правовой регламентации, а также об отсутствии единого понимания понятийного аппарата. Отсутствует и содержательное правовое регулирование использования цифровых технологий в образовательном процессе.

Более того, условия пандемии предопределили необходимость перевода обучающихся на дистанционное обучение. Данный опыт позволил выявить как положительные, так и отрицательные аспекты дистанционного обучения. При этом качество оказываемых образовательных услуг в высших учреждениях пострадало, по мнению большинства обучающихся, что подтверждается и практикой правоприменения, а именно количеством споров, связанных с качеством образовательных услуг в условиях дистанционного обучения. Как следствие,



возникает необходимость в более скрупулезном анализе такого опыта внедрения дистанционного обучения в практику российских высших учебных заведений.

Фактически практика показала, что образовательные учреждения оказались неготовыми к полному переходу на дистанционное обучение. Права обучающихся на получение качественных образовательных услуг оказались не в полной мере выполнимыми. Кроме того, преподавателям также было достаточно сложно идентифицировать наличие обучающихся на занятиях. В связи с этим образовательный процесс в условиях дистанционного формата оказался малоэффективным.

При этом все проблемы использования информационных технологий в сфере высшего образования в России можно поделить на правовые и организационные.

### Выводы и предложения

Нами были отмечены проблемы, возникшие при внедрении дистанционного обучения в практику российских высших учебных заведений, однако следует отметить, что при правильном подходе к выстраиванию политики по внедрению дистанционного обучения в области высшего образования можно прогнозировать спрос и на высшее образование в целом<sup>11</sup>.

Иными словами, граждане перестают видеть перспективность получения высшего образования. Как следствие, спрос на поступление в высшие учебные заведения уменьшается. Главным образом это связано с нежеланием тратить время на посещение занятий, малым количеством бюджетных мест и одновременно ростом цен на образовательные услуги и др.

В данной связи возможно было бы предусмотреть набор обучающихся по определенным образовательным программам именно на условиях дистанционного обучения. Это позволит студентам экономить время, заниматься обучением в любом удобном месте. Более того, дистанционное обучение в полной мере позволяет совмещать работу и учебу. Представляется, что проработанность вопросов организационного, технического и правового характера позволит в полной мере повысить перспективность высшего образования.

Вместе с тем для внедрения дистанционного обучения необходимо устранить возможные проблемы и учесть уже имеющийся в высших образовательных учреждениях опыт обучения в режиме онлайн.

П. А. Огорельцев видит проблему, связанную с внедрением дистанционного обучения, в уходе из вузов преподавателей старшего возраста, поскольку им сложно будет подстроиться под дистанционный формат обучения<sup>12</sup>. Разрешить эту проблему, на наш взгляд, можно путем *частичного* внедрения дистанционного обучения в сферу высшего образования, а именно предусмотреть дистанционную

<sup>11</sup> Как в России устроена система высшего образования // URL: <https://journal.tinkoff.ru/statistic-universities/> (дата обращения: 18.01.2023).

<sup>12</sup> Огорельцев П. А., Купорез К. Д. Высшее образование в условиях пандемии: итоги и проблемы дистанционного обучения // Документ. Архив. История. Современность. 2021. № 21. С. 45.

форму обучения в том виде, в каком она была организована в условиях пандемии<sup>13</sup>.

В этой связи представляется возможным также не только позаимствовать опыт зарубежных стран по внедрению смешанного обучения (и его содержательного правового регулирования), но и, например, учесть опыт модели «Паспорт на образование».

Таким образом, одним из перспективных направлений развития высшего образования в России является внедрение возможности обучения в дистанционном формате. В связи с этим современная государственная политика должна быть выстроена с учетом данного фактора. При этом необходимо разрешить возможные проблемы организационного, технического и правового характера, принимая во внимание имеющийся опыт дистанционного обучения в государстве.

Предлагается дополнить Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» самостоятельной главой о дистанционном обучении. В рамках данной главы должны быть установлены особенности получения высшего образования в электронном формате, специфика организации занятий в дистанционном режиме и т.д.

Представляется, что развитие дистанционного обучения в Российской Федерации позволит повысить и востребованность получения высшего образования, подготовку кадров, специализирующихся на использовании цифровых технологий, что особенно важно в условиях цифровой революции.

## БИБЛИОГРАФИЯ

1. *Абрамчикова Н. В.* Дистанционное обучение как один из инновационных подходов в подготовке специалистов высшего образования // *Фундаментальные и прикладные исследования в области управления, экономики и торговли : сборник трудов Всероссийской научно-практической и учебно-методической конференции.* Санкт-Петербург, 1—4 июня 2021 г. — СПб. : Политех-Пресс, 2021.
2. Как в России устроена система высшего образования // URL: <https://journal.tinkoff.ru/statistic-universities/> (дата обращения: 18.01.2023).
3. *Козлова Н. Ш., Козлов Р. С., Козлова Д. Р.* Современные тенденции цифровизации образования (обзор зарубежного опыта) // *Шаг в науку : сборник материалов IV Международной научно-практической конференции с участием студентов.* Грозный, 15 октября 2021 г. — Грозный : Чеченский государственный педагогический университет ; Алеф, 2021. — С. 301—305.
4. *Огорельцев П. А., Купорез К. Д.* Высшее образование в условиях пандемии: итоги и проблемы дистанционного обучения // *Документ. Архив. История. Современность.* — 2021. — № 21.

<sup>13</sup> *Абрамчикова Н. В.* Дистанционное обучение как один из инновационных подходов в подготовке специалистов высшего образования // *Фундаментальные и прикладные исследования в области управления, экономики и торговли : сборник трудов Всероссийской научно-практической и учебно-методической конференции.* Санкт-Петербург, 1—4 июня 2021 г. СПб. : Политех-пресс, 2021. С. 32.





**Марина Борисовна  
ДОБРОБАБА,**

профессор кафедры  
информационного права  
и цифровых технологий  
Университета имени  
О.Е. Кутафина (МГЮА),  
профессор кафедры  
административного и  
финансового права  
Российской таможенной  
академии,  
доктор юридических наук,  
доцент  
**[mbdobrobaba@msal.ru](mailto:mbdobrobaba@msal.ru)**  
125993, Россия, г. Москва,  
ул. Садовая-Кудринская, д. 9

## Понятие персональных данных: проблема правовой определенности

**Аннотация.** В статье анализируется проблема содержания правовой дефиниции «персональные данные». На основе проведенного исследования автором делается вывод о том, что под определение персональных данных, имеющее нормативное закрепление, в силу его широты подпадает практически любая информация, что не позволяет обеспечить должную защиту прав субъекта персональных данных, а кроме того, может нарушить его иные гарантируемые законодательством права. Автор показывает, что гибкий режим персональных данных исключает необходимость установления их исчерпывающего перечня, что допускает возможность закрепления в законодательстве видов персональных данных, подлежащих свободному обращению, в том числе определение перечня случаев использования персональных данных без получения согласия заинтересованного лица.

При решении вопроса об отнесении к персональным данным той или иной информации предложен следующий алгоритм: анализ положений отраслевого законодательства на предмет перечисления сведений, относящихся к персональным данным; при отсутствии такового — анализ судебной практики по аналогичным делам, применение разъяснений Роскомнадзора и Минцифры; использование метода идентификации. Обосновано, что ввиду неоднозначного судебного толкования категории «персональные данные», в ряде случаев не совпадающего с позицией Роскомнадзора, требуется выработка единых подходов к толкованию норм законодательства о персональных данных со стороны высшей судебной инстанции.

**Ключевые слова:** персональные данные, личность гражданина, субъект персональных данных, оператор, информация, идентификация, отраслевое законодательство, разъяснения Роскомнадзора, судебная практика.

DOI: 10.17803/2311-5998.2023.102.2.042-052

**MARINA B. DOBROBABA,**

*Professor of the Department of information law and digital technologies  
of the Kutafin Moscow State Law University (MSAL),  
Professor of the Department of administrative and financial law  
of the Russian Customs Academy, Dr. Sci. (Law), Associate professor  
mbdobrobaba@msal.ru  
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993*

**Concept of personal data: the Problem of Legal Certainty**

**Abstract.** *The article analyzes the problem of the content of the legal definition of “personal data”. On the basis of the study, the author concludes that, due to its breadth, almost any information falls under the definition of personal data, which has a regulatory framework, which does not allow for adequate protection of the rights of the subject of personal data, in addition, may violate other rights guaranteed by law. The author shows that the flexible mode of personal data eliminates the need to establish an exhaustive list of them, which allows for the possibility of enshrining in the legislation the types of personal data subject to free circulation, including the definition of a list of cases of using personal data without obtaining the consent of the person concerned. When deciding whether to classify this or that information as personal data, the following algorithm is proposed: analysis of the provisions of sectoral legislation for listing information related to personal data; in the absence of such, an analysis of judicial practice in similar cases, the application of clarifications from Roskomnadzor and the Ministry of Digital Development; use of the identification method. It is substantiated that due to the ambiguous judicial interpretation of the category “personal data”, which in some cases does not coincide with the position of Roskomnadzor, it is necessary to develop common approaches to the interpretation of the norms of legislation on personal data by the highest court.*

**Keywords:** *personal data, identity of a citizen, subject of personal data, operator, information, identification, industry legislation, clarifications of Roskomnadzor, judicial practice.*

**Актуальность проблемы**

Персональные данные представляют собой довольно сложный формирующийся правовой институт. Перечень данных, признаваемых персональными в силу требований законодательства, неуклонно расширяется, что влечет за собой усложнение связей между субъектами правоотношений, складывающихся по поводу персональных данных. Несмотря на определенные преимущества увеличения обмена информацией, появляются факторы, свидетельствующие об угрозах для ряда конституционных прав граждан: на неприкосновенность частной жизни, личную и семейную тайну.

Для минимизации данных угроз важно решение проблемы, связанной с обработкой и защитой персональных данных, что, прежде всего, требует выявления содержания дефиниции «персональные данные» и будет способствовать обеспечению невмешательства в частную жизнь<sup>1</sup>.

### Понятие персональных данных

Согласно п. 1 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) «О персональных данных»<sup>2</sup> (далее — Закон о персональных данных), к *персональным данным* может быть отнесена «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)». Данное определение корреспондирует дефиниции, изложенной в Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (п. «а» ст. 2)<sup>3</sup>.

Термин «персональный» происходит от латинского слова *persōna* — личность, личный, присущий каждому отдельному индивидууму<sup>4</sup>. Соответственно, информация, относящаяся к юридическому лицу, к персональным данным не относится. В этом плане интересно изучение зарубежного опыта. Так, в Великобритании, в «Акте о защите данных о физических лицах», содержится прямое указание на «живое» физическое лицо<sup>5</sup>.

Несмотря на то, что в отечественном законодательстве подобное уточнение не делается, остается до конца не решенным вопрос о том, можно ли считать субъектом персональных данных юридическое лицо. Так, согласно Федеральному закону от 07.07.2003 № 126-ФЗ (ред. от 14.07.2022) «О связи»<sup>6</sup>, к информации ограниченного доступа относятся следующие сведения об абонентах — юридических лицах: наименование (фирменное наименование) абонента — юридического лица, фамилия, имя, отчество руководителя и работников этого юридического лица, а также адрес абонента или адрес установки оконечного оборудования, абонентские номера и другие данные, позволяющие идентифицировать абонента

<sup>1</sup> См.: *Симонова Е. В.* Определение понятия персональных данных в Российской Федерации // Молодой ученый. 2017. № 10 (144). С. 323—326.

<sup>2</sup> СЗ РФ. 2006. № 31 (ч. I). Ст. 3451 ; 2022. № 29 (ч. III). Ст. 5233.

<sup>3</sup> Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом министров в Страсбурге 15.06.1999) // СЗ РФ. 2014. № 5. Ст. 419.

<sup>4</sup> Словарь иностранных слов, вошедших в состав русского языка: материалы для лексической разработки заимствованных слов в рус. лит. речи / сост. А. Н. Чудинов. 3-е изд., испр. и доп. (более 5 000 новых слов) преимущественно соц.-полит. терминами, вошедшими в жизнь в последние годы. СПб., 1910.

<sup>5</sup> Персональные данные // URL: <http://elibsystem.ru/docs/personal-data> (дата обращения: 13.01.2023).

<sup>6</sup> СЗ РФ. 2003. № 28. Ст. 2895 ; 2022. № 29 (ч. III). Ст. 5323.

или его окончное оборудование, в том числе идентификатор пользовательского оборудования (окончного оборудования), сведения баз данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента (п. 1 ст. 53). Примечательно, что в ряде государств осуществляется защита персональных данных не только физических, но и юридических лиц (Австрия, Исландия, Швейцария).

Следует признать, что в законодательстве отсутствует нормативно закрепленный исчерпывающий перечень сведений, которые являются персональными данными. В то же время Закон о персональных данных в ред. от 04.06.2011 содержал открытый перечень персональных данных, в который входили: фамилия, имя, отчество субъекта персональных данных, год, месяц, дата и место его рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, а также другая информация.

В судебной практике преобладает судебное толкование через открытое определение персональных данных, содержащееся в прежней редакции Закона о персональных данных<sup>7</sup>. Очевидно, что установленный ранее перечень, включающий помимо конкретных перечисленных сведений «другую информацию», не решил проблему конкретизации персональных данных, что вызывало сложности у правоприменителя.

В настоящее время отношение законодателя к понятию «персональные данные» трансформировалось: сократив его словесную формулировку, законодатель по смысловой нагрузке сделал данное понятие «гораздо более широким»<sup>8</sup>, при этом понимание персональных данных стало контекстно-ориентированным, позволяющим определить физическое лицо в совокупности с другими данными<sup>9</sup>. Так, Роскомнадзор указал, что принцип идентификации физического лица *по фамилии, имени, отчеству* из всего массива информации не является единственно возможным критерием отнесения обработанных сведений к персональным данным<sup>10</sup>.

При отнесении к персональным данным той или иной информации не имеет значения, носит она объективный или оценочный характер, получена непосредственно от субъекта персональных данных или из любых других источников, создана на основе другой информации и т.д. Так, информация о наличии серьезного заболевания у конкретного гражданина носит объективный характер и является персональными данными, относящимися к специальной категории (сведения о состоянии здоровья), несмотря на то, что впоследствии диагноз о наличии данного заболевания у этого гражданина может не подтвердиться. Другая информация о гражданине, заключающаяся в том, что он является ненадежным

<sup>7</sup> См.: постановление Арбитражного суда Северо-Кавказского округа от 03.04.2019 № Ф08-1028/2019 по делу № А53-26369/2018 ; постановление Тринадцатого арбитражного апелляционного суда от 21.06.2010 по делу № А56-4788/2010.

<sup>8</sup> См.: *Бычков А. И.* Категории персональных данных // СПС «КонсультантПлюс».

<sup>9</sup> *Савельев А. И.* Электронная коммерция в России и за рубежом: правовое регулирование. М. : Статут, 2016.

<sup>10</sup> Письмо Роскомнадзора от 20.01.2017 № 08АП-6054 «О результатах рассмотрения обращения Казначейства России».

и недобросовестным должником, носит оценочный характер, однако при этом также охватывается понятием персональных данных<sup>11</sup>.

Столь широкий и абстрактный подход к понятию персональных данных не представляется удачным, поскольку не позволяет четко дифференцировать информацию и безошибочно определить возможность отнесения ее к персональным данным. Это, в свою очередь, может оказать негативное влияние на защиту прав субъекта персональных данных либо создаст препятствия в реализации его иных прав, гарантированных законодательством.

### Режим персональных данных

Отнесение персональных данных к информации ограниченного доступа позволяет сделать вывод об их специальном режиме. Примечательно, что значительная часть персональных данных является открытой. Речь в данном случае идет о «номинативной» информации, к которой относятся: фамилия, имя, отчество лица.

Однако при наличии тех или иных обстоятельств субъект персональных данных может ограничить их использование, и данная информация уже будет рассматриваться как конфиденциальная, охватываемая режимом той или иной тайны (например, коммерческой или профессиональной), что демонстрирует гибкость режима персональных данных<sup>12</sup>.

### Анализ судебной практики и позиций Роскомнадзора

Как показывает анализ судебной практики, к персональным данным относят довольно широкий перечень сведений, включающий, например: содержание кадастрового паспорта, адрес индивидуального предпринимателя, информацию об имуществе лица, информацию о пересечении государственной границы гражданином, условия трудового договора работника, ИНН, реквизиты банковской карты лица и т.д.<sup>13</sup>

Следует признать, что ни в Конвенции Совета Европы, ни в последующих за ее принятием разъяснениях, ни в российском законодательстве не приводятся критерии отграничения персональных данных физического лица от иной информации о нем, что вызывает определенные сложности у правоприменителя. Отсутствие единообразного подхода к решению вопроса о содержании категории «персональные данные» приводит к тому, что каждый суд проявляет свои подходы к толкованию данного понятия. Более того — порой суды и Роскомнадзор как орган, выполняющий контрольно-надзорные функции в области

<sup>11</sup> Савельев А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». 2-е изд., перераб. и доп. М. : Статут, 2021. 468 с.

<sup>12</sup> Минбалева А. В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2012. № 2 (14). С. 7.

<sup>13</sup> См., например: апелляционное определение Верховного суда Республики Саха (Якутия) от 23.10.2013 № 33-4172/13.

защиты персональных данных, демонстрируют противоположные подходы к толкованию дефиниции «персональные данные», что также усложняет правоприменение.

**IP-адрес пользователя Сети как персональные данные.** Суды не единодушны в решении вопроса об отнесении к персональным данным *IP-адреса пользователя Сети*, в одних случаях признавая данную информацию персональными данными<sup>14</sup>, в других — не признавая ее таковыми<sup>15</sup>. Представляется необходимым, исходя из возможности идентификации пользователя, рассматривать отдельно статический и динамический IP-адреса пользователя. Поскольку идентификация пользователя сети Интернет осуществляется через установление его персональных данных по IP-адресу, назначаемому оператором связи и закрепленному за ним при заключении договора на оказание услуг доступа к сети Интернет (статистический IP-адрес), данная информация должна признаваться персональными данными. В свою очередь, динамический адрес пользователя к персональным данным не относится (решение Октябрьского районного суда г. Самары от 24.09.2015 по делу № 2-5354/2015).

На практике владельцы доменов, разработчики мобильных приложений в целях подстраховки включают в политику обработки персональных данных пункт об IP-адресе и в целом о любых технических параметрах устройств пользователя. Так, разрешая спор Роскомнадзора и МТС, суд пришел к выводу об отнесении к персональным данным собираемых с помощью *cookie-файлов* сведений (дело № А40-14902/16). Неслучайно пользователи уведомляются о применении данной технологии с помощью всплывающего окна. Лицо, не согласное с получением его данных таким способом, вправе покинуть сайт<sup>16</sup>.

**Паспортные данные как персональные данные.** Спорным является и вопрос об отнесении к персональным данным *паспортных данных*, что объясняется отсутствием нормативного закрепления понятия «паспортные данные», а также указанием в различных нормативных актах на признаки, идентифицирующие лицо. Так, в Налоговом кодексе РФ пометка на учет физических лиц сопровождается предоставлением сведений: фамилия, имя, отчество; дата и место рождения; пол; место жительства; данные паспорта или иного документа, удостоверяющего личность налогоплательщика; данные о гражданстве (п. 1 ст. 84)<sup>17</sup>.

Вместе с тем относить все данные паспорта к персональным данным вряд ли необходимо, учитывая, что данный документ включает в себя две категории сведений: сведения о личности гражданина и обязательные реквизиты бланка паспорта. Так, согласно Положению о паспорте гражданина Российской Федерации, утв. постановлением Правительства РФ от 08.07.1997 № 828 (ред. от

<sup>14</sup> См., например: постановление Второго арбитражного апелляционного суда от 08.08.2019 № 02АП.5517/2019 по делу № А31-3955/2019.

<sup>15</sup> См., например: постановление Восемнадцатого арбитражного апелляционного суда от 05.04.2017 № 18АП-2210/2017 по делу № А07-24090/2016.

<sup>16</sup> Балдынова А. Персональные данные // Административное право. 2020. № 4. С. 23—27.

<sup>17</sup> Налоговый кодекс РФ (часть первая) от 31.07.1998 № 146-ФЗ (ред. от 28.12.2022) // СЗ РФ. 1998. № 31. Ст. 3824 ; Российская газета. 2022. 30 дек.

15.07.2021)<sup>18</sup>, в паспорт вносятся следующие *сведения о личности гражданина*: фамилия, имя, отчество, пол, дата рождения и место рождения (п. 4).

Возникает вопрос: если сведения о личности гражданина однозначно относятся к персональным данным, можно ли отнести к ним реквизиты паспорта как документа? Ответ на этот вопрос можно дать, определив, какие из перечисленных данных позволяют идентифицировать личность гражданина.

Полагаем, что реквизиты, относящиеся исключительно к бланку документа, не являются персональными данными, поскольку они не связаны с личностью гражданина (например, сведения об органе, выдавшем документ, о дате выдачи). Что же касается серии и номера паспорта, то они строго индивидуальны, что позволяет идентифицировать личность владельца документа. Подобный вывод подтверждает и практика высшей судебной инстанции<sup>19</sup>.

Однако и в данном случае судебная практика не отличается единообразием: в одних случаях применяется более широкий подход, при котором к персональным данным, помимо *сведений о личности владельца*, относят отдельные реквизиты бланка документа, такие как серия, номер паспорта, дата выдачи<sup>20</sup>, в других подобные сведения не относят к персональным данным<sup>21</sup>.

**Иные государственные идентификаторы физического лица.** Спорным является и практика отнесения к персональным данным иных государственных идентификаторов — ИНН, СНИЛС. Так, с одной стороны, ИНН, используемый в целях налогового учета, представляет собой не что иное, как набор цифр, который сам по себе не позволяет идентифицировать его владельца<sup>22</sup>. Однако данные сведения можно отнести к общим дополнительным персональным данным. Согласно разъяснениям представителей Роскомнадзора, государственные идентификаторы физического лица — это его персональные данные<sup>23</sup>.

**Электронная почта и номер телефона.** Не решена однозначно проблема отнесения к персональным данным электронной почты и номера телефона гражданина, являющихся, наряду с Ф.И.О. наиболее часто обрабатываемыми данными. Так, постановлением Правительства РФ от 13.09.2019 № 1197<sup>24</sup> состав сведений, размещаемых в единой информационной системе персональных

<sup>18</sup> СЗ РФ. 1997. № 28. Ст. 3444 ; 2021. № 30. Ст. 5782.

<sup>19</sup> См.: определение Верховного Суда РФ от 08.09.2020 № 308-ЭС20-11154 по делу № А63-13382/2019.

<sup>20</sup> Определение Московского городского суда от 13.05.2019 № 4г-4164/19.

<sup>21</sup> См.: постановление Седьмого арбитражного апелляционного суда от 05.04.2018 № 07АП-1437/2018 по делу № А45-31682/2017.

<sup>22</sup> Апелляционное определение Санкт-Петербургского городского суда от 03.02.2015 № 33-1644/2015 по делу № 2-3097/2014 // СПС «КонсультантПлюс».

<sup>23</sup> Публичный семинар Роскомнадзора по персональным данным и планы рабочей группы ЮФО // URL: <https://www.securitylab.ru/blog/personal/sborisov/347661.php> (дата обращения: 15.01.2023).

<sup>24</sup> См.: постановление Правительства РФ от 13.09.2019 № 1197 «О внесении изменения в состав сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предо-

данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, был дополнен пунктом «д» о контактных данных физического лица (номере абонентского устройства подвижной радиотелефонной связи, адресе электронной почты).

Вместе с тем по данному вопросу позиции Роскомнадзора и судебных инстанций диаметрально противоположны, отсутствует единый подход и у судебных органов. Так, по мнению Роскомнадзора, номер телефона является всего лишь атрибутом аппаратного средства связи<sup>25</sup>, поэтому обособленно от каких-либо других данных номер телефона не относится к персональным данным. Как только оператор обрабатывает данные в совокупности (например, фамилию, имя, отчество и телефон или фамилию, имя, отчество и адрес электронной почты), речь идет об обработке оператором персональных данных.

Неоднозначность судебной практики по данному вопросу можно продемонстрировать на примере следующих дел. Так, районный суд города Москвы, рассматривая дело, в котором коллекторской компанией без получения согласия взыскателя на использование данных его телефонного номера осуществлялся дозвон, посчитал, что данный факт свидетельствует о нарушении Закона о персональных данных<sup>26</sup>. Одним из определений Верховного Суда РФ номер телефона гражданина также был отнесен к его персональным данным<sup>27</sup>.

В другом случае суд, соглашаясь с Роскомнадзором, не увидел нарушений в размещении компанией в сети Интернет телефонного номера гражданина города Белгорода без указания его владельца. Как было указано в решении суда, номер телефона не позволяет провести идентификацию, а значит, не может быть отнесен к персональным данным<sup>28</sup>.

Что касается адреса электронной почты, то согласно разъяснениям Роскомнадзора, к персональным данным относится только такой электронный адрес, который содержит информацию о фамилии, имени и отчестве лица.

## Выводы и предложения

Широкая трактовка понятия персональных данных и неоднозначность правоприменительной деятельности требуют правовой определенности в решении вопроса о том, какая информация относится к персональным данным.

---

ставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных» // СЗ РФ. 2019. № 38. Ст. 5310.

<sup>25</sup> О персональных данных // Управление Роскомнадзора по центральному федеральному округу. URL: <https://77.rkn.gov.ru/p3852/p13239/p13309/> (дата обращения: 15.01.2023).

<sup>26</sup> Решение Черемушкинского районного суда г. Москвы от 18.06.2019 по делу № 12-973\_2019.

<sup>27</sup> Определение Судебной коллегии по гражданским делам Верховного Суда РФ от 01.08.2017 № 78-КГ17-45.

<sup>28</sup> Решение Октябрьского районного суда г. Белгорода от 12 сентября 2019 г. по делу № 12-393/2019).



Представляется целесообразным использовать следующие подходы.

1. При решении вопроса об отнесении к персональным данным той или иной информации определяющими являются *положения отраслевого законодательства*, которые напрямую перечисляют сведения, относящиеся к персональным данным в рамках соответствующих отраслевых правоотношений.

Так, согласно трудовому законодательству, *при заключении трудового договора* персональными данными являются перечисленные в ст. 65 Трудового кодекса РФ<sup>29</sup> документы: паспорт или иной документ, удостоверяющий личность; трудовая книжка; ИНН; документ об образовании и (или) о квалификации или наличии специальных знаний; справка о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям; справка о том, является или не является лицо подвергнутым административному наказанию за потребление наркотических средств или психотропных веществ без назначения врача либо новых потенциально опасных психоактивных веществ и др.

К персональным данным, являющимся таковыми *при постановке лица на учет в налоговом органе*, относятся (п. 1 ст. 84 НК РФ): фамилия, имя, отчество; дата и место рождения; пол; место жительства; данные паспорта или иного документа, удостоверяющего личность налогоплательщика; данные о гражданстве.

Согласно транспортному законодательству, *при оформлении проездных документов (билетов) и формировании персонала (экипажей) транспортных средств* к персональным данным о пассажирах и персонале (экипаже) транспортных средств относятся: фамилия, имя, отчество; дата рождения; вид и номер документа, удостоверяющего личность, по которому приобретается проездной документ (билет); пункт отправления, пункт назначения, вид маршрута следования (беспересадочный, транзитный); дата поездки; пол; гражданство (п. 5 ст. 11 Федерального закона «О транспортной безопасности»<sup>30</sup>).

2. Если в отраслевом законодательстве соответствующие положения отсутствуют, в основу анализа должны быть положены: *судебная практика* по аналогичным делам, а также *разъяснения* Роскомнадзора и Минцифры России.

Следует отметить отсутствие однозначного ответа на вопрос, какая комбинация данных, по мнению законодателя, судебных и административных органов, является персональными данными, а какая нет. В связи с этим необходима выработка единых подходов к толкованию норм Закона о персональных данных со стороны высшей судебной инстанции.

3. Если предыдущие подходы не позволили однозначно решить вопрос о том, следует ли относить конкретную информацию к персональным данным, целесообразно использовать *метод идентификации*.

<sup>29</sup> Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ (ред. от 19.12.2022) // СЗ РФ. 2001. № 1 (ч. I). Ст. 3 ; 2022. № 29 (ч. III). Ст. 5250.

<sup>30</sup> Федеральный закон от 09.02.2007 № 16-ФЗ (ред. от 28.06.2022) «О транспортной безопасности» // СЗ РФ. 2007. № 7. Ст. 837 ; 2022. № 27. Ст. 4620.

В связи с этим представляет интерес предложенный Н. А. Воронковым тест, позволяющий идентифицировать личность человека посредством последовательного ответа на ряд вопросов<sup>31</sup>:

А. Содержатся ли в информации сведения о конкретном человеке? При отрицательном ответе данную информацию нельзя считать персональными данными. В противном случае предлагается ответить на следующий вопрос.

Б. Возможно ли определить на основе данной информации субъекта, о котором предоставлена информация? При положительном ответе предоставленные данные относятся к персональным данным, при отрицательном — следует продолжить опрос.

В. Возможно ли определить, о ком идет речь, получив дополнительные сведения? Положительный ответ позволяет отнести информацию к персональным данным.

Подводя итог, следует отметить, что нормативно закрепленное широкое определение персональных данных, отличаясь низким уровнем формальной определенности, позволяет отнести к персональным данным практически любую информацию. Вместе с тем ввиду стремительного развития информационных технологий составить исчерпывающий перечень персональных данных вряд ли возможно, да и нецелесообразно. Как верно отметил А. В. Минбалеев, гибкий режим персональных данных исключает необходимость установления их исчерпывающего перечня, что, однако, допускает возможность закрепления в законодательстве видов персональных данных, в отношении которых возможно их свободное обращение, в том числе определение перечня случаев использования персональных данных без получения согласия заинтересованного лица<sup>32</sup>.

В целом же для правоприменителя важно выработать четкие критерии, позволяющие однозначно определить, относится ли та или иная информация к персональным данным. Это позволит обеспечить их должную защиту, не допустить нарушения Закона о персональных данных и в целом упростит правоприменение, а следовательно, минимизирует риски привлечения к ответственности организаций, осуществляющих обработку и хранение персональных данных граждан.

## БИБЛИОГРАФИЯ

1. *Балдынова А.* Персональные данные // Административное право. — 2020. — № 4. — С. 23—27.
2. *Бычков А. И.* Категории персональных данных // СПС «КонсультантПлюс».
3. *Воронков Н. А.* Определение персональных данных // Молодой ученый. — 2022. — № 27 (422). — С. 78—80.
4. *Минбалеев А. В.* Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. — Безопасность в информационной сфере. — 2012. — № 2 (14). — С. 4—9.

<sup>31</sup> *Воронков Н. А.* Определение персональных данных // Молодой ученый. 2022. № 27 (422). С. 78—80.

<sup>32</sup> См.: *Минбалеев А. В.* Указ. соч. С. 8.

5. Приватность человека и защита его персональных данных // URL: [https://ethics.cdto.ranepa.ru/5\\_1](https://ethics.cdto.ranepa.ru/5_1) (дата обращения: 13.01.2023).
6. *Савельев А. И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». — 2-е изд., перераб. и доп. — М. : Статут, 2021. — 468 с.
7. *Савельев А. И.* Электронная коммерция в России и за рубежом: правовое регулирование. — М. : Статут, 2016.
8. *Симонова Е. В.* Определение понятия персональных данных в Российской Федерации // Молодой ученый. — 2017. — № 10 (144). — С. 323—326.
9. Словарь иностранных слов, вошедших в состав русского языка : материалы для лексической разработки заимствованных слов в рус. лит. речи / сост. А. Н. Чудинов. — 3-е изд., тщательно испр. и знач. доп. (более 5 000 новых слов) преимущественно соц.-полит. терминами, вошедшими в жизнь в последние годы. — СПб. : В. И. Губинский, 1910. — 676 с.

## Квазисубъекты в киберправе

**Аннотация.** Система субъектов киберправа находится в процессе постоянного развития, обусловленного появлением новых цифровых технологий. Актуальной теоретической проблемой является развитие теории квазисубъектов в праве и определение правового статуса электронного лица как квазисубъекта права.

Под квазисубъектом понимается лицо, не обладающее всеми признаками субъекта права. На основе объема правовых характеристик в киберпространстве можно выделить такие виды квазисубъектов, как лица: наделенные субъективными правами и обязанностями, но не несущие ответственность (интеллектуальные агенты, киберфизические системы, системы искусственного интеллекта, роботы); не обладающие правосубъектностью, но реализующие свои интересы через интересы субъектов права, как правило, в качестве конституционно-правового императива (будущие поколения).

**Ключевые слова:** киберправо, система субъектов киберправа, цифровые технологии, электронное лицо, квазисубъект права, системы искусственного интеллекта, киберфизические системы.



**Светлана Георгиевна ЧУБУКОВА,**

доцент кафедры  
информационного права и  
цифровых технологий  
Университета имени  
О.Е. Кутафина (МГЮА),  
кандидат юридических  
наук, доцент

**sgchubukova@msal.ru**  
125993, Россия, г. Москва,  
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2023.102.2.053-061

**SVETLANA G. CHUBUKOVA,**

Associate Professor of the Department  
of information law and digital technologies  
of the Kutafin Moscow State Law University (MSAL),  
Cand. Sci. (Law), Associate Professor  
**sgchubukova@msal.ru**

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

### Quasi-subjects in cyber law

**Abstract.** The system of subjects of cyber law is in the process of constant development due to the emergence of new digital technologies. An actual theoretical problem is the development of the theory of quasi-subjects in law and the definition of the legal status of an electronic person as a quasi-subject of law.

A quasi-subject is a person who does not possess all the characteristics of a subject of law. It is possible to distinguish such types of quasi-subject as persons: endowed with subjective rights and obligations, but not responsible (intellectual agents, cyberphysical systems, artificial intelligence systems, robots); not having legal personality, but realizing their interests through the interests of subjects of law, as a rule, as constitutional and legal imperative (future generations).

© Чубукова С. Г., 2023

**Keywords:** *cyber law, system of subjects cyber law, digital technologies, electronic person, quasi-subject of law, artificial intelligence systems, cyber-physical systems.*

Научный и технологический прогресс привел к появлению нестандартных, с точки зрения правовой науки, участников общественных отношений в цифровой среде. Системы искусственного интеллекта, киберфизические системы, роботы в настоящее время признаются уже нередко реальными участниками гражданского оборота, осуществляющими деятельность, автономную от их создателей и владельцев.

На практике данные технологии и системы не только выполняют предписанные разработчиком действия, но при этом сами являются инициаторами изменения своего поведения в киберпространстве. Технологии машинного обучения, самостоятельного извлечения знаний из предметной области, в которой функционирует подобная интеллектуальная система, создают определенную автономию от воли их создателей, владельцев и пользователей.

В киберпространстве появляются децентрализованные автономные организации (Decentralized autonomous organization, DAO), решения в которых принимаются в электронном виде на основе правил, реализованных в форме программы<sup>1</sup>. Они не имеют статуса юридического лица, их члены не заключают никаких официальных юридических договоров, не создаются традиционные органы управления. Деятельность строится на самоисполняемых умных контрактах (smart contracts), регулирующих поведение всех участников данного объединения. Это поставило перед юристами непростой вопрос о правовой идентификации данных технологических новаций.

По вопросу правового статуса новых появившихся участников отношений в киберпространстве, к которым сегодня можно отнести интеллектуальных (программных) агентов, роботов, киберфизические системы и другие интеллектуальные программные и технологические решения и системы, в юридической науке имеются абсолютно различные, нередко полярные точки зрения: от непризнания их в качестве возможных субъектов права до разработки правового статуса электронного лица и постановки других не менее спорных вопросов, связанных, например, с их ответственностью.

При этом во многих странах развивается практика правового регулирования отношений с участием данных электронных лиц. «Право превращает участников общественных отношений в субъекты правоотношений»<sup>2</sup>. По мнению британского футуролога Яна Пирсона, в ближайшем будущем электронные формы жизни получают конституционные права во многих государствах<sup>3</sup>.

<sup>1</sup> Например, DAO company, Digix.global and the cryptocurrency Dash.

<sup>2</sup> Венгеров А. Б. Теория государства и права : учебник. 2-е изд. М. : Омега-Л, 2005. С. 458—459.

<sup>3</sup> Ян Пирсон новую расу на Земле прогнозирует уже к 2030 году // Послезавтра. 22 марта 2012 г. URL: <http://poslezavtra.org.ua/?tag=2020>.

Следует отметить, что в юридической науке на протяжении ее истории уже предпринимались попытки осмысления с позиции права подобных и еще более абстрактных явлений.

Так, известный ученый, правовед Л. И. Петражицкий в своей психологической теории констатировал, что не только реальные, но и воображаемые существа могут быть субъектами прав и обязанностей. С позиции Петражицкого, договор, который суеверный или психически нездоровый человек подписывает с дьяволом, имеет императивно-атрибутивную природу. И, по мнению ученого, данная ситуация «не особо отличается от других случаев связывания себя волей несуществующих лиц, к которым относятся государство, юридические лица и другие образования, не обладающие волей, сознанием и вообще самостоятельным (от представлений людей) существованием, но которым люди приписывают власть над своим поведением»<sup>4</sup>.

Попытки рассмотреть в качестве субъекта права участников отношений, не обладающих всеми признаками субъекта, привели к появлению в науке и законодательстве таких новых понятий, как «квазиправосубъектность» и «квазисубъект права». Их применение в юридической доктрине связано, как правило, с обозначением таких лиц, общностей, организаций, которые не обладают всеми традиционно называемыми признаками субъекта права: сознанием, волей, субъективным интересом, субъективными потребностями и др.

Так, к квазисубъектам права относят: национальные меньшинства, коренные народы, субъекты федераций, непризнанные и самопровозглашенные государства<sup>5</sup>; нации, трудовые коллективы, семью<sup>6</sup>, неправительственные организации, международные организации, транснациональные корпорации<sup>7</sup>; собрания работников, их представительные органы<sup>8</sup>; иностранные организации, не являющиеся юридическими лицами по иностранному праву<sup>9</sup>.

В научной литературе уже предпринимаются попытки выделения признаков, характерных для феномена квазисубъекта права. Еще Н. Н. Алексеев подчеркивал, что для защиты определенной социально-правовой ценности законодатель наделяет ее правами, тем самым определяя ее правоспособность. Так, ценностью правопорядок признает не только активных правовых деятелей, но и социальные

<sup>4</sup> Петражицкий Л. И. Теория права и государства в связи с теорией нравственности. СПб., 2000. С. 98, 102—106.

<sup>5</sup> См.: Лукичев П. Н., Скорик А. П. Квазигосударственность // Полис. 2001. № 2. С. 139—142; Хабриева Т. Я. Введение // Правосубъектность: общетеоретический, отраслевой, и международно-правовой анализ: сборник материалов к XII Ежегодным научным чтениям памяти профессора С. Н. Братуся. М.: Статут, 2017. С. 28.

<sup>6</sup> Пономарева Е. В. Субъекты и квазисубъекты права: теоретико-правовые проблемы разграничения: дис. ... канд. юрид. наук. Екатеринбург, 2019. 208 с.

<sup>7</sup> См.: Черниченко С. В. Контуры международного права. Общие вопросы. М., 2014. С. 29, 315.

<sup>8</sup> Долинская В. В. Проблемы квазисубъектных образований в частном праве // Правосубъектность: общетеоретический, отраслевой, и международно-правовой анализ. С. 315.

<sup>9</sup> Елисеев И. В. Новое в коллизионном праве России // URL: [http://antonivanov.ru/balfort/collision\\_law.html](http://antonivanov.ru/balfort/collision_law.html) (дата обращения: 10 января 2023 г.).



коллективы, общности и животных, которые не обладают необходимым составом признаков субъекта права<sup>10</sup>.

Социально-правовая ценность «технологических» участников отношений в киберпространстве сегодня все чаще признается в правовом сообществе.

Вопрос правового статуса систем искусственного интеллекта и киберфизических систем приобрел актуальность в связи с выходом резолюции Европарламента от 16 февраля 2017 г. 2015/2013(INL) P8\_TA-PROV(2017)0051 «Нормы права о робототехнике»<sup>11</sup>, которая поставила вопросы о гражданско-правовом статусе и ответственности роботов и искусственного интеллекта.

До этого момента российская юридическая доктрина рассматривала роботов исключительно как технические устройства и относила их только к объектам права.

С выходом указанной резолюции Европарламента некоторые российские исследователи выступили с законодательными инициативами.

Так, Д. С. Гришиным был разработан проект федерального закона «О внесении изменений в Гражданский кодекс Российской Федерации в части совершенствования правового регулирования отношений в области робототехники». В нем предложено дополнить первую часть Гражданского кодекса главой «Роботы-агенты». Согласно сделанным предложениям, робот призван участвовать в гражданском обороте, иметь самостоятельное имущество, самостоятельно отвечать по своим обязательствам, приобретать и осуществлять гражданские права и обязанности от своего имени, выступать в качестве участника гражданского процесса<sup>12</sup>.

Исследовательский центр проблем регулирования робототехники и искусственного интеллекта «Робоправо» с целью выявления основных проблем, которые могут возникнуть в обществе и правовой системе в связи с активным развитием киберфизических систем, обобщил основные правила робототехники и определил возможные направления решения существующих и ожидаемых проблем. Указанные исследования нашли отражение в подготовленном проекте конвенции по робототехнике и искусственному интеллекту. Проект в качестве объектов робототехники рассматривает все категории роботов, независимо от назначения, опасности, мобильности или автономности, и киберфизические системы с любой формой искусственного интеллекта<sup>13</sup>.

Несмотря на подобные кардинальные, по сути, предложения о решении правовых проблем робототехники, современная юридическая доктрина в основном рассматривает искусственный интеллект и роботы как объекты права, объекты *sui generis*<sup>14</sup>.

<sup>10</sup> Алексеев Н. Н. Основы философии права. СПб., 1998. С. 131—134.

<sup>11</sup> European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) // URL: [https://www.europarl.europa.eu/doceo/document/ta-8-2017-0051\\_en.html](https://www.europarl.europa.eu/doceo/document/ta-8-2017-0051_en.html) (дата обращения: 10 января 2023 г.).

<sup>12</sup> URL: [https://robopravo.ru/proiektu\\_aktov](https://robopravo.ru/proiektu_aktov) (дата обращения: 10 января 2023 г.).

<sup>13</sup> Проект модельной конвенции по робототехнике и искусственному интеллекту. Правила создания и использования роботов и искусственного интеллекта (авторы: А. Незнамов, В. Наумов) // URL: [http://robopravo.ru/modielnaia\\_konvientsiia](http://robopravo.ru/modielnaia_konvientsiia) (дата обращения: 10 января 2023 г.).

<sup>14</sup> Минбалева А. В. Механизмы регулирования использования искусственного интеллекта // Право цифровой среды : монография / под ред. Т. П. Подшивалова, Е. В. Титовой, Е. А. Громовой. М., 2022. С. 699—710.

Так, 10 октября 2019 г. Президентом РФ был издан Указ «О развитии искусственного интеллекта в Российской Федерации», которым была утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 года. Стратегия вводит понятие искусственного интеллекта как «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру... программное обеспечение (в том числе то, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений»<sup>15</sup>.

При этом Стратегия вводит понятие «сильный искусственный интеллект» для систем общего назначения с интеллектом, сопоставимым с интеллектом человека и способных имитировать разумное поведение человека<sup>16</sup>, что оставляет актуальными вопросы о его правовой определенности.

Так, В. В. Архипов и В. Б. Наумов анализируют возможность применения к искусственному интеллекту статуса юридического лица<sup>17</sup>. А. А. Иванов отмечает возможность возникновения двойственного статуса искусственного интеллекта, поскольку он сможет быть как объектом, так и субъектом гражданского права<sup>18</sup>. Также высказывается мнение, что к искусственному интеллекту применимо правило, используемое еще в римском праве — *servi res sunt* (рабы — вещи). С этой точки зрения искусственный интеллект не может быть самостоятельным субъектом права, но он может приобретать права и обязанности для своего хозяина<sup>19</sup>.

О. А. Ястребов, следуя «чистому учению о праве» Г. Кельзена, вводит в российской правовой науке понятие электронного лица, которое предлагает трактовать как персонифицированное единство норм права, которые обязывают и уполномочивают искусственный интеллект (электронный индивид), обладающий критериями «разумности»<sup>20</sup>.

<sup>15</sup> Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года) // СЗ РФ. 2019. № 41. Ст. 5700.

<sup>16</sup> Искусственный интеллект // URL: <https://www.merriam-webster.com/dictionary/artificial%20intelligence> (дата обращения: 10 января 2023 г.).

<sup>17</sup> Архипов В. В., Наумов В. Б. Искусственный интеллект и автономные устройства в контексте права: о разработке первого в России закона о робототехнике // Труды СПИИ РАН. 2017. Вып. 6 (55). С. 46—62.

<sup>18</sup> Иванов А. А. Мечтают ли андроиды об электроовцах? // URL: [zakon.ru/blog/2017/2/15/mechtajut\\_li\\_androidy\\_ob\\_elektroovcakh](http://zakon.ru/blog/2017/2/15/mechtajut_li_androidy_ob_elektroovcakh) (дата обращения: 10 января 2023 г.).

<sup>19</sup> E-commerce и взаимосвязанные области (правовое регулирование) : сборник статей / Е. А. Останина, Л. В. Кузнецова, Е. С. Хохлов [и др.] ; рук. авт. кол. и отв. ред. М. А. Рожкова. М. : Статут, 2019. С. 407.

<sup>20</sup> Ястребов О. А. Правосубъектность электронного лица: теоретико-методологические подходы // Труды Института государства и права Российской академии наук. 2018. Т. 13. № 2. С. 36—55.



П. М. Морхат определяет электронное лицо как «обладающий некоторыми признаками юридической фикции (по аналогии с юридическим лицом) формализованный технико-юридический образ, отражающий модальную фреймизацию и детерминирующий в юридическом пространстве специфическую правосубъектность персонифицированного юнита искусственного интеллекта, обособленную от человеческого субстрата и гетерогенную (в части комплексов прав и обязанностей юнита) в зависимости от функционально-целевого назначения и возможностей такого юнита, и в силу этого аппроксимированный к конкретному целеполаганию производства и задействования такого юнита, то есть его функционально-целевому назначению»<sup>21</sup>.

Однако, вводя в оборот понятие электронного лица, все исследователи отмечают особенности его правосубъектности — невозможность обладания им всеми признаками субъекта права. Если практика также идет по пути наделения указанных лиц субъективными правами и обязанностями, то такая важная составляющая правосубъектности, как возможность нести юридическую ответственность, отсутствует для электронных лиц.

Применительно к системам искусственного интеллекта вопрос об ответственности впервые широко поднимался в резолюции Европарламента от 16 февраля 2017 г., где указывается, что искусственный интеллект не может нести ответственность, поскольку его действия или бездействие зависят от оператора (владельца) или производителя. Однако в резолюции также отмечается, что, чем выше автономность искусственного интеллекта, тем меньше он может расцениваться как обычный инструмент.

В распоряжении Правительства РФ от 19 августа 2020 г. № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» отмечено, что наиболее значимыми вопросами применения систем искусственного интеллекта и робототехники в контексте гражданско-правовых отношений являются вопросы гражданско-правовой ответственности за вред, причиненный системами искусственного интеллекта и робототехники. Реальный уровень развития технологий искусственного интеллекта и робототехники не предполагает кардинальных изменений в регулировании института юридической ответственности, однако требует постепенной доработки его отдельных элементов<sup>22</sup>.

В этой связи требуется дальнейшая проработка механизмов гражданско-правовой, уголовной и административной ответственности в случае причинения вреда системами искусственного интеллекта и робототехники, имеющими высокую степень автономности, при принятии ими решений, в том числе с точки зрения определения лиц, которые будут нести ответственность за их действия, доработки при необходимости механизмов безвиновной гражданско-правовой ответственности, а также возможности использования способов, позволяющих возместить причиненный действиями систем искусственного интеллекта и

<sup>21</sup> Морхат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы : дис. ... д-ра юрид. наук. М., 2018. С. 30—31.

<sup>22</sup> СЗ РФ. 2020. № 35. Ст. 5593.

робототехники вред (например, страхование ответственности, создание компенсационных фондов и др.)<sup>23</sup>.

Такие особенности электронных лиц, как отсутствие воли в правовом смысле, отсутствие собственных интересов, неспособность формировать субъективное отношение к совершаемым деяниям и нести юридическую ответственность по причине отсутствия чувства вины, позволяют нам рассматривать указанные лица как квазисубъекты права.

Наконец, необходимо выделить еще одну категорию лиц, не обладающую правосубъектностью, чьи интересы и ценности, однако, реализуются в киберпространстве через правосубъектность других субъектов — *будущие поколения*.

В настоящий момент исследование данного правового феномена осуществляется преимущественно специалистами в области конституционного права<sup>24</sup>. Это обусловлено тем, что понятие «будущие поколения» содержится в преамбуле Конституции РФ и используется в контексте определения ответственности народа Российской Федерации за свою Родину. В этой связи есть все основания рассматривать будущие поколения как квазисубъект права, так как их интересы входят в сферу правовых ценностей. Последние должны рассматриваться в рамках концепции ответственности перед будущими поколениями в качестве конституционно-правового императива регулирования реализации права на информацию и отношений, складывающихся в киберпространстве в области ее охраны<sup>25</sup>.

Так, проблемой современного общества стало намеренное распространение ложных (фейковых) новостей в социальных медиа в виртуальной среде и традиционных средствах массовой информации с целью введения в заблуждение и получения определенной финансовой или политической выгоды. В современных условиях недостоверная информация становится эффективным и действенным оружием. «Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности»<sup>26</sup>.

Все острее встает проблема пересмотра истории и искажения понимания и значения многих важных дат российской истории, особенно исторических событий Великой Отечественной войны. «Эта проблема не может быть отнесена к числу сугубо научных, связанных с поиском исторической истины, так как в зависимости от трактовки многих событий по-разному может выстраиваться понимание

<sup>23</sup> Щитова А. А. Правовое регулирование информационных отношений по использованию систем искусственного интеллекта : дис. ... канд. юрид. наук. М., 2022. С. 184—185.

<sup>24</sup> Зорькин В. Д. Правовое будущее России // Журнал российского права. 2011. № 10. С. 7—16.

<sup>25</sup> Чубукова С. Г. Принцип ответственности перед будущими поколениями в информационном праве // Аграрное и земельное право. 2018. № 11. С. 134—137.

<sup>26</sup> Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

современной России, повышаться или понижаться уровень патриотизма среди подрастающего поколения»<sup>27</sup>.

Известный российский философ Александр Зиновьев предупреждал о том, что «впереди у России, пожалуй, самый страшный этап агрессии со стороны Запада, который связан с искажением роли русских, занижением их вклада в историю человечества и исключением из человеческой памяти всех следов пребывания великого русского народа»<sup>28</sup>.

Решение этих вопросов определит будущее российского народа. Очевидно, что интересы и возможности будущих поколений являются отражением интересов и возможностей нынешнего поколения, а реализация права на достоверную информацию, обеспечение надежности и сохранности информационных ресурсов будет определять способность будущих поколений жить и развиваться.

Интересы будущих поколений нашли отражение в новой Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы<sup>29</sup>. В ней речь идет уже не о построении информационного общества, а о формировании информационного пространства, основанного на знаниях. Целями информационного пространства знаний являются обеспечение прав граждан на объективную, достоверную, безопасную информацию и создание условий для удовлетворения их потребностей в постоянном развитии, получении качественных и достоверных сведений, новых компетенций, расширении кругозора.

Таким образом, в современном информационном обществе такие вопросы, как развитие цифровых информационных ресурсов, сохранение и получение достоверной информации, обеспечение информационной безопасности, напрямую связаны не только с интересами существующих субъектов информационной деятельности, но и с интересами будущих поколений.

На основе проведенного анализа можно сделать вывод о том, что система субъектов киберправа находится в процессе постоянного развития, обусловленного появлением новых цифровых технологий.

Актуальной теоретической проблемой является развитие теории квазисубъектов в праве и определение правового статуса электронного лица как квазисубъекта права.

На основе объема правовых характеристик в киберпространстве можно выделить такие виды квазисубъектов, как лица:

- наделенные субъективными правами и обязанностями, но не несущие ответственность (интеллектуальные агенты, киберфизические системы, системы искусственного интеллекта, роботы);
- не обладающие правосубъектностью, но реализующие свои интересы через интересы субъектов права, как правило, в качестве конституционно-правового императива (будущие поколения).

<sup>27</sup> Чарыков Д. В., Бугас О. Д. Фальсификация истории Великой Отечественной войны как научная и социальная проблема // Военно-исторический журнал. 2019. № 2.

<sup>28</sup> Зиновьев А. А. Русская трагедия (Гибель утопии). М., 2002. С. 60.

<sup>29</sup> Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

**БИБЛИОГРАФИЯ**

1. *Алексеев Н. Н.* Основы философии права. — СПб., 1998. — 215 с.
2. *Архипов В. В., Наумов В. Б.* Искусственный интеллект и автономные устройства в контексте права: о разработке первого в России закона о робототехнике // Труды СПИИ РАН. — 2017. — Вып. 6 (55). — С. 46—62.
3. *Венгеров А. Б.* Теория государства и права : учебник — 2-е изд. — М. : Омега-Л, 2005. — 608 с.
4. *Долинская В. В.* Проблемы квазисубъектных образований в частном праве // Правосубъектность: общетеоретический, отраслевой и международно-правовой анализ : сборник материалов к XII Ежегодным научным чтениям памяти профессора С. Н. Братуся. — М. : Статут, 2017. — С. 315—324.
5. Е-commerce и взаимосвязанные области (правовое регулирование) : сборник статей / Е. А. Останина, Л. В. Кузнецова, Е. С. Хохлов [и др.] ; рук. авт. кол. и отв. ред. М. А. Рожкова. — М. : Статут, 2019. — 448 с.
6. *Зиновьев А. А.* Русская трагедия (Гибель утопии). — М., 2002. — 95 с.
7. *Зорькин В. Д.* Правовое будущее России // Журнал российского права. — 2011. — № 10. — С. 7—16.
8. *Лукичев П. Н., Скорик А. П.* Квазигосударственность // Полис. — 2001. — № 2. — С. 139—142.
9. *Минбалеев А. В.* Механизмы регулирования использования искусственного интеллекта // Право цифровой среды : монография / под ред. Т. П. Подшивалова, Е. В. Титовой, Е. А. Громовой. — М., 2022. — С. 699—710.
10. *Морхат П. М.* Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы : дис. ... д-ра юрид. наук. — М., 2018. — 420 с.
11. *Петражицкий Л. И.* Теория права и государства в связи с теорией нравственности. — СПб., 2000. — 606 с.
12. *Пономарева Е. В.* Субъекты и квазисубъекты права: теоретико-правовые проблемы разграничения : дис. ... канд. юрид. наук. — Екатеринбург, 2019. — 208 с.
13. *Черниченко С. В.* Контуры международного права. Общие вопросы. — М., 2014. — 592 с.
14. *Чубукова С. Г.* Принцип ответственности перед будущими поколениями в информационном праве // Аграрное и земельное право. — 2018. — № 11. — С. 134—137.
15. *Щитова А. А.* Правовое регулирование информационных отношений по использованию систем искусственного интеллекта : дис. ... канд. юрид. наук. — М., 2022. — 225 с.
16. *Ястребов О. А.* Правосубъектность электронного лица: теоретико-методологические подходы // Труды Института государства и права Российской академии наук. — 2018. — Т. 13. — № 2. — С. 36—55.





**Анна Валерьевна  
ЯКОВЛЕВА,**

профессор кафедры  
экономической теории  
и экономического  
образования  
Российского  
государственного  
педагогического  
университета имени  
А. И. Герцена,  
доктор экономических наук,  
доцент  
[yeif@mail.ru](mailto:yeif@mail.ru)  
191186, Россия,  
г. Санкт-Петербург, Реки  
Мойки наб., д. 48

## Проблемы правового обеспечения в становлении института кибергигиены

**Аннотация.** Киберпространство, кибермир или виртуальный мир стали неизбежной реальностью жизни современного общества. Период пандемии COVID-19 еще более активизировал отношения граждан с киберпространством, что, в свою очередь, ведет к росту киберпреступлений в современном виртуальном мире. Поэтому для защиты своего информационного пространства каждому пользователю, в самом широком смысле этого термина, стало необходимо применять безопасные методы при использовании Интернета. Совокупность этих мер безопасности получила название «кибергигиена».

Данная статья посвящена проблемам правового обеспечения развивающегося института кибергигиены, который на современном этапе играет решающую роль в защите не только информационной инфраструктуры современного бизнеса, но и данных отдельных пользователей. Автор акцентирует внимание на том, что в данный период еще не сформировался понятийный аппарат правового обеспечения в практике информационных отношений в сфере кибергигиены. При этом подчеркиваются важность и необходимость становления и развития данного института на основе анализа растущих киберпреступлений, свидетельствующих о пока еще слабом уровне кибергигиены.

**Ключевые слова:** кибергигиена; информационная безопасность; кибербезопасность; киберпреступления; институт кибергигиены.

DOI: 10.17803/2311-5998.2023.102.2.062-070

**ANNA V. IAKOVLEVA,**

Professor of the Department of economic theory and economic education  
of the Herzen Russian State Pedagogical University,  
Dr. Sci. (Economics), Associate Professor  
[yeif@mail.ru](mailto:yeif@mail.ru)

48, Reki Mojki naberezhnaya, Saint Petersburg, Russia, 191186

### Problems of Legal Support of the Cyber Hygiene Institute

**Abstract.** Cyberspace, cyberworld or the virtual world has become an inevitable reality of the modern society life. The period of the COVID 19 pandemic has further intensified the relationship between citizens and cyberspace, which in turn leads to an increase in cybercrime in the modern virtual world. Therefore, it has become necessary for each user, taken in the broadest sense of the term, to use secure methods when navigating the Internet in order to protect their own information space. The combination of these security measures is called “cyber hygiene”.

*This article is devoted to the problems of legal support for the developing concept of “cyber hygiene”, which at present plays a decisive role in protecting, not only the information infrastructure of modern business, but also the data of individual users. The author focuses on the fact that, currently, the conceptual apparatus of legal support in the practice of information relations in the field of cyber hygiene has not yet been formed. At the same time, the importance and necessity of the formation and development of this legal concept is emphasized on the basis of an analysis of growing cybercrimes, indicating a still insufficient level of cyber hygiene.*

**Keywords:** *cyber hygiene; information security; cybersecurity; cybercrime; institute of cyber hygiene.*

Каждое крупное нарушение в сфере информационной безопасности, кибербезопасности заставляет экспертов по безопасности со всего мира говорить о необходимости улучшения и продвижения кибергигиены. Доказательством тому служат достаточно известные инциденты последнего времени с далеко идущими последствиями. В частности, 6 ноября 2022 г. пользователь известного форума хакеров опубликовал CSV-файл объемом 60 ГБ, содержащий неанонимную личную информацию, включая 257 829 454 записи о 228 миллионах пользователей Deezer (французский интернет-сервис потоковой передачи музыки).

Согласно анализу выборки данных, раскрытая конфиденциальная информация, затронувшая миллионы людей из таких стран, как США, Великобритания, Франция, Германия, Бразилия, Мексика, Италия, Турция, Колумбия, Гватемала, включала адреса электронной почты, имена и фамилии пользователей, даты рождения, пол, данные о местоположении, включая город и страну, идентификатор пользователя и дату регистрации. Нужно сказать, что указанная утечка данных произошла еще в 2019 г.

В январе 2022 г. благотворительная организация Красный Крест подверглась компьютерной атаке, в результате которой было скомпрометировано более 500 тысяч записей: преступники похитили информацию о «крайне уязвимых лицах» (как правило, это жертвы войны и возможные свидетели). Подобная информация в последующем может быть продана международным преступным группировкам, которые часто преследуют этих людей.

В 2017 г. произошла атака программ-вымогателей, которая началась с уничтожения данных из компьютерных сетей Национальной системы здравоохранения Великобритании (NHS), а затем распространилась на компьютерные сети более чем в 100 странах мира. 2016 год печально известен взломом серверов Национального комитета Демократической партии во время президентских выборов в США. В 2015 г. было похищено 21,5 миллиона высокой степени секретных записей о текущих и бывших чиновниках федерального правительства США<sup>1</sup>. Этот список с каждым годом продолжает пополняться все новыми инцидентами.

<sup>1</sup> См.: Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J. Cyber hygiene: The concept, its measure, and its initial tests // Decision Support Systems. Vol. 128. January, 2020. URL: <https://www.sciencedirect.com/science/article/abs/pii/S0167923619301897> (дата



К улучшению кибергигиены призывают не только эксперты по безопасности, но и политики и правительства почти всех стран. Например, в ответ на отчет Управления правительственной отчетности США (GAO), подробно описывающий продолжающееся использование Adobe Flash на компьютерах федерального правительства в июне 2018 г., сенатор-демократ Уайден написал письмо, в котором порицал Агентство национальной безопасности (АНБ), Министерство внутренней безопасности (DHS) и Белый дом за их неспособность применять меры по кибергигиене. Аналогичная критика за недостаточные усилия для обеспечения мер по кибергигиене также была высказана против президента Обамы и его команды<sup>2</sup>.

Несмотря на то, что многие эксперты сетуют на недостаточный уровень кибергигиены, неясно, что действительно значит сам термин «кибергигиена». Следует согласиться с авторами, которые отмечают, что фактически нет ни одной академической исследовательской статьи, в которой объяснялось бы это понятие или шла бы речь о ее измерении. Путаница усугубляется еще и тем, что, например, поисковая система Google выдает сотни веб-страниц, созданных блогерами, ИТ-компаниями, и различными экспертами по кибербезопасности, предлагающими всевозможные меры — от очевидных (например, лучше защищать свою электронную почту) до очень специфических (как, например, рекомендация использовать определенную операционную систему или антивирусное программное обеспечение).

Советы из Интернета также включают в себя широкий спектр подходов. Некоторые призывают к усилению бдительности, другие — к повышенной информированности, а третьи советуют пользователям полностью изменить свое поведение (например, звонить в банк по телефону вместо того, чтобы отвечать на любые письма от них).

Еще большую путаницу вносят противоречащие друг другу рекомендации от разных организаций. Например, Национальный институт стандартов и технологий (NIST) в 2018 г. опубликовал руководство, в котором речь шла о кибергигиене в контексте практики управления исправлениями в ИТ<sup>3</sup>; Европейский союз в 2018 г. представил серию общеевропейских инициатив под названием #SaferInternet4EU, охватывающих широкий круг тем, в том числе улучшения кибергигиены среди детей<sup>4</sup>.

Валютное управление Сингапура (MAS) в 2018 г. выпустило консультационный документ «Уведомление о кибергигиене», содержащий набор основных практик

---

обращения: 01.04.2022) ; Яковлева А. В. Проблемы правового регулирования информационной безопасности в условиях развития цифровой экономики. Саратов : Амирит, 2021. 272 с.

<sup>2</sup> Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J. Op. cit.

<sup>3</sup> Critical Cybersecurity Hygiene: Patching the Enterprise. August 31, 2018 // URL: <https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/ch-pe-project-description-draft.pdf> (дата обращения: 14.03.2022).

<sup>4</sup> См.: #SaferInternet4EU campaign // URL: <https://www.betterinternetforkids.eu/en-GB/saferinternet4eu> (дата обращения: 14.03.2022) ; Building a safer and better digital space for children in the EU — Brochure // URL: <https://digital-strategy.ec.europa.eu/en/library/building-safer-and-better-digital-space-children-eu-brochure> (дата обращения: 14.03.2022).

кибербезопасности, которые должны внедрить финансовые учреждения с целью управления киберугрозами. К таким практикам относятся: своевременное устранение недостатков безопасности системы; установка и реализация надежной безопасности системы; обеспечение безопасности системных подключений; установка антивирусного программного обеспечения; ограничение использования учетных записей системного администратора, которые могут изменять конфигурацию системы; усиление аутентификации пользователей.

В целом можно говорить о том, что MAS включило в понятие «кибергигиена» многофакторную аутентификацию, использование межсетевых экранов и антивирусные программы. Важно подчеркнуть, что MAS предлагает вышеперечисленные меры предусмотреть в качестве базового стандарта гигиены для кибербезопасности, превратив их в юридически обязательные требования<sup>5</sup>.

Следует отдельно отметить Директиву ЕС 2022/2055 Европейского Парламента и Совета от 14.12.2022 «О мерах по обеспечению высокого общего уровня кибербезопасности в Союзе, внесении изменений в Регламент (ЕС) № 910/2014 и Директиву (ЕС) 2018/1972, а также об отмене Директивы (ЕС) 2016/1148 (Директива NIS 2)», в которой указано, что политика продвижения кибергигиены обеспечивает основу для защиты инфраструктур сетей и информационных систем, оборудования, программного обеспечения и безопасности онлайн-приложений, а также данных бизнеса или конечных пользователей, на которые полагаются организации.

Данная политика включает общий базовый набор методов, таких как обновление программного и аппаратного обеспечения, смена паролей, управление новыми установками, ограничение доступа на уровне администратора и резервное копирование данных; упреждающую основу для обеспечения готовности и общую безопасность и защищенность в случае инцидента или киберугрозы.

В документе указано, что Европейское агентство сетевой и информационной безопасности (ENISA) будет отслеживать и анализировать политику государств-членов в области кибергигиены. Далее в тексте документа подчеркивается, что осведомленность о кибербезопасности и кибергигиене необходима для повышения уровня кибербезопасности в Союзе, в частности в свете растущего числа подключенных к сети устройств, которые все чаще используются в кибератаках. В связи с этим следует предпринять усилия для повышения общей осведомленности о рисках, связанных с такими устройствами, как на внутреннем так и на внешнем рынке.

Основные и важные организации должны использовать широкий спектр определяющих методов кибергигиены, таких как принципы нулевого уровня слепого доверия, обновление программного обеспечения, конфигурация устройств, сегментация сети, управление идентификацией и доступом или осведомленность

<sup>5</sup> См.: MAS consults on draft Notice on Cyber Hygiene for financial institution. 27 September, 2018 // URL: <https://www.allenandgledhill.com/sg/publication/articles/7505/mas-consults-on-draft-notice-on-cyber-hygiene-for-financial-institutions> (дата обращения: 14.03.2022) ; Consultation Paper on Notice on Cyber Hygiene. 03 September, 2018 // URL: <https://www.mas.gov.sg/publications/consultations/2018/consultation-paper-on-notice-on-cyber-hygiene> (дата обращения: 14.03.2022).

пользователей, организовать обучение своего персонала и повышать осведомленность о киберугрозах, фишинге или методах социальной инженерии.

Кроме того, организации должны оценивать свои собственные возможности кибербезопасности и при необходимости стремиться к интеграции технологий повышения кибербезопасности, таких как искусственный интеллект или системы машинного обучения, для расширения своих возможностей и безопасности сетей и информационных систем.

Данной Директивой вменяется в обязанность государствам — членам ЕС осуществлять продвижение и развитие образования и обучения по кибербезопасности, а также руководство по передовым методам и средствам контроля кибергиены, предназначенным для граждан, заинтересованных сторон и организаций<sup>6</sup>.

Из всего вышеизложенного становится ясно, что кибергиена не является единичным действием, а включает комплекс разнообразных мер: от эффективного управления исправлениями до отказа от использования определенных типов программного обеспечения, а также от резервного копирования файлов компьютеров до избежания кибертравли и определения ложных новостей. И этот комплекс мер должен быть применим к различным субъектам: от организаций гражданского общества и ИТ-менеджеров до обычных пользователей Интернета, детей и даже президента.

На практике мы наблюдаем, что каждый раз предлагаются разные меры, и пользователям не всегда понятны их значение и важность. Кроме того, такое расплывчатое определение столь важного понятия, как «кибергиена» и не всегда проверенные предлагаемые меры мало помогают повышению киберустойчивости, тем самым сбивая с толку и ИТ-менеджеров, и конечных пользователей, предлагая противоречивые советы, которые еще больше ослабляют нашу способность защитить киберпространство. Если мы когда-либо надеемся достичь кибер-устойчивости, нам необходимо четко объяснить, что такое кибергиена и почему она так важна<sup>7</sup>.

Известно, что первым употребил термин «кибергиена» старший вице-президент по интернет-архитектуре и технологиям MCI WorldCom Винтон Г. Серф в своем заявлении для объединенного экономического комитета 23 февраля в 2000 г.. Он сказал: «Я считаю, что сам Интернет по большей части безопасен, хотя есть шаги, которые, как мы знаем, можно предпринять для повышения безопасности и устойчивости. Большинство уязвимостей исходит от тех, кто использует Интернет (компании, правительства, академические учреждения и отдельные лица), но не соблюдает то, что я называю хорошей кибергиеной. Они недостаточно чувствительны к необходимости защиты безопасности интернет-сообщества,

<sup>6</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) // URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> (дата обращения: 14.01.2023).

<sup>7</sup> Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J. Op. cit.

частью которого они являются. Когда дело касается безопасности, открытость Интернета — это одновременно его благословение и проклятие»<sup>8</sup>.

В английской Энциклопедии законодательства по информационным технологиям (The IT Law Wiki) «кибергигиена» определяется как шаги, которые пользователи компьютеров могут предпринять для повышения своей кибербезопасности и лучшей защиты в Интернете. Это может включать реорганизацию ИТ-инфраструктуры, оборудования и устройств; использование патчей для лицензионного программного обеспечения и удаление нелегального программного обеспечения; постоянный мониторинг, обучение и осведомленность; а также формализацию существующих неформальных мер контроля информационной безопасности<sup>9</sup>.

Агентство Европейского союза по сетевой и информационной безопасности (ENISA) отмечает, что кибергигиена должна рассматриваться так же, как и личная гигиена, и после правильной интеграции в организацию это будут простые повседневные распорядки, правильное поведение и периодические проверки, чтобы убедиться, что онлайн-здоровье организации находится на высоте. Кибергигиена включает оборудование, программное обеспечение, ИТ-инфраструктуру, обучение информированности о кибербезопасности и собственные устройства сотрудников компании<sup>10</sup>.

В китайском источнике «Что такое кибергигиена? Почему она важна?» о кибергигиене говорится как о шагах, предпринимаемых пользователями компьютеров для защиты своего оборудования и поддержания его в наилучшем состоянии: «Так же, как вы следуете определенным гигиеническим привычкам, чтобы оставаться здоровым, компьютерная сеть, которую вы используете, также должна быть в порядке. Кибергигиена означает проверку того, соответствует ли сеть, используемая вашей компанией, надлежащим требованиям, чтобы у киберпреступников (хакеров) было меньше возможностей взлома и контроля». Другими словами, термин «кибергигиена» означает обеспечение безопасности и актуализации вашего компьютера и сети, что затрудняет доступ хакеров к ним<sup>11</sup>.

В индийском Интернете (англо- и хиндиязычном) четкое определение термина «кибергигиена» отсутствует. Чаще всего индийский Google при соответствующем запросе выводит на страницу Лаборатории Касперского с разделами «Cyber hygiene definition» и «What is cyber hygiene?». Несмотря на то, что страница эта создана специально для Индии, ее содержание полностью совпадает с содержанием других англоязычных страниц Лаборатории (для Великобритании, США и Австралии). На странице Министерства электроники и ИТ Индии также

<sup>8</sup> Statement of Dr. Vinton G. Cerf Senior Vice President of Internet Architecture & Technology MCI WorldCom For the Joint Economic Committee February 23, 2000 // URL: <https://www.jec.senate.gov/archive/Documents/Hearings/cerf22300.htm> (дата обращения: 15.04.2022).

<sup>9</sup> The IT Law Wiki // URL: [https://itlaw.wikia.org/wiki/Cyber\\_hygiene](https://itlaw.wikia.org/wiki/Cyber_hygiene) (дата обращения: 15.04.2021).

<sup>10</sup> ¿Qué es la higiene cibernética y por qué es importante? // URL: [https://ciberseguridad.com/guias/higiene-cibernetica/#%c2%bfque\\_es\\_la\\_higiene\\_cibernetica](https://ciberseguridad.com/guias/higiene-cibernetica/#%c2%bfque_es_la_higiene_cibernetica) (дата обращения: 15.04.2021).

<sup>11</sup> 什么是网络卫生？为什么重要？ // URL: <https://zh.anipi.org/maintain-cyber-hygiene-4980#menu-1> (дата обращения: 15.04.2021).



нет четкого определения этого термина, хотя он представлен в Общем онлайн-курсе по кибербезопасности, целью которого является прежде всего обучение практическим навыкам кибергигиены. В целом складывается впечатление, что там отсутствует разграничение понятий «кибергигиена» и «кибербезопасность», они оказываются взаимозаменяемыми<sup>12</sup>.

Что касается позиции отечественных авторов в отношении термина «кибергигиена», то под ней понимается: соблюдение элементарных основ цифровой безопасности при работе с сетью Интернет (С. Кузнецов)<sup>13</sup>. Такой же точки зрения придерживается Е. В. Сафронов, с той лишь оговоркой, что это должно происходить на уровне повседневной привычки<sup>14</sup>. В. Минин отмечает, что главное — соблюдать информационную гигиену и профилактику. Нужны внимание и самоконтроль, а также корпоративное обучение со стороны руководителей ИТ- и ИБ-служб<sup>15</sup>.

А. А. Козырева в своем исследовании предприняла попытку определить понятие «кибергигиена», с учетом возможности его применения в правовом поле, как «систематическое применение технических мер предосторожности, предпринимаемых пользователями с целью обеспечения конфиденциальности личной информации, безопасности и безопасности конфиденциальных данных от преступлений с применением современных ИКТ».

Таким образом, исследователи определяют термин «кибергигиена» через шаги, которые компьютерные пользователи могут предпринять, чтобы улучшить личную кибербезопасность и лучше защитить себя в Интернете. Следует не согласиться с авторами, указывающими на то, что «безусловно, закрепление ответственности за неприменение кибергигиены на законодательном уровне не является необходимым, так как это является личным делом каждого пользователя». При этом, отмечается, что именно внедрение «кибергигиенических» привычек может позволить минимизировать объем преступлений, совершаемых с применением ИКТ<sup>16</sup>.

Мы считаем, что в век стремительного развития ИКТ и появления новых угроз соблюдение определенных «кибергигиенических» мер становится обязательным и требует закрепления ответственности за неприменение указанных мер на законодательном уровне, так как, по нашему мнению, просто прививать культуру «кибергигиены» недостаточно.

В поддержку данного тезиса необходимо привести следующие аргументы. Так, по данным Центра рассмотрения жалоб на интернет-преступления (IC3) ФБР

<sup>12</sup> Government of India. Ministry of Electronics and Information Technology (MeitY) presents «Generic Online Training Course in Cyber Security» // URL: <https://www.infosecawareness.in/cybhyg> (дата обращения: 14.12.2022).

<sup>13</sup> Кузнецов С. Кибергигиена — личное дело? // URL: <https://iz.ru/news/670025> (дата обращения: 14.03.2022).

<sup>14</sup> Сафронов Е. В. Азы кибергигиены: Методологические и правовые аспекты. М. : Проспект, 2018. С. 25.

<sup>15</sup> Козырева А. А. Определение термина «кибергигиена» и возможность его применения в правовом поле // Проблемы в российском законодательстве. 2018. № 7. С. 92—94.

<sup>16</sup> Козырева А. А. Указ. соч. С. 92—94.

(США) за 2021 г. им было получено рекордное количество жалоб от американской общественности: количество принятых жалоб составило 847 376, что на 7 % больше, чем в 2020 г., были заявлены потери, превышающие 6,9 миллиарда долларов.

Преступления, связанные с компрометацией корпоративной деловой электронной почты (ВЕС) и преступное использование криптовалюты по-прежнему отнимают больше всего денег: по 19 954 жалобам был заявлен общий убыток примерно в 2,4 миллиарда долларов, что на 33 % больше, чем в 2020 г. (1,8 миллиарда долларов).

Распространено также мошенничество с «выуживанием» информации (фишингом, вишингом, смишингом, фармингом): 323 972 жалобы, по которым был заявлен общий убыток в размере более 44 миллионов долларов. Количество инцидентов с программами-вымогателями также продолжает расти: в 2021 г. было зарегистрировано 3 729 247 таких инцидентов, по сравнению с 2020 г. этот показатель вырос на 51%<sup>17</sup>. Безусловно, это далеко не все преступления, которые представлены в указанном отчете. И, как мы можем отметить, сомнений не вызывает тот факт, что слабая кибергигиена обходится обществу дорого.

Таким образом, несмотря на то, что термин «кибергигиена» используется достаточно широко, на сегодняшний день он не имеет официальной трактовки, поскольку не закреплен на законодательном уровне. Отмечается, что в национальном законодательстве «кибер» как часть сложных слов не используется. В Доктрине информационной безопасности 2016 г.<sup>18</sup> закрепляется термин «информационная безопасность», что гораздо шире по своему значению, чем «кибербезопасность».

Тем не менее предполагается, что закрепление термина «кибергигиена» (который является неотъемлемой составляющей «кибербезопасности» или в широком смысле «информационной безопасности») в нормативных правовых документах будет способствовать применению и прививанию навыков личной информационной безопасности и осознанной ответственности пользователей информационно-коммуникационной сети Интернет.

В качестве основной задачи кибергигиены выделяется соблюдение технических мер предупреждения возможных преступлений, совершаемых с использованием современных ИКТ, лично каждым пользователем<sup>19</sup>. И в этой связи на первоначальном этапе встает вопрос о разработке стандартов кибергигиены в сфере информационной безопасности (кибербезопасности) и реализации их как юридически обязательных требований, а в дальнейшем — о развитии института кибергигиены в России.

Важно отметить, что 1 августа 2022 г. в России в рамках федерального проекта «Информационная безопасность» национальной программы «Цифровая

<sup>17</sup> См.: Internet Crime Report 2020 // URL: [https://www.ic3.gov/media/pdf/annualreport/2020\\_ic3report.pdf](https://www.ic3.gov/media/pdf/annualreport/2020_ic3report.pdf) (дата обращения: 16.05.2022) ; Internet Crime Report 2021 // URL: [https://www.ic3.gov/media/pdf/annualreport/2021\\_ic3report.pdf](https://www.ic3.gov/media/pdf/annualreport/2021_ic3report.pdf) (дата обращения: 18.04.2022).

<sup>18</sup> Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

<sup>19</sup> Козырева А. А. Указ. соч.

экономика» была запущена трехгодичная всероссийская программа кибергиены (Минцифры России совместно с СПбГУТ имени М. А. Бонч-Бруевича, «Ростелеком-Солар» и АНО «Диалог Регионы»). Отмечается, что ее целью является привлечение внимания к вопросам кибербезопасности и формирование у граждан навыков безопасного поведения в Интернете. При ее реализации планируется повысить информационную безопасность госслужащих, обучить кибергиене детей и подростков, а также провести всероссийский мониторинг уровня осведомленности граждан о базовых принципах кибербезопасности<sup>20</sup>.

### БИБЛИОГРАФИЯ

1. *Козырева А. А.* Определение термина «кибергиена» и возможность его применения в правовом поле // Пробелы в российском законодательстве. — 2018. — № 7. — С. 92—94.
2. *Кузнецов С.* Кибергиена — личное дело? // URL: <https://iz.ru/news/670025> (дата обращения: 14.03.2022).
3. *Сафронов Е. В.* Азы кибергиены: методологические и правовые аспекты. — М. : Проспект, 2018.
4. *Яковлева А. В.* Зрелость нормативно-правовой базы в области кибербезопасности стран Латинской Америки по модели СММ // Проблемы экономики и юридической практики. — 2022. — Т. 18. — № 4. — С. 20—29.
5. *Яковлева А. В.* Проблемы правового регулирования информационной безопасности в условиях развития цифровой экономики. — Саратов : Амирит, 2021. — 272 с.
6. *Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J.* Cyber hygiene: The concept, its measure, and its initial tests // Decision Support Systems. — Vol. 128. — January, 2020. — URL: <https://www.sciencedirect.com/science/article/abs/pii/S0167923619301897> (дата обращения: 01.04.2022).
7. 什么是网络卫生？为什么重要？ // URL: <https://zh.anipi.org/maintain-cyber-hygiene-4980#menu-1> (дата обращения: 15.04.2022).

<sup>20</sup> Минцифры повышает киберграмотность россиян // URL: <https://digital.gov.ru/ru/events/41771/> (дата обращения: 18.12.2022).

## Искусственный интеллект

### Проблемы правовой охраны персональных данных в процессе использования нейронных сетей

***Аннотация.** Развитие высокотехнологичных отраслей экономики во многом обусловлено формированием системного правового регулирования складывающихся отношений в цифровой среде, в том числе отдельных сквозных технологий. Одними из важнейших таких технологий выступает искусственный интеллект и неразрывно связанные с ним нейронные сети. Данная статья посвящена анализу одной из ключевых проблем в сфере использования нейронных сетей — защите персональных данных. Авторы приходят к выводу, что в законодательстве о персональных данных должно быть закреплено, что обработка персональных данных с использованием нейронных сетей должна производиться только при условии письменного согласия субъекта персональных данных. Кроме того, любые изменения персональных данных, произведенные в результате процессов машинного обучения, должны регулярно согласовываться с субъектом персональных данных. Ему должна быть обеспечена возможность ознакомления с обновленными персональными данными.*

***Ключевые слова:** нейронные сети, персональные данные, правовое регулирование, охрана.*

DOI: 10.17803/2311-5998.2023.102.2.071-079



**Алексей Владимирович МИНБАЛЕЕВ,**

заведующий кафедрой  
информационного права  
и цифровых технологий  
Университета имени  
О.Е. Кутафина (МГЮА),  
доктор юридических наук,  
профессор  
[alexmin@bk.ru](mailto:alexmin@bk.ru)  
125993, Россия, г. Москва,  
ул. Садовая-Кудринская, д. 9



**Екатерина Эдуардовна СТОРОЖАКОВА,**

директор бюро переводов  
Translate2u  
[mail@2u.com.ru](mailto:mail@2u.com.ru)  
125993, Россия, г. Москва,  
ул. Садовая-Кудринская, д. 9

**ALEKSEY 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*

**EKATERINA E. STOROZHAKOVA,**

*Director of the translation agency Translate2u*

**mail@2u.com.ru**

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

**Problems of legal protection  
of personal data  
in the process of using neural networks**

**Abstract.** *The development of high-tech sectors of the economy is largely due to the formation of a systematic legal regulation of the emerging relations in the digital environment, including the regulation of certain end-to-end technologies. One of the most important such technologies is artificial intelligence and inextricably linked neural networks. This article is devoted to the analysis of one of the key problems in the use of neural networks — the protection of personal data. The authors conclude that the legislation on personal data should stipulate that the processing of personal data using neural networks should be carried out only with the written consent of the subject of personal data. In addition, any changes to personal data made as a result of machine learning processes must be regularly coordinated with the subject of personal data. He should be provided with the opportunity to get acquainted with the updated personal data.*

**Keywords:** *neural networks, personal data, legal regulation, protection.*

Нейронные сети являются сегодня ключевым инструментом и технологией, направленной на обеспечение использования искусственного интеллекта и машинного обучения. В современном гражданском обороте все чаще возникают вопросы договорного сопровождения использования тех или иных нейронных сетей в процессе функционирования систем искусственного интеллекта. Происходит это чаще всего через различные создаваемые приложения, устанавливаемые клиентами в компьютерных устройствах.

Активно используются и смарт-контракты, с помощью которых автоматически происходит обработка той или иной информации нейронными сетями, например автоматические актуализации по тому или иному запросу на предмет поиска определенного варианта действий на основе произошедших изменений и дополнений в онтологии за счет как поступившей информации, так и произведенного машинного самообучения системой. Обеспечение договорного процесса в сфере услуг, связанных с искусственным интеллектом, облачной платформой и

нейронными сетями, сегодня является весьма актуальным и вызывает на практике много вопросов и проблем<sup>1</sup>.

Сегодня постепенно приходит осознание того, что сами нейронные сети не могут регулироваться в отрыве от технологий искусственного интеллекта. В то же время отдельные аспекты правовой природы нейронных сетей, как и всех сквозных технологий, необходимо учитывать в процессе правотворческой и правоприменительной деятельности<sup>2</sup>. К сожалению, сегодня приходится констатировать, что исследований<sup>3</sup>, посвященных нейронным сетям, ничтожно мало, в то время как тема является очень важной с позиции юридического анализа.

С точки зрения защиты персональных данных при использовании нейронных сетей возникает несколько проблем.

1. Существуют проблемы законности обработки тех или иных персональных данных, которые используются в онтологии или при разработке алгоритма, а также законности использования тех или иных персональных данных при формировании запроса к нейронной сети; обеспечения и защиты прав граждан на персональные данные и их использование. В данном случае в основном используются классические механизмы защиты и, если отсутствует согласие на обработку персональных данных и она осуществляется вне обязательных требований, установленных федеральным законом, то имеется факт нарушения.

Персональные данные могут содержаться как в онтологии системы (по сути, в данном случае мы можем говорить об аналогии с охраной персональных данных в определенной базе данных или информационной системе и прибегать к соответствующим инструментам охраны).

Персональные данные могут содержаться и в самом алгоритме, и эта ситуация гораздо сложнее, поскольку чаще всего в алгоритме заложены косвенные персональные данные. Термин «алгоритм» часто используется для обозначения приложений искусственного интеллекта, например, через такие термины,

<sup>1</sup> Drew Stevens (2018) Neural Networks and Advanced AI Contract Issues // URL: <https://drewstevenslaw.com/neural-networks-and-advanced-ai-contract-issues/> (дата обращения: 10.12.2022).

<sup>2</sup> См.: Право и иные регуляторы в развитии цифровых технологий / А. В. Минбалеев, А. В. Мартынов, Г. Г. Камалова [и др.]. Саратов : Амирит, 2022 ; Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций : колл. монография : в 2 т. / Е. Н. Абанина, О. Ю. Авдеевна, Р. В. Амелин [и др.] Саратов : Саратовская государственная юридическая академия, 2020 ; Информационно-технологическое обеспечение юридической деятельности (LegalTech) : учебник / А. В. Минбалеев, Т. А. Полякова, М. Б. Добробаба [и др.] М. : Проспект, 2023.

<sup>3</sup> См.: *Бойченко И. С.* Модели правового регулирования нейросетей // Образование и право. 2019. № 1. С. 235—237 ; *Он же.* Формирование правового регулирования нейронных сетей // Формирование системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе. Вторые Бачиловские чтения : сборник научных трудов, Москва, 8 февраля 2019 г. М. ; Саратов : Амирит, 2019. С. 218—223 ; *Полякова Т. А., Химченко А. И.* Правовые проблемы обеспечения информационной безопасности при использовании облачных технологий // Правовая информатика. 2013. № 2. С. 12—16.



как «алгоритмическое принятие решений». Однако понятие алгоритма является более общим, чем понятие искусственного интеллекта, поскольку оно включает в себя любую последовательность однозначно определенных инструкций для выполнения задачи, в частности, но не исключительно, с помощью математических вычислений.

Чтобы быть выполняемыми компьютерной системой, алгоритмы должны быть выражены с помощью языков программирования и стать, таким образом, машинно-исполняемыми программами. Алгоритмы могут быть очень простыми, указывая, например, как упорядочивать списки слов в алфавитном порядке или как найти наибольший общий делитель между двумя числами (например, так называемый алгоритм Евклида). Они также могут быть очень сложными, такими как алгоритмы шифрования файлов, сжатия цифровых файлов, распознавания речи или финансового прогнозирования. В данном случае как раз проблема и состоит в том, что персональные данные будут находиться в зашифрованном виде и не доступны простому субъекту персональных данных, который не в состоянии их выявить и проверить.

Очевидно, что не все алгоритмы включают искусственный интеллект, но каждая система искусственного интеллекта, как и любая компьютерная система, включает в себя алгоритмы, часть которых имеет дело с задачами, непосредственно касающимися функций искусственного интеллекта. Алгоритмы искусственного интеллекта могут включать различные виды эпистемологических или практических рассуждений (обнаружение паттернов и формы, применение правил, составление прогнозов или планов), а также различные способы обучения.

Все это может осуществляться с использованием отдельных персональных данных, например, при формировании алгоритмов, связанных с таргетинговой рекламой, основанной на вкусах и предпочтениях потребителей. Причем в большинстве случаев, конечно, персональные данные будут обезличены, но в ряде случаев — нет. Логично, что и нейронная сеть, функционирующая на базе таких алгоритмов, может использовать персональные данные, в том числе нарушая права тех или иных субъектов.

Нейронная сеть, используя данные пользователей, может улучшить себя, разработав новые эвристики (предварительные стратегии решения проблем), модифицируя свои внутренние данные или даже генерируя новые алгоритмы. Например, система искусственного интеллекта для электронной коммерции может предоставлять скидки потребителям, отвечающим определенным условиям (применять правила), предоставлять рекомендации (например, изучать и использовать корреляции между особенностями пользователей и их покупательскими привычками), оптимизировать управление запасами (например, разрабатывать и внедрять лучшие торговые стратегии). При этом, естественно, закладывается необходимость обработки персональных данных потребителей<sup>4</sup>.

<sup>4</sup> Подробнее см.: *Минбалева А. В.* Проблемы социальной эффективности и защиты прав человека при использовании искусственного интеллекта в рамках социального скоринга // Вестник Южно-Уральского государственного университета. Серия : Право. 2020. Т. 20. № 2. С. 96—101.

Хотя система искусственного интеллекта включает в себя множество алгоритмов, ее также можно рассматривать как единый сложный алгоритм, объединяющий алгоритмы, выполняющие ее различные функции, а также верхние алгоритмы, которые управляют функциями системы путем активации соответствующих алгоритмов более низкого уровня. Например, бот, который отвечает на запросы на естественном языке, будет включать в себя организованную комбинацию алгоритмов для обнаружения звуков, захвата синтаксических структур, извлечения соответствующих знаний, построения выводов, генерации ответов и т.д.

2. Наиболее проблемным является вопрос о создании новых данных, полученных в результате самообучения нейронной сети. В системе, способной к обучению, особо важным компонентом будет не изученная алгоритмическая модель, т.е. алгоритмы, которые непосредственно выполняют задачи, возложенные на систему (например, составление классификаций, прогнозов или решений), а, скорее, алгоритмы обучения, которые модифицируют алгоритмическую модель, чтобы она лучше выполняла его функцию. Например, в системе классификатора, которая распознает изображения с помощью нейронной сети, решающим элементом является алгоритм обучения (тренажер), который изменяет внутреннюю структуру алгоритмической модели (обученная нейронная сеть), изменяя его (изменяя его внутренние связи и веса) таким образом, чтобы он правильно классифицировал объекты в своей области (например, животных, звуки, лица, позы и т.д.).

Алгоритм обучения системы (ее тренажер) использует обучающий набор для построения алгоритмической модели: нейронную сеть, дерево решений, набор правил и т.д. Алгоритмическая модель предназначена для сбора соответствующих знаний, изначально заложенных в обучающий набор, а именно корреляций между случаями и ответами. Затем эта модель используется алгоритмом прогнозирования для предоставления, как всегда надеются разработчики, правильных ответов на новые случаи, имитируя корреляции в обучающем наборе.

Если примеры в обучающий набор, наиболее близкий к новому случаю (с точки зрения соответствующих функций), связан с определенным ответом, тот же ответ будет предложен для нового случая. Например, если картинки, наиболее похожие на новый ввод, были помечены как кошки, то и новый ввод будет помечен таким же образом; если прошлые кандидаты, характеристики которых наилучшим образом соответствуют характеристикам нового кандидата, были связаны с отклонением, система предложит отклонить также нового кандидата; если прошлые работники, которые ближе всего подходят к новому кандидату, показали хорошие (или плохие) результаты, системы предсказывают, что и заявитель будет действовать аналогичным образом<sup>5</sup>. Все это требует особого подхода с позиции выработки новых персональных данных. Необходимо учитывать согласие и иные законные основания для подобной обработки персональных данных, а также возможность их использования в измененной в ходе машинного обучения форме.

<sup>5</sup> The impact of the General Data Protection Regulation (GDPR) on artificial intelligence / European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 641.530 June 2020. P. 4, 11.



В последнее время глубокое обучение, основанное на многоуровневых нейронных сетях, было очень успешно внедрено — особенно, но не исключительно — там, где необходимо распознавать паттерны и связывать их с классификациями и решениями (например, при обнаружении объектов на изображениях, распознавании звуков и их источников, постановке медицинского диагноза, переводе текстов, выборе стратегий в играх и т.д.). Нейронные сети состоят из набора узлов, называемых нейронами, расположенных в несколько слоев и соединенных ссылками. Они так называются, поскольку воспроизводят некоторые аспекты нервной системы человека, действительно состоящую из взаимосвязанных специализированных клеток, биологических нейронов, которые получают и передают информацию.

Нейронные сети и были разработаны в предположении, что искусственный интеллект может быть достигнут путем воспроизведения человеческого мозга, а не путем моделирования человеческого мышления, т.е. что искусственное мышление естественным образом возникнет из искусственного мозга. Хотя может встать вопрос: в какой степени искусственные нейронные сети и человеческий мозг действительно имеют сходные структуры и процессы. Каждый нейрон получает сигналы (числа) от подключенных нейронов или извне, и эти сигналы усиливаются или уменьшаются по мере пересечения входящих связей, в соответствии с весами последних.

Нейрон применяет некоторые вычисления к входным данным, которые он получает, и, если результат достигает порогового значения нейрона, нейрон становится активным, посылая сигналы подключенным нейронам или снаружи из сети. Активация начинается с узлов, получающих внешние входные данные, и распространяется по сети. Обучение сети происходит путем информирования сети о том, являются ли ее ответы (ее выходные данные) правильными или неправильными. Если ответ сети неверен, алгоритм обучения обновляет сеть, т.е. корректирует веса соединений, так что в следующий раз, когда сети будут предоставлены эти входные данные, она выдаст правильный ответ.

В случае нейронной сети алгоритм обучения модифицирует сеть до тех пор, пока она не достигнет желаемого уровня производительности, в то время как результатом обучения — алгоритмической моделью — является сеть в ее окончательной конфигурации.

Как отмечалось ранее, алгоритм обучения способен модифицировать нейронную сеть таким образом, чтобы сеть была способна предоставлять наиболее подходящие ответы. При контролируемом подходе к обучению обученная сеть будет воспроизводить поведение в обучающий набор; в соответствии с подходом к обучению с подкреплением сеть будет придерживаться поведения, которое максимизирует ее эффективность (пример — бонусные баллы, связанные с прибылью от инвестиций или с победами в играх).

Важная проблема состоит еще и в том, что «нейронная сеть не дает объяснений своим результатам. Можно определить, как данный результат был получен в результате активации сети и как эта активация в ответ на заданный ввод была определена соединениями между нейронами (и весами, присвоенными таким соединениям в результате обучения сети) и математическими функциями, управляющими каждым нейроном. Однако эта информация не показывает логического

обоснования, значимого для людей: она не говорит нам, почему был дан определенный ответ. В связи с этим важно понимать, что субъекту персональных данных оператор не может указать, почему получена именно такая информация.

Существует множество подходов к объяснению поведения нейронных сетей и других непрозрачных систем (также называемых «черными ящиками»). Некоторые из этих подходов рассматривают систему, подлежащую объяснению, и строят объяснения соответствующим образом. Другие подходы строят объяснения на основе внешнего поведения сети: они рассматривают только связь между входными данными, предоставляемыми сетью, и результатами, которые она обеспечивает, и, соответственно, строят аргументы или другие объяснения.

Однако достижения в объяснении нейронных сетей, понятных человеку, до сих пор были весьма ограниченными. К сожалению, во многих областях системы, функционирующие в меньшей степени является системой машинного обучения, наилучший баланс также зависит от области, в которой используется система, и от важности затрагиваемых интересов. Когда речь идет о публичных действиях и на карту поставлены ключевые интересы человека (например, как в судебных решениях), объяснение имеет первостепенное значение.

Однако даже тогда, когда систему можно рассматривать только как «черный ящик», некоторый критический анализ ее поведения все еще возможен. С помощью анализа чувствительности, т.е. систематической проверки того, изменяется ли результат при изменении значения определенных входных характеристик, оставляя все остальные характеристики неизменными, мы можем понять, какие функции определяют выходные данные системы. Например, проверяя, изменяется ли прогноз системы, предназначенной для оценки кредитоспособности, если мы изменяем место рождения или жительства заявителя, мы можем определить, имеет ли эта входная функция отношение к выходным данным системы. Следовательно, мы можем задать вопрос, не является ли система чрезмерно дискриминирующей людей в зависимости от их этнической принадлежности или социального статуса, который может быть связан с местом рождения или проживания<sup>6</sup>.

Особую обеспокоенность вызывает вопрос о защите информации, сохраняемой нейронными сетями, в том числе персональными данными. Нейронные сети могут сохранять части набора данных, используемые для обучения и генерации текста. Вредоносные объекты могут проникнуть в сеть для получения конфиденциальных данных, таких как номера кредитных карт и номера социального страхования. «В идеале, даже если бы обучающие данные содержали редкую, но конфиденциальную информацию о некоторых отдельных пользователях, нейронная сеть не запоминала бы эту информацию и никогда не выдавала бы ее как завершение предложения»<sup>7</sup>.

Нужно также учитывать, что это может быть преднамеренным и непреднамеренным запоминанием. Когда речь идет о непреднамеренном запоминании,

<sup>6</sup> The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. P. 14—15.

<sup>7</sup> Nicholas Carlini, Chang Liu, Úlfar Erlingsson, Jernej Kos, Dawn Song. (2019) The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Network // URL: <https://doi.org/10.48550/arXiv.1802.08232>.



модели глубокого обучения (в частности, генеративные модели), по-видимому, часто запоминают редкие детали обучающих данных, которые совершенно не связаны с предполагаемой задачей, в то время как модель все еще изучает базовое поведение (т.е. в то время как потеря теста все еще уменьшается). Такое непреднамеренное запоминание редких деталей обучения может вызвать серьезные проблемы с конфиденциальностью при использовании конфиденциальных данных для обучения моделям глубокого обучения.

Самое тревожное, что такое запоминание может произойти даже для примеров, которые присутствуют в обучающих данных всего несколько раз, особенно когда эти примеры являются выбросами в распределении данных; это верно даже для языковых моделей, которые используют современные методы регуляризации для предотвращения традиционных форм переобучения и перетренированности. На сегодняшний день не существует хорошего метода, помогающего практикующим специалистам измерить степень запоминания моделью аспектов обучающих данных<sup>8</sup>. В случае преднамеренного запоминания речь должна идти об административной или уголовной ответственности.

Сложности, связанные с выявлением фактов использования персональных данных в нейронных сетях и их модификаций, обуславливают ограничения в возможности защиты прав на персональные данные, в том числе их гражданско-правовой защиты и возможного возмещения причиненного ущерба и компенсации морального вреда. В связи с этим важно обеспечить законодательные требования к информированию субъектов персональных данных.

В связи с этим нам представляется, что в законодательстве о персональных данных должно быть закреплено, что обработка персональных данных с использованием нейронных сетей должна производиться только при условии письменного согласия субъекта персональных данных. Кроме того, любые изменения персональных данных, произведенные в результате процессов машинного обучения, должны регулярно согласовываться с субъектом персональных данных. Ему должна быть обеспечена возможность ознакомления с обновленными персональными данными.

## БИБЛИОГРАФИЯ

1. *Бойченко И. С.* Модели правового регулирования нейросетей // Образование и право. — 2019. — № 1. — С. 235—237.
2. *Бойченко И. С.* Формирование правового регулирования нейронных сетей // Формирование системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе. Вторые Бачиловские чтения : сборник научных трудов. Москва, 8 февраля 2019 г. — М. ; Саратов : Амирит, 2019. — С. 218—223.
3. Информационно-технологическое обеспечение юридической деятельности (LegalTech) : учебник / А. В. Минбалеев, Т. А. Полякова, М. Б. Добробаба [и др.]. — М. : Проспект, 2023. — 368 с.

<sup>8</sup> *Carlini Nicholas, Chang Liu, Úlfar Erlingsson, Jernej Kos, Dawn Song.* Op. cit.

4. Минбалеев А. В. Проблемы социальной эффективности и защиты прав человека при использовании искусственного интеллекта в рамках социального скоринга // Вестник Южно-Уральского государственного университета. — Серия : Право. — 2020. — Т. 20. — № 2. — С. 96—101.
5. Полякова Т. А., Химченко А. И. Правовые проблемы обеспечения информационной безопасности при использовании облачных технологий // Правовая информатика. — 2013. — № 2. — С. 12—16.
6. Право и иные регуляторы в развитии цифровых технологий / А. В. Минбалеев, А. В. Мартынов, Г. Г. Камалова [и др.]. — Саратов : Амирит, 2022. — 338 с.
7. Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций : колл. монография : в 2 т. / Е. Н. Абанина, О. Ю. Авдевина, Р. В. Амелин [и др.]. — Саратов : Саратовская государственная юридическая академия, 2020. — 204 с.
8. Carlini Nicholas, Chang Liu, Úlfar Erlingsson, Jernej Kos, Dawn Song. (2019) The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks // URL: <https://doi.org/10.48550/arXiv.1802.08232>.
9. Drew Stevens. (2018) Neural Networks And Advanced AI Contract Issues // URL: <https://drewstevenslaw.com/neural-networks-and-advanced-ai-contract-issues/> (дата обращения: 10.12.2022).
10. The Impact of the General Data Protection Regulation (GDPR) on artificial intelligence / European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 641.530 — June 2020.



**Кира Кирилловна  
ТАРАН,**

ассистент кафедры  
информационного права  
и цифровых технологий  
Университета имени  
О.Е. Кутафина МГЮА,  
эксперт Центра цифровой  
экономики и  
финансовых инноваций  
МГИМО (У) МИД России  
[taran.kira@yandex.ru](mailto:taran.kira@yandex.ru)  
125993, Россия, г. Москва,  
ул. Садовая-Кудринская, д. 9

## Формирование в ЕС нормативно-правовой базы, регулирующей отношения по использованию искусственного интеллекта

**Аннотация.** В Европейском союзе активно развивается регулирование отношений по созданию, внедрению и использованию технологии искусственного интеллекта. Нормативная правовая база в настоящее время является достаточно обширной. Также большое значение придается проекту регламента Европарламента и Совета ЕС, закрепляющему гармонизированные правила в отношении искусственного интеллекта (закон об искусственном интеллекте) и вносящему изменения в соответствующие законодательные акты Союза.

Цель статьи — провести комплексное исследование основных нормативных правовых актов ЕС и уделить особое внимание положениям закона об искусственном интеллекте ЕС. Методологическую основу составляют методы анализа и синтеза. Исследованы основные нормативные правовые акты ЕС в указанной сфере, выделены наиболее важные вопросы регулирования. К последним относятся: фрагментация цифрового рынка, риски при использовании технологии, этическая основа, сертификация, контроль за использованием технологии, ответственность за нарушение нормативной правовой основы.

**Ключевые слова:** искусственный интеллект, робототехника, Европейский союз, информационные технологии.

DOI: 10.17803/2311-5998.2023.102.2.080-089

**KIRA K. TARAN,**

Assistant of the Department of  
information law and digital technologies  
of the Kutafin Moscow State Law University (MSAL),  
Expert of the Center for Digital Economy and Financial Innovations  
of the MGIMO University  
[taran.kira@yandex.ru](mailto:taran.kira@yandex.ru)  
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

### Constituting a regulatory framework in the EU that regulates relations on the using artificial intelligence

**Abstract.** There is an active development of regulation of creating, implementing and using artificial intelligence technology in the European Union. The regulatory legal framework is currently quite extensive. The Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain

*Union Legislative Acts will take leading place. Purpose: to conduct a comprehensive study of the main EU legal acts and pay special attention to the provisions of the Artificial Intelligence Act. The methodological basis is the analysis and synthesis. Results: main legal acts of the EU are researched; the most important regulatory issues are highlighted. Conclusions: the most important issues are fragmentation of the digital market, risks in the using technology, ethical basis, certification, control over the use of technology, liability for violation of the regulatory legal framework.*

**Keywords:** artificial intelligence, robotics, European Union, information technologies.

**В** настоящее время на международном уровне и уровне государств активно ведется разработка нормативной правовой базы регулирования отношений по использованию искусственного интеллекта (ИИ). Данная технология является крайне перспективной и может быть использована в различных сферах общественной жизни: в государственном управлении, медицине, транспорте, сельском хозяйстве, образовании и т.д. Технология ИИ является инновационным, научным и высокотехнологичным продуктом, который комплексно затрагивает различные сферы общественной жизни, безопасность и т.д. В связи с этим важными представляются вопросы формирования правовой основы регулирования данной технологии, экспериментальных правовых режимов, создания технологических стандартов, правил, которые исключают возможность нанесения вреда человеку, обществу, государству и окружающей среде.

На международном уровне уже существуют документы, которые регулируют различные правовые вопросы, возникающие при разработке, внедрении и использовании ИИ, в том числе:

- Рекомендация по искусственному интеллекту, принятая Советом Организации экономического сотрудничества и развития 22 мая 2019 г.;
- Записка секретариата Комиссии ООН по праву международной торговли «Правовые вопросы, касающиеся цифровой экономики, искусственного интеллекта» A/CN.9/1012/Add.1/ (53-я сессия ГА ООН, 6—17 июля 2020 г.);
- Рекомендация ЮНЕСКО об этических аспектах ИИ, принятая на 41-й сессии Генеральной конференции ЮНЕСКО 9—24 ноября 2021 г.;
- Отчет Международного союза электросвязи «Исследование МСЭ-D потенциальных направлений развития региона СНГ в период 2022—2025. Направление — Кибербезопасность» (7 апреля 2021 г.) и др.

Данные документы являются руководящей правовой основой для государств в сфере развития законодательства, регулирующего вопросы использования информационных технологий (ИТ) и ИИ.

В Европейском союзе (ЕС) с 2017 г. ведется серьезная научная работа по изучению вопросов регулирования отношений по использованию ИИ. Формирование правовой основы на уровне регионального образования поможет государствам в создании гармонизированной правовой основы. ЕС развивает правовую основу для функционирования единого цифрового рынка, чтобы противодействовать *фрагментации*, которая может выражаться в различии требований к продуктам



и услугам в сфере ИИ в государствах ЕС, в том числе к их использованию, ответственности в этой сфере, надзору со стороны государственных органов; в *снижении правовой определенности* как для поставщиков, так и для пользователей систем, оснащенных ИИ (далее — системы ИИ).

Основные правовые проблемы, которые возникают при разработке, развитии и использовании данной технологии, связаны с возможным развитием правосубъектности у роботов, оснащенных ИИ; с определением ответственного лица за действия, которые осуществляются системой ИИ; определением лица, которому будут принадлежать авторские права на те результаты (научные, технические выборки, произведения и т.д.), которые получены ИИ или при помощи ИИ; с разработкой технических стандартов, учетом и сертификацией устройств с ИИ и др.

При анализе правовых проблем, которые возникают в связи с развитием, внедрением и использованием ИИ, помимо кибербезопасности, Е. В. Холодная выделяет также трансформацию рынка труда, социальный раскол в обществе в связи с сокращением среднего класса, важность разработки этических фильтров (на уровне правовых норм) для сохранения достоинства личности и т.д.<sup>1</sup> Данные проблемы являются актуальными для стран ЕС и для других государств, которые занимаются развитием рассматриваемой технологии.

**Правовую основу** регулирования отношений в сфере создания, использования и внедрения ИИ составляют следующие документы.

*Резолюция Европарламента для Европейской комиссии относительно норм гражданского права о робототехнике* от 16 февраля 2017 г.<sup>2</sup> Она является комплексным документом, в котором изучаются вопросы признания за сложными роботами статуса электронного лица. Предполагается, что такие сложные роботы смогут принимать решения. Данный документ создает предпосылки для возложения на роботов ответственности в случае причинения ущерба. В документе рассматриваются основные принципы развития робототехники и ИИ для гражданского использования, этические принципы, стандартизация и безопасность таких устройств; использование автономных транспортных средств, дронов; роботов для ухода за пожилыми людьми; роботов, применимых в медицине, и др.

*Декларация о сотрудничестве в области искусственного интеллекта* от 10 апреля 2018 г.<sup>3</sup> Декларация подписана представителями 25 европейских стран, включая Великобританию и Норвегию. Согласно документу государства-участники решают задачи по развитию технологии ИИ, инновационных бизнес-моделей, ускорению экономического роста, созданию новых высококвалифицированных профессий и трансформации рынка труда, созданию правовой и технической

<sup>1</sup> Холодная Е. В. О перспективных направлениях правового регулирования в сфере технологии искусственного интеллекта // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 12 (64). С. 93—94.

<sup>2</sup> European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2013(INL) // URL: [https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html) (дата обращения: 17 января 2023 г.).

<sup>3</sup> Declaration of cooperation on Artificial Intelligence, 2018 // URL: <https://ec.europa.eu/jrc/communities/sites/default/files/2018aideclarationatdigitaldaydocxpdf.pdf> (дата обращения: 17 января 2023 г.).

основы для использования соответствующей технологии, а также по проведению научных исследований в данной сфере, созданию научных центров и обмену национальным опытом.

*Коммюнике «Искусственный интеллект для Европы»* от 25 апреля 2018 г.<sup>4</sup> Документ содержит примеры использования ИИ в различных сферах. Цель документа — технологическое и индустриальное использование ИИ в частном и публичном секторе; проведение подготовительных работ для социальноэкономических изменений в области образования, в сфере труда и т.д.; развитие этической и правовой основы в Союзе на основе ценностей, закрепленных в правовой базе Союза. Документ рассматривает конкурентную позицию ЕС с такими государствами, как США и Китай, в которых успешно осуществляются инвестиции в сфере ИИ. В документе содержится информация о проектах по использованию ИИ.

*Руководство по этике для надежного искусственного интеллекта* от 8 апреля 2019 г.<sup>5</sup> Данный документ является основой для разработки, внедрения и использования такой технологии ИИ, которая будет характеризоваться как вызывающая доверие, надежная. В документе закрепляются основные этические принципы, такие как уважение человеческой автономии, предотвращение вреда, справедливость и объяснимость. Руководство по этике для надежного искусственного интеллекта содержит семь основных требований, которые должны выполняться по отношению к системе ИИ: подконтрольность человеку, надзор; техническая безопасность; неприкосновенность частной жизни, конфиденциальность и управление данными; прозрачность; отсутствие дискриминации и справедливость; общественное и экологическое благополучие; подотчетность.

*Политические и инвестиционные рекомендации для надежного искусственного интеллекта* от 26 июня 2019 г.<sup>6</sup> Данный документ направлен на то, чтобы ИИ приносил пользу людям и обществу в целом, частному сектору, публичному сектору, был востребован при проведении исследований в Европе, при работе с данными (включая вопросы доступности), в сферах образования, управления и регулирования, создания фондов и инвестиций.

Для ЕС крайне важной является сфера кибербезопасности, в связи с этим существенную роль играет *Регламент ЕС 2019/881 Европарламента и Совета ЕС об ENISA (Агентство ЕС по кибербезопасности) и сертификации по кибербезопасности информационных и коммуникационных технологий* от 17 апреля 2019 г., который отменяет действие Регламента 526/2013 (Закон о кибербезопасности)<sup>7</sup>. Данный Регламент будет применяться по отношению к ИИ, так как

<sup>4</sup> Communication from the Commission Artificial Intelligence for Europe, 2018 // URL: <https://eur-lex.europa.eu/legal-content/en/txt/?uri=com%3a2018%3a237%3afin> (дата обращения: 17 января 2023 г.).

<sup>5</sup> Ethics guidelines for trustworthy AI, 2019 // URL: <https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html> (дата обращения: 17 января 2023 г.).

<sup>6</sup> Policy and investment recommendations for trustworthy Artificial Intelligence, 2019 // URL: <https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence> (дата обращения: 17 января 2023 г.).

<sup>7</sup> Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and



использование данной технологии может быть связано с высоким уровнем риска в области кибербезопасности.

Одним из ведущих документов является *Стратегическая программа «Цифровая Европа» на 2021—2027 годы*<sup>8</sup>, в которой рассматриваются вопросы развития ИИ и робототехники.

Нормативная правовая база ЕС отличается высоким уровнем развития механизмов, которые разработаны для регулирования отношений в сфере создания, использования и внедрения ИИ. А. И. Филипова утверждает, что в Европе региональное регулирование является наиболее разработанным, при этом она рассматривает также документы Совета Европы и региональное регулирование ИИ техническими стандартами<sup>9</sup>.

Б. С. Шталь, Р. Родригес, Н. Сантьяго, К. Мэкиш считают, что и регулирование, и технология ИИ не могут быть сведены к одной географической области или юрисдикции, так как по своей природе данная технология носит трансграничный характер. Ученые рассматривают механизмы, создаваемые на уровне ЕС, как наиболее эффективные, позволяющие учесть использование соответствующей технологии на территории нескольких государств<sup>10</sup>.

М. Б. Добробаба отмечает, что «правовое регулирование ИИ отличается междисциплинарным подходом, поскольку имеет конституционно-правовые, гражданско-правовые, административно-правовые, уголовно-правовые, трудовые и другие аспекты»<sup>11</sup>.

В 2021 г. был подготовлен проект регламента Европарламента и Совета ЕС, содержащий гармонизированные правила в отношении искусственного интеллекта (закон об искусственном интеллекте) и вносящий изменения в соответствующие законодательные акты Союза (com/2021/206 final)<sup>12</sup> (далее — Проект). Документ достаточно объемный и состоит из основной части и приложений.

---

communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) // URL: [https://eur-lex.europa.eu/legal-content/en/txt/?uri=uriserv:OJ.L\\_.2019.151.01.0015.01.eng](https://eur-lex.europa.eu/legal-content/en/txt/?uri=uriserv:OJ.L_.2019.151.01.0015.01.eng) (дата обращения: 17 января 2023 г.).

<sup>8</sup> The Digital Europe programme for the period 2021—2027 / European Commission // URL: <https://digital-strategy.ec.europa.eu/en/activities/digital-programme> (дата обращения: 17 января 2023 г.).

<sup>9</sup> Филипова И. А. Правовое регулирование искусственного интеллекта : учебное пособие, 2-е изд., обновл. и доп. Н. Новгород : Нижегородский госуниверситет, 2022. С. 75—79.

<sup>10</sup> Stahl B. C., Rodrigues R., Santiago N., Macnish K. A. European Agency for Artificial Intelligence: Protecting fundamental rights and ethical values / Computer Law & Security Review. 12 March 2022. Vol. 45 (Cover date: July 2022). Article 105661 // URL: <https://www.sciencedirect.com/science/article/pii/S0267364922000097?via%3dihub>. P. 2. (дата обращения: 25 декабря 2022 г.).

<sup>11</sup> Добробаба М. Б. Искусственный интеллект: объект или субъект права? // Новеллы Конституции Российской Федерации и задачи юридической науки : материалы конференций в рамках X Московской юридической недели : в 5 ч. М., 2021. С. 304.

<sup>12</sup> Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) and amending certain

Проект содержит информацию о том, как велась работа, какие документы были изучены.

Проект был подготовлен в целях:

- обеспечить, чтобы системы ИИ, размещенные и используемые на рынке Союза, были безопасными и соответствовали действующему законодательству об основных правах и ценностях Союза;
- гарантировать правовую определенность для содействия инвестициям и инновациям в области ИИ;
- усовершенствовать управление, правоприменение и исполнение требований безопасности, применимых к системам ИИ;
- способствовать развитию единого рынка для приложений ИИ и предотвратить фрагментацию рынка.

Проект направлен на регулирование всего жизненного цикла ИИ. С учетом того, что использование данной технологии связано с высоким уровнем риска, после принятия документ будет дополняться положениями Общего регламента по защите данных (Регламент (ЕС) 2016/679), Директивы по обеспечению правопорядка (Директива (ЕС) 2016/680), Директивы об электронной коммерции 2000/31/ЕС, инициативными предложениями и др.

Комиссия ЕС рассматривала различные варианты регулирования указанных вопросов с точки зрения экономики, права и социальных последствий для функционирования единого цифрового рынка и пришла к выводу, что наиболее предпочтительным является создание нормативной базы только для систем ИИ с высоким уровнем риска. Проект содержит обязательные требования в отношении данных, документации, прослеживаемости действий системы ИИ, предоставления информации, прозрачности, надзора. Введение кодексов поведения для невысокорисковых систем ИИ компании могут осуществлять на добровольной основе.

Использование систем ИИ с высоким риском в сложных сферах (машиностроение, медицинские устройства и др.) потребует создания новой правовой основы для данных сфер. Старый подход к регулированию, который использовался по отношению к источникам повышенной опасности, например таким, как автомобиль, воздушное судно, будет применяться не напрямую.

Рассмотрим **основные положения Проекта**. Сфера применения Проекта достаточно широкая (ст. 2), распространяется на:

- а) поставщиков (провайдеров), размещающих на рынке или вводящих в эксплуатацию системы ИИ в Союзе, независимо от того, учреждены они на территории ЕС или в третьем государстве;
- б) пользователей систем ИИ, расположенных на территории Союза;
- в) провайдеров и пользователей систем ИИ, расположенных в третьем государстве, если произведенные системой результаты используются в ЕС.

В Проекте устанавливается экстерриториальность, аналогичная закрепленной в Регламенте ЕС 2016/679 (General Data Protection Regulation)<sup>13</sup>.

Union Legislative Acts COM/2021/206 final // URL: <https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a52021pc0206> (дата обращения: 25 декабря 2022 г.).

<sup>13</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on



Как уже отмечалось, Проект был ориентирован на высокорисковые системы ИИ, документ построен на основе риск-ориентированного подхода и устанавливает несколько уровней риска.

**Запреты на использование системы ИИ.** Статья 5 Проекта устанавливает запреты на использование ИИ, если:

- используются методы, которые выходят за пределы сознания человека и лицу может быть причинен физический или психологический вред;
- система использует уязвимости определенной группы лиц (возраст, физическая или умственная неполноценность), тем самым лицу может быть причинен физический или психологический вред;
- введение систем ИИ государственными органами или от их имени для оценки или классификации благонадежности физических лиц на протяжении определенного периода времени на основе их социального поведения или известных, прогнозируемых личностных характеристик.

Относительно биометрической идентификации ст. 5 Проекта предусматривает принятие индивидуального решения на основе предварительного разрешения, выданного судебным органом или независимым административным органом государства-члена. При этом в экстренной ситуации использование системы может быть начато без разрешения.

**Сферы использования с наибольшими рисками.** В приложении 3 к Проекту устанавливается перечень сфер, в которых проявляются высокие риски при использовании технологии:

- 1) биометрическая идентификация и распределение физических лиц на категории;
- 2) управление и эксплуатация критической инфраструктуры (планируется использование в следующих сферах: дорожное движение, водо-, газо-, электроснабжение, отопление);
- 3) образование и профессиональная подготовка;
- 4) занятость, управление сотрудниками и доступ к информации о самозанятых (использование ИИ для отбора сотрудников, оценки кандидатов, принятия решений о повышении в должности, прекращении трудовых договоров, распределении задач и др.);
- 5) доступ к основным услугам, предоставляемым частными лицами, и государственным услугам, пользование ими (использование ИИ для оценки кредитоспособности; определения права на получение льгот, государственной помощи и т.д., определение приоритета при работе служб (пожарной, медицинской) и др.);
- 6) правоприменение (проверка рисков совершения правонарушения, ИИ как детектор лжи, оценка достоверности доказательств, прогнозирование рецидивов преступлений, проведение расследований, работа с наборами данных и др.);
- 7) управление миграцией, вопросами предоставления убежища и пограничным контролем (ИИ для оценки рисков безопасности, подлинности документов, рассмотрения заявлений на предоставление визы, вида на жительство и др.).

---

the Free Movement of such Data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) // URL: <https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:32016r0679&from=en> (дата обращения: 25 ноября 2022 г.).

8) организация правосудия и демократических процессов (ИИ для помощи судебным органам в исследовании, толковании фактов и законов и др.).

Данный перечень рисков будет пополняться согласно положениям регламента и установленным в нем критериям (ст. 7).

**Управление рисками.** Для противодействия рискам высокого уровня Проект предусматривает создание системы управления рисками, которая будет регулярно обновляться. Оценка рисков будет осуществляться на протяжении всего жизненного цикла системы ИИ при выполнении следующих видов работ (ст. 9 Проекта):

- идентификация и анализ известных и предвидимых рисков;
- оценка рисков, которые могут возникнуть в связи с неправильным использованием системы ИИ;
- оценка рисков, которые могут быть основаны на данных;
- одобрение подходящих мер по управлению рисками.

Риски высокого уровня, связанные с данными, могут быть снижены путем их подготовки для работы с ИИ, включая их аннотирование, отметку, очистку, дополнение и агрегирование (объединение), проведение предварительной оценки доступности количества наборов данных и т.д. В случае возникновения инцидентов регламент обязывает провайдеров систем ИИ с высоким уровнем риска сообщать о них, а также сообщать о неправильной работе системы (ст. 62 Проекта).

Статья 69 Проекта призывает государства ЕС разработать кодексы поведения по использованию невысокорисковых систем ИИ. При использовании систем ИИ с ограниченным риском (голосовые помощники и т.п.) человек должен быть проинформирован, что взаимодействует с технологией ИИ. Проект не затрагивает регулирование систем ИИ с минимальным риском в части прав и безопасности граждан.

Меры по противодействию рискам высокого уровня включают ведение технической документации (ст. 11 Проекта), постоянное протоколирование и фиксацию операций, которые совершает Система ИИ (ст. 12 Проекта), предоставление полной и прозрачной (транспарентной) информации пользователю о том, как пользоваться системой (ст. 13 Проекта), контроль со стороны человека для предотвращения или минимизации рисков здоровью, безопасности и нарушения фундаментальных прав, которые могут возникнуть при неправильном использовании высокорисковых систем ИИ (ст. 14 Проекта). Высокорисковые системы ИИ должны функционировать для выполнения определенных целей, для которых они созданы, при этом проводимые операции должны характеризоваться точностью, надежностью, должны соблюдаться меры по обеспечению кибербезопасности (ст. 15 Проекта).

Проект регламента устанавливает обязанности по отношению к провайдерам систем ИИ, изготовителям, импортерам, дистрибьютерам, пользователям и третьим лицам.

Предполагается, что высокорисковые системы ИИ, которые соответствуют гармонизированным стандартам или их частям, ссылки на которые были опубликованы в Официальном журнале Европейского союза (Official Journal of the European Union), соответствуют требованиям, изложенным в главе 2 Проекта.

Высокорисковые системы ИИ могут подлежать сертификации, в том числе по кибербезопасности. Согласно ст. 44 Проекта сертификат будет выдаваться



уполномоченным органом государства ЕС на официальном языке ЕС. Срок действия сертификата не должен превышать пяти лет. Более того, прежде чем система ИИ с высоким уровнем риска будет размещена на рынке, она должна быть зарегистрирована в базе данных ЕС.

Проект регламента указывает на необходимость создания «регуляторных песочниц», т.е. системы должны тестироваться согласно всем техническим и правовым требованиям, включая обработку персональных данных, ограниченный период времени до размещения на рынке либо до запланированного запуска. Согласно ст. 54 документа персональные данные, которые были на законном основании собраны для других целей, могут обрабатываться и использоваться для тестирования в рамках «регуляторной песочницы» при соблюдении установленных условий.

Проект предусматривает создание европейского совета по ИИ (European Artificial Intelligence Board), который будет содействовать работе Комиссии ЕС. В его состав войдут представители (руководители) национальных органов. Планируется создание внутригосударственных органов, которые будут контролировать соблюдение положений регламента.

За нарушение положений регламента предусматривается штраф до 30 000 000 евро. Данный штраф предусматривается в случае нарушений ст. 5 Проекта регламента, в которой содержится запрет ряда ИИ систем с неприемлемым уровнем риска, и ст. 10 документа — при нарушении требований к системам ИИ с высоким уровнем риска.

Интеграция использования сервисов, оснащенных ИИ, будет осуществляться согласно Регламенту Европарламента и Совета ЕС от 19.10.2022 о едином рынке цифровых услуг (Закон о цифровых услугах), изменяющему Директиву ЕС 2000/31/ЕС<sup>14</sup>. Данный документ обязывает предоставлять сведения об оказании цифровых услуг, регулирует деятельность провайдеров, распространение незаконной информации и др.

Уровень развития права и технологий в ЕС является достаточно высоким, создание нормативной базы позволяет объединению и состоящим в нем государствам быть конкурентоспособными наряду с такими ведущими ИТ-державами, как США и КНР. Вопросы развития отношений по созданию, внедрению и использованию ИИ являются сложными и в настоящий момент не могут быть урегулированы в ЕС одним документом.

Предложение по Регламенту Европейского парламента и Совета ЕС, закрепляющему гармонизированные правила об искусственном интеллекте (закон об искусственном интеллекте) и внесении изменений в соответствующие законодательные акты Союза (com/2021/206 final) является проработанным документом, который включает в себя наиболее важные вопросы, связанные с использованием данной технологии: определение сфер, в которых проявляются наибольшие риски; определение рисков и их мониторинг на всех этапах использования

<sup>14</sup> Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) // URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj> (дата обращения: 17 января 2023 г.).

технологии, сертификация, контроль за использованием технологии, ответственность за нарушение положений документа.

Не менее важными вопросами являются фрагментация цифрового рынка, развитие этической основы регулирования, применение технологии в различных сферах, финансирование и инвестирование. Документы ЕС в данной сфере могут быть использованы различными государствами в целях изучения опыта для дальнейшего развития собственного законодательства.

### БИБЛИОГРАФИЯ

1. *Добробаба М. Б.* Искусственный интеллект: объект или субъект права? // Новеллы Конституции Российской Федерации и задачи юридической науки : материалы конференций в рамках X Московской юридической недели : в 5 ч. — М., 2021. — С. 303—308.
2. *Филипова И. А.* Правовое регулирование искусственного интеллекта : учебное пособие. — 2-е изд., обновл. и доп. — Н. Новгород : Нижегородский госуниверситет, 2022. — 275 с.
3. *Холодная Е. В.* О перспективных направлениях правового регулирования в сфере технологии искусственного интеллекта // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2019. — № 12 (64). — С. 89—96.
4. *Stahl B. C., Rodrigues R., Santiago N., Macnish K. A.* European Agency for Artificial Intelligence: Protecting fundamental rights and ethical values // Computer Law & Security Review. 12 March 2022. Vol. 45 (Cover date: July 2022) Article 105661. URL: <https://www.sciencedirect.com/science/article/pii/S0267364922000097?via%3Dihub> (дата обращения: 25.12.2022).

## Информационная безопасность гражданского общества



**Сергей Васильевич  
СОЛОВКИН,**

аспирант кафедры  
информационного права и  
цифровых технологий  
Университета имени  
О.Е. Кутафина (МГЮА)  
[svsolovkin@msal.ru](mailto:svsolovkin@msal.ru)  
125993, Россия, г. Москва,  
ул. Садовая-Кудринская, д. 9

### Автоматизированный сбор данных о человеке: неявные принципы правового регулирования<sup>1</sup>

**Аннотация.** В условиях цифровой трансформации возникла объективная необходимость в модернизации действующего правового регулирования в сфере данных о человеке. Предпринимаемые законодателем попытки модернизации указанного регулирования не приводят к решению некоторых проблем фундаментального уровня. В настоящей работе автором предпринята попытка выявить и критически проанализировать неявные принципы правового регулирования отношений в сфере сбора данных о человеке. Автором установлено наличие как минимум трех неявных принципов, определяющих актуальное отечественное регулирование в исследуемой сфере, а именно: (1) превентивная охрана данных о человеке априори обеспечивает охрану и защиту прав субъектов данных; (2) защита прав субъектов персональных данных должна осуществляться преимущественно публичными способами; (3) субъекты персональных данных являются разумными, в связи с чем они должны нести бремя определения судьбы своих персональных данных.

Выявленные принципы были также критически проанализированы автором, в результате чего была установлена их несостоятельность и неэффективность в современном контексте. Сделан вывод о необходимости концептуального реформирования регулирования в сфере автоматизированного сбора данных о человеке на базовом уровне, что уже сейчас должно стать предметом широких дискуссий в юридической среде. Кроме того, даны некоторые авторские рекомендации по потенциальному реформированию регулирования в сфере сбора данных о человеке в ближайшем будущем.

**Ключевые слова:** принципы правового регулирования, цифровая трансформация, датафикация, данные, защита данных, информационная безопасность, информационное право, компьютерная безопасность, большие данные, персональные данные, программное обеспечение, сбор данных в Интернете.

DOI: 10.17803/2311-5998.2023.102.2.090-100

**SERGEY V. SOLOVKIN,**

postgraduate student of the Department of information law  
and digital technologies  
of the Kutafin Moscow State Law University (MSAL),  
[svsolovkin@msal.ru](mailto:svsolovkin@msal.ru)  
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

### **Automated Collection of Data on a Person: Implicit Principles of Legal Regulation**

**Abstract.** *In the digital transformation context, an objective need has arisen to modernize the current personal data regulation. The legislator's attempts to develop this regulation do not bring the required results. In this paper, the author makes an attempt to identify and critically analyze the implicit principles of legal regulation of relations in the field of collecting of data on a person. The author establishes the presence of at least three implicit principles that determine the current domestic regulation, namely: (1) "preventive protection of data on a person a priori ensures the protection of the data subjects' rights"; (2) "the protection of the data subjects' rights should be carried out mainly through public means"; (3) "the data subjects are reasonable, so that they should bear the burden of determining the future of their personal data." The identified principles are also critically analyzed by the author. As a result, the inconsistency and inefficiency of them in the modern context are established. The author concludes that it is necessary to conceptually reform the data collection regulation at a fundamental level, which should already be the subject of extensive discussions in the legal community. In addition, the author provides a number of recommendations on potential regulatory reform.*

**Keywords:** *legal regulation principles, digital transformation, datafication, data, data protection, information security, information law, computer security, big data, personal data, software, online data collection.*

## **Введение**

Неизбежно совершается цифровая трансформация общественной жизни<sup>2</sup>. Актуальные общесоциальные изменения выступают катализатором активного развития права России. Согласимся с А. Г. Кравченко в том, что парадигмальный сдвиг в праве объективен и неизбежен<sup>3</sup>. Это утверждение также верно и в отношении

<sup>2</sup> Полякова Т. А., Минбалеев А. В., Кроткова Н. В. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. 2020. № 5. С. 75—87.

<sup>3</sup> Кравченко А. Г. Сдвиг правовой парадигмы в эпоху цифровой экономики // Азиатско-Тихоокеанский регион: экономика, политика, право. 2022. Т. 24. № 1. С. 191.



информационного права, в частности правового, регулирования отношений в сфере данных о человеке<sup>4</sup>.

Сегодня цифровые технологии пронизывают всю нашу жизнь, в том числе приводят к ее датафикации<sup>5</sup>, в условиях которой данные собираются всегда и везде. При этом граждане сами (умышленно или по неосторожности) предоставляют значительные объемы данных третьим лицам.

Ключевой инициативой в рамках дискуссии о будущем регулирования сферы персональных данных выступает разработка концепции по защите цифровых прав граждан. Так, Советом при Президенте РФ по развитию гражданского общества и правам человека (СПЧ) был подготовлен Доклад «Цифровая трансформация и защита прав граждан в цифровом пространстве<sup>6</sup>», на основе которого был разработан проект концепции обеспечения прав и свобод человека и гражданина в цифровом пространстве Российской Федерации<sup>7</sup>. Указанный проект призван стать основой для дальнейшей разработки нормативных правовых актов России, регулирующих процессы развития цифрового пространства России посредством установления принципов, целей, задач и механизмов обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации на современном этапе научно-технологического развития данной сферы.

Принципы правового регулирования выступают неотъемлемой частью фундамента отдельных отраслей и институтов права. Некоторые правовые принципы прямо закреплены в действующих нормативных правовых актах, другие, пронизывая правовое регулирование, остаются неявными, скрытыми, поддающимися выявлению и исследованию только при анализе конкретных правовых норм. В настоящей работе нами предпринята попытка идентифицировать скрытые принципы правового регулирования отношений по автоматизированному сбору данных о человеке, а также осуществить критический анализ указанных принципов в современном контексте.

Актуальность исследуемого вопроса обусловлена «необходимостью гармонизации требований соблюдения прав и свобод человека и гражданина, требований научно-технологического и социально-экономического развития Российской

<sup>4</sup> Подробнее см., например: *Добробаба М. Б.* Квантовые коммуникации: перспективы правового регулирования // Вестник Университета имени О.Е. Кутафина. 2022. № 4 (92). С. 25—37; *Полякова Т. А., Минбалеев А. В., Бойченко И. С.* Цифровая трансформация: вызовы праву и векторы научных исследований // Информационное право. 2020. № 2. С. 46—48; *Холодная Е. В.* О перспективных направлениях правового регулирования в сфере технологии искусственного интеллекта // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 12 (64). С. 89—96; *Чубукова С. Г.* Информационная правосубъектность: цифровая трансформация // Информационное право. 2019. № 3. С. 24—28.

<sup>5</sup> *Hildebrandt M.* Law as Information in the Era of Data-Driven Agency // *The Modern Law Review*. 2016. Vol. 79. № 1. P. 5.

<sup>6</sup> IFAP.RU : общественное движение. 2021. URL: <https://ifap.ru/pr/2021/n211213a.pdf> (дата обращения: 11.12.2022).

<sup>7</sup> ROCIT.RU : региональная общественная организация. 2021. URL: <https://rocit.ru/uploads/4f68dc0a2487678a7675ad7589280277050b4004.docx?t=1639585614> (дата обращения: 11.12.2022).

Федерации, задач развития безопасного информационного пространства, защиты российского общества от деструктивного информационно-психологического воздействия, культурного развития граждан и роста человеческого потенциала Российской Федерации, обеспечения безопасности личности, общества и государства»<sup>8</sup>.

Целью настоящего исследования выступает обоснование необходимости концептуальной модернизации регулирования в сфере сбора данных о человеке на уровне принципов регулирования с учетом множества социальных, технологических и иных факторов. В результате нами выявлены и критически проанализированы неявные принципы регулирования в исследуемой сфере и даны рекомендации по их обновлению.

### Неявные принципы регулирования отношений по автоматизированному сбору данных о человеке

Регулирование в сфере персональных данных базируется на провозглашении необходимости охраны и защиты государством прав субъектов персональных данных. Указанная посылка следует из некоторых конституционных норм и закреплена в ст. 2 Закона о персональных данных<sup>9</sup>, согласно которой целью указанного Закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Аналогичным образом выражена и ценностная основа проекта концепции обеспечения прав и свобод человека и гражданина в цифровом пространстве Российской Федерации.

Первостепенность защиты прав и свобод граждан при обработке их персональных данных как принцип обусловлена историей формирования современного регулирования в сфере персональных данных. Проведя детальный исторический анализ этапов формирования указанного регулирования, Н. А. Дмитрик указывает, что «появлению законодательства о персональных данных способствовал страх. Орудием страха первоначально стали компьютерные технологии, которые правительства стали использовать для слежки за гражданами из страха перед террористами. И сразу же ответный страх общества, пережившего фашизм: раз технологии используются против свободы, следует ограничить использование технологий»<sup>10</sup>. Таким образом, исторически законодательство о персональных данных складывалось как инструмент противодействия стремительному развитию технологий, которые могут использоваться во вред субъектам данных.

Вместе с тем на практике российский законодатель акцентирует внимание на защите информации персонального характера в процессе ее сбора, т.е. самих

<sup>8</sup> Проект концепции обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации. С. 1—2.

<sup>9</sup> Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.

<sup>10</sup> Дмитрик Н. А. История, смысл и перспективы института персональных данных // Вестник гражданского права. 2020. № 3. С. 43—82.



данных о человеке, в отрыве от защиты прав субъектов персональных данных и их интересов. Данное обстоятельство также отмечают Л. К. Терещенко и О. И. Тиунов<sup>11</sup>. В результате де-факто существенный объем правил в сфере персональных данных призван обеспечить охрану самих данных, но не прав граждан. Так, основной акцент сделан российским законодателем именно на создании свода требований, при соблюдении которых в процессе сбора данных риски нарушений в сфере персональных данных будут минимальными.

Вместе с тем сегодня соблюдение указанных правил совершенно не исключает риски нарушения прав субъектов персональных данных как минимум по причине существования множества «внешних» угроз, например, рисков взлома информационных систем оператора третьими лицами, а также с учетом того, что операторы могут злоупотреблять своими правами и при формальном соблюдении требований законодательства наносить вред субъектам. Именно поэтому превентивность является формальной. На формальный характер действующего законодательства также указывает Н. А. Дмитрик<sup>12</sup>. Аналогичная ситуация имеет место и в иных юрисдикциях. Так, анализируя соответствующее законодательство Великобритании, А. К. Жарова заключает, что в Великобритании предпринимаются все меры для превентивной защиты персональных данных (путем установления обязанностей контролера данных по обеспечению их защиты)<sup>13</sup>.

Таким образом, принцип (1) может быть сформулирован так: «превентивная охрана данных о человеке априори обеспечивает охрану и защиту прав субъектов данных».

Формальная превенция нарушений в сфере персональных данных обуславливает наличие принципа (2): «защита прав субъектов персональных данных должна осуществляться посредством преимущественно публичных способов». В случае нарушения оператором регулирования в сфере персональных данных при сборе данных государство предоставляет преимущественно публичные способы защиты в отсутствие инструментов самостоятельной (частной) защиты и восстановления нарушенных прав субъектами персональных данных.

Как отмечает В. В. Долинская, в национальном праве преобладают меры публично-правового регулирования и административная ответственность в сфере персональных данных<sup>14</sup>. Н. А. Дмитрик, занимая радикальную позицию, указывает, что интересы субъектов персональных данных де-факто не защищаются, поскольку составы правонарушений в сфере персональных данных, предусмотренные КоАП РФ, являются формальными, т.е. само по себе нарушение установленных правил влечет ответственность независимо от наличия или отсутствия общественно опасных последствий. Аналогично формальными

<sup>11</sup> Терещенко Л. К., Тиунов О. И. Правовой режим персональных данных // Журнал российского права. 2014. № 12 (216). С. 43.

<sup>12</sup> Дмитрик Н. А. Указ. соч.

<sup>13</sup> Жарова А. К. Опыт правового обеспечения безопасности персональных данных (на примере Аргентины и Великобритании) // Информационное право. 2017. № 4. С. 16—27.

<sup>14</sup> Долинская В. В. Защита прав в сфере персональных данных в России и ЕС // Законы России: опыт, анализ, практика. 2019. № 9. С. 22—29.

являются и составы преступлений в сфере компьютерной безопасности, которые теоретически могут быть применены в случаях несанкционированного сбора данных<sup>15</sup>.

В свою очередь, субъект персональных данных фактически обладает лишь возможностью обращения в суд для возмещения морального вреда, однако размер соответствующей компенсации, как показывает практика, обычно незначителен. Вышеуказанные принципы (1) и (2) позволяют заключить, что российскому праву персональных данных свойствен патернализм.

Наконец, как в российском законодательстве, так и в иных правовых порядках (например, в рамках ЕС) установлена презумпция рациональности субъектов данных<sup>16</sup> и, как следствие, бремя определения судьбы данных возложено на самих субъектов — принцип (3): «субъекты данных являются разумными, в связи с чем они должны нести бремя определения судьбы своих персональных данных». При этом в данном контексте бремя принятия решений относительно своих персональных данных может интерпретироваться правоведами в положительном смысле — как «право на информационное самоопределение», подразумевающее возможность гражданина реагировать и влиять по своему желанию и в своих интересах на сбор своих данных или же с учетом этого выстраивать свою собственную жизнь<sup>17</sup>.

К. В. Нам отмечает, что наложение активных информационных обязанностей на операторов с санкционированием в случае их нарушения больших денежных штрафов призвано служить реальному содержательному наполнению права на информационное самоопределение<sup>18</sup>. Следовательно, правовед фактически подчеркивает неразрывную связь между принципами (1) и (3), поскольку формальное соблюдение установленных правил трактуется как благодатная почва для последующего рационального поведения граждан.

Таким образом, суммируя выявленные скрытые принципы действующего регулирования отношений в сфере сбора данных о человеке, в качестве ценностной основы соответствующего регулирования можно привести следующий тезис.

При постулировании необходимости защиты прав физических лиц закон направлен на создание условно безопасной для данных среды посредством возложения на операторов значительных обязанностей [принцип (1)], а на субъектов — бремени ответственности в вопросах распоряжения своими данными [принцип (3)], предоставляя им, в свою очередь, публично-правовые способы защиты (но не восстановления) прав [принцип (2)].

<sup>15</sup> Подробнее см.: Соловкин С. В. Проблемы ответственности за автоматизированный сбор (скрейпинг) данных в сети Интернет // Информационное право. 2022. № 3 (73). С. 35—38.

<sup>16</sup> Соловкин С. В. Значение парадокса приватности для законодательства о персональных данных в условиях становления общества наблюдения // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 4 (92). С. 112.

<sup>17</sup> Нам К. В. Особенности развития правового регулирования оборота и защиты персональных данных // Вестник гражданского права. 2020. Т. 20. № 5. С. 73—89.

<sup>18</sup> Нам К. В. Указ. соч.



### **Критический взгляд на неявные принципы регулирования отношений по автоматизированному сбору данных о человеке в современном контексте**

Охрана и защита государством прав граждан в сфере персональных данных, безусловно, чрезвычайно важны, поскольку отражают общую направленность соответствующего регулирования на создание условий информационной безопасности физических лиц и обеспеченности их прав. Представляется позитивным шагом, что при дальнейшем развитии регулирования в сфере персональных данных в России указанная направленность будет сохраняться.

Однако в контексте конкретных норм отечественного законодательства выясняется, что полноценное практическое воплощение данного принцип получает не всегда, в связи с чем, как указано выше, имеет место лишь постулирование необходимости защиты прав граждан в сфере персональных данных.

Сегодня неразвитым остается корпус норм в части определения прав субъектов в сфере сбора персональных данных, адекватных современным условиям, и соответствующих механизмов их обеспечения, охраны и защиты. Фактически отсутствует ясность в том, какие именно права в сфере сбора данных о человеке в современных условиях государство должно признавать и обеспечивать.

Таким образом, первая проблема состоит в отсутствии проработанности на законодательном уровне корпуса специальных информационных прав человека в сфере сбора персональных данных, которые якобы обеспечивает законодатель.

Кроме того, определение цели законодательства о персональных данных как обеспечение прав человека, среди которых отдельно выделено право на неприкосновенность частной жизни, размывает границы между специальными правами физических лиц в сфере персональных данных (в частности, по главе 3 Закона о персональных данных) в отдельности и между совокупностью указанных прав и конституционным правом на неприкосновенность частной жизни.

В действующем законодательстве недостаточно четко проведена граница между частной жизнью человека и сферой его персональных данных, что становится проблемой в условиях, когда практически любая информация, связанная с физическим лицом, может считаться его персональными данными<sup>19</sup>. Следовательно, не любое нарушение законодательства о персональных данных будет являться нарушением права на неприкосновенность частной жизни, что должно учитываться на законодательном уровне. Дополнительно необходимо определить и иные цифровые права граждан, как это предлагается в проекте концепции обеспечения прав и свобод человека и гражданина в цифровом пространстве России.

Что касается критерия превентивности охраны персональных данных, то на данный момент охрана действительно в разы эффективнее защиты, следующей за нарушением, ввиду нематериальной природы персональных данных и сложностей с действительным восстановлением нарушенных прав субъектов. Однако в условиях цифровой трансформации, когда персональными данными в

<sup>19</sup> *Purtova N.* The law of everything. Broad concept of personal data and future of EU data protection law // *Law, Innovation and Technology.* 2018. Vol. 10. № 1. P. 40—81.

определенных случаях может быть признана практически любая информация, так или иначе связанная с человеком<sup>20</sup>, наличие данного критерия может порождать существенные проблемы.

Во-первых, соблюдение операторами всех без исключения правил с учетом большого объема информации, потенциально являющейся персональными данными, рано или поздно станет чрезмерно обременительным, несмотря на существенные административные штрафы, установленные законом. В результате уровень соответствия правовым нормам может постепенно снижаться. Во-вторых, государству также будет сложнее осуществлять контроль за соблюдением правил, ведь у профильного госоргана (Роскомнадзора) будет отсутствовать объективная возможность отслеживать и рассматривать все случаи нарушения права персональных данных, что приведет к ускорению темпов игнорирования операторами отдельных, особо обременительных правил обработки.

Соответственно, другая проблема — это необоснованная в современных условиях избыточность требований, предъявляемых к операторам данных.

В данном контексте считаем необходимым на законодательном уровне: i) отказаться от презумпции «охрана персональных данных неизбежно влечет обеспеченность прав субъектов»; ii) отказаться от тенденции наращивания объемов «обременения» операторов обязанностями и требованиями; iii) перейти от формального постулирования необходимости защиты прав граждан к созданию совокупности эффективных правовых механизмов реализации данного принципа. В частности, необходимо определить совокупность актуальных информационных прав граждан в сфере персональных данных и предусмотреть действенные способы обеспечения, охраны и защиты именно таких прав, а не самих персональных данных.

В таком случае обновленный принцип (1) может быть сформулирован следующим образом: создание условий, в которых государством осуществляются эффективные обеспечение, охрана и защита конституционных и специальных информационных прав и свобод человека и гражданина в ситуациях сбора персональных данных, в том числе посредством обеспечения охраны персональных данных.

Анализируя принцип (2), отметим, что права человека и гражданина в сфере персональных данных в случае их нарушения не могут быть эффективно обеспечены в отсутствие законодательно разработанных действенных правовых средств восстановления нарушенных прав. В частности, до настоящего времени не внедрен предложенный в доктрине институт взыскания денежной компенсации, альтернативной убыткам и компенсации морального вреда<sup>21</sup>, или иной институт.

В данном контексте считаем необходимым на законодательном уровне разработать комплекс эффективных правовых механизмов, направленных на

<sup>20</sup> Подробнее см.: Соловкин С. В. Данные о человеке в цифровом мире: проблемы и парадоксы юридических дефиниций // Новые горизонты развития системы информационного права в условиях цифровой трансформации / Т. А. Полякова, А. В. Минбалева, В. Б. Наумов [и др.]. М.: Институт государства и права РАН, 2022. С. 346—352.

<sup>21</sup> Савельев А. И. На пути к концепции регулирования данных в условиях цифровой экономики // Закон. 2019. № 4. С. 174—195.



восстановление нарушенных цифровых прав в сфере персональных данных, в том числе внедрить институт взыскания компенсации в случае нарушения прав субъектов персональных данных, причинения им вреда. Обновленный принцип (2) может быть сформулирован следующим образом: предоставление государством совокупности различных способов защиты и восстановления нарушенных прав субъектов данных, а также механизмов привлечения нарушителей к ответственности.

Корректность принципа (3) также может быть поставлена под сомнение. Во-первых, само по себе постулирование рациональности субъектов персональных данных не соответствует актуальной социальной реальности<sup>22</sup>. Во-вторых, что более значимо, в современных условиях управление субъектами собственной приватностью становится все более затруднительным. Д. Солове указывает на существование множества когнитивных, структурных и системных проблем управления субъектами собственной приватностью<sup>23</sup>. Структурные и системные проблемы обусловлены современными технологическими особенностями обработки данных в цифровых средах. Указанные обстоятельства подчеркивают несостоятельность принципа (3).

### Заключение

В настоящей работе нами были выделены и критически проанализированы скрытые принципы, которые оказывают влияние на российское законодательство в сфере сбора данных о человеке.

В результате мы можем заключить, что современная законотворческая деятельность, будучи направленной на локальное решение отдельных проблем в сфере персональных данных, должна быть переориентирована на теоретическое, а затем и практическое, построение принципиально новой парадигмы регулирования сферы персональных данных с учетом множества социальных, технологических, экономических и иных факторов современности, а также цифровой трансформации в целом.

С одной стороны, безусловно, важной мерой является разработка СПЧ проекта концепции обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации, которая должна стать основой будущего нормативного правового массива, регулирующего отношения в сфере персональных данных в новых условиях.

С другой стороны, сохранение, концептуальная неизменность принципов регулирования с учетом их несовершенства, выявленного в рамках настоящего исследования, влечет за собой риск неэффективности будущего правового

<sup>22</sup> Соловкин С. В. Значение парадокса приватности для законодательства о персональных данных в условиях становления общества наблюдения // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 4 (92). С. 109—119.

<sup>23</sup> Solove D. J. Introduction: Privacy Self-Management and the Consent Dilemma // Harvard Law Review. 2013. Vol. 126. No. 7. P. 1880—1903.

регулирования, в связи с чем внимание законодателя должно быть обращено именно на проработку и модернизацию базовых подходов к правовому регулированию сферы персональных данных.

## БИБЛИОГРАФИЯ

1. *Дмитрик Н. А.* История, смысл и перспективы института персональных данных // Вестник гражданского права. — 2020. — № 3. — С. 43—82.
2. *Добробаба М. Б.* Квантовые коммуникации: перспективы правового регулирования // Вестник Университета имени О.Е. Кутафина. — 2022. — № 4 (92). — С. 25—37.
3. *Долинская В. В.* Защита прав в сфере персональных данных в России и ЕС // Законы России: опыт, анализ, практика. — 2019. — № 9. — С. 22—29.
4. *Жарова А. К.* Опыт правового обеспечения безопасности персональных данных (на примере Аргентины и Великобритании) // Информационное право. — 2017. — № 4. — С. 16—27.
5. *Кравченко А. Г.* Сдвиг правовой парадигмы в эпоху цифровой экономики // Азиатско-Тихоокеанский регион: экономика, политика, право. — 2022. — Т. 24. — № 1. — С. 184—194.
6. *Нам К. В.* Особенности развития правового регулирования оборота и защиты персональных данных // Вестник гражданского права. — 2020. — Т. 20. — № 5. — С. 73—89.
7. *Полякова Т. А., Минбалеев А. В., Бойченко И. С.* Цифровая трансформация: вызовы праву и векторы научных исследований // Информационное право. — 2020. — № 2. — С. 46—48.
8. *Полякова Т. А., Минбалеев А. В., Кроткова Н. В.* Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. — 2020. — № 5. — С. 75—87.
9. *Савельев А. И.* На пути к концепции регулирования данных в условиях цифровой экономики // Закон. — 2019. — № 4. — С. 174—195.
10. *Соловкин С. В.* Данные о человеке в цифровом мире: проблемы и парадоксы юридических дефиниций // Новые горизонты развития системы информационного права в условиях цифровой трансформации / Т. А. Полякова, А. В. Минбалеев, В. Б. Наумов [и др.]. — М. : Институт государства и права РАН, 2022. — С. 346—352.
11. *Соловкин С. В.* Значение парадокса приватности для законодательства о персональных данных в условиях становления общества наблюдения // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2022. — № 4 (92). — С. 109—119.
12. *Соловкин С. В.* Проблемы ответственности за автоматизированный сбор (скрейпинг) данных в сети Интернет // Информационное право. — 2022. — № 3 (73). — С. 35—38.
13. *Терещенко Л. К., Тиунов О. И.* Правовой режим персональных данных // Журнал российского права. — 2014. — № 12 (216). — С. 42—49.



14. *Холодная Е. В.* О перспективных направлениях правового регулирования в сфере технологии искусственного интеллекта // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2019. — № 12 (64). — С. 89—96.
15. *Чубукова С. Г.* Информационная правосубъектность: цифровая трансформация // Информационное право. — 2019. — № 3. — С. 24—28.
16. *Hildebrandt M.* Law as Information in the Era of Data-Driven Agency // The Modern Law Review. — 2016. — Vol. 79. — № 1. — P. 1—30.
17. *Purtova N.* The law of everything. Broad concept of personal data and future of EU data protection law // Law, Innovation and Technology. — 2018. — Vol. 10. — № 1. — P. 40—81.
18. *Solove D. J.* Introduction: Privacy Self-Management and the Consent Dilemma // Harvard Law Review. — 2013. — Vol. 126. — No. 7. — P. 1880—1903.

## Формирование цифровой среды доверия: динамика развития инфраструктуры идентификации при реализации цифровых услуг

**Аннотация.** Статья посвящена исследованию развития инструментов идентификации на современном этапе цифровой трансформации для формирования цифровой среды доверия. Автором использовались методы: построение гипотез, идеализация, правовое моделирование, сравнительный правовой метод. В результате автор приходит к следующим выводам: в условиях цифровой трансформации происходит активное распространение дистанционной модели работы, увеличение доли дистанционных сервисов и услуг в традиционном деловом обороте, а также их усложнение и масштабирование. В указанных условиях возникает необходимость в применении качественных решений по идентификации, способствующих формированию среды доверия в цифровом пространстве.

В статье исследуется динамика развития действующего законодательства в части идентификации, анализируются актуальные информационно-правовые механизмы реализации идентификации, существующие проблемы и тенденции применения при оказании дистанционных услуг и функций.

**Ключевые слова:** идентификация, инфраструктура идентификации, персональные данные, цифровое пространство, среда доверия, цифровая трансформация, цифровые услуги.



**Алексей Игоревич  
ХИМЧЕНКО,**

старший преподаватель  
кафедры информационного  
права и цифровых  
технологий Университета  
имени О.Е. Кутафина  
(МГЮА),  
кандидат юридических наук  
[alekseykhimchenko@  
yandex.ru](mailto:alekseykhimchenko@yandex.ru)  
125993, Россия, г. Москва,  
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2023.102.2.101-109

**ALEKSEY I. KHIMCHENKO,**

Senior lecturer of the Department  
of information law and digital technologies  
of the Kutafin Moscow State Law University (MSAL), Cand. Sci. (Law)  
[alekseykhimchenko@yandex.ru](mailto:alekseykhimchenko@yandex.ru)  
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

### Formation of a digital environment of trust: dynamics of development of identification infrastructure in the implementation of digital services

**Abstract.** The study focuses on the development of identification tools at the present stage of digital transformation for the formation of a digital environment of trust. The author used the following methods: hypothesis building, idealization, legal modeling, comparative legal method. The results obtained: In the conditions of digital transformation, there is an active spread of the

© Химченко А. И., 2023

*remote work model, an increase in the share of remote services and services in the traditional business turnover, as well as their complication and scaling. In these conditions, there is a need to apply high-quality identification solutions that contribute to the formation of an environment of trust in the digital space. The article examines the dynamics of the development of the current legislation in terms of identification, analyzes the current information and legal mechanisms for the implementation of identification, existing problems and trends in the provision of remote services and functions.*

**Keywords:** *information technology, digital environment of trust, legal regulation, information sovereignty, digital transformation, digital services, personal data, identification.*

**П**роцессы цифровой трансформации в системе государственного управления и системе публичной власти оказывают существенное влияние на всю инфраструктуру реализации технологических процессов. Формирование среды доверия реализации всего спектра общественных отношений в цифровом пространстве в указанных условиях становится приоритетной задачей.

Формирование цифровой среды доверия, являясь комплексной задачей, предполагает создание взаимосвязанного набора правовых, технологических и методологических решений для функционирования эффективных и безопасных средств дистанционного взаимодействия.

Указанной тематике, находящейся в фокусе государственного управления, с определенного момента стало уделяться достаточное внимание. Так, при разработке программы «Цифровая экономика Российской Федерации» к вызовам цифровой трансформации была отнесена проблема обеспечения доверия граждан к цифровой среде, при этом сформулирована задача формирования единой цифровой среды доверия для наделения участников цифровой экономики инструментами доверенных цифровых дистанционных коммуникаций.

В исследованиях отмечается, что даже в условиях современной активной цифровой трансформации проблематика удаленной идентификации длительное время не находила законодательного урегулирования, а институт дистанционной идентификации только начинает формироваться<sup>1</sup>.

Отдельный интерес вызывает исследование правового регулирования процессов использования дистанционных технологий<sup>2</sup>, и в то же время по результатам произошедших изменений в системе принудительной работы в дистанционном формате поднимается вопрос о доверии общества к праву в целом и его соответствующем авторитете<sup>3</sup>.

<sup>1</sup> Наумов В. Б. Задача обеспечения тайны идентификации в информационном праве // Мониторинг правоприменения. 2019. № 3 (32). С. 70—75.

<sup>2</sup> Полякова Т. А., Минбалеев А. В., Кроткова Н. В. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. 2020. № 5. С. 84.

<sup>3</sup> 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.

Таким образом актуальность поиска решений по формированию среды доверия в цифровом пространстве лишь повышается и становится непрерывной динамической задачей. При этом существующий уровень вызовов и угроз информационной инфраструктуры обуславливает критическую необходимость формирования среды доверия в информационном пространстве<sup>4</sup>.

### Текущие технологии идентификации (ЕСИА, ЕБС)

Технологии идентификации востребованы как при оказании традиционных государственных услуг и функций, так и при развитии структурных элементов цифровой экономики, реализации дистанционных форматов их функционирования.

В настоящее время основным механизмом, реализующим технологию удаленной идентификации, является единая система идентификации и аутентификации (ЕСИА), созданная в соответствии с постановлением 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»<sup>5</sup>.

Актуальной тенденцией развития института удаленной идентификации стало формирование механизмов на основе биометрических персональных данных.

Так, положениями Федерального закона от 31.12.2017 № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»<sup>6</sup> были созданы правовые основы для реализации удаленной идентификации граждан по биометрическим персональным данным.

Ключевое значение в этом процессе имеет Единая биометрическая система (ЕБС), которая в соответствии со ст. 14.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»<sup>7</sup> является государственной информационной системой, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица. ЕБС функционирует в целях повышения качества и доступности услуг в электронном виде, при этом регулирование порядка функционирования ЕБС осуществляется специальными требованиями законодательства.

До определенного момента специфика использования ЕБС ограничивалась использованием для открытия счетов и кредитования, обязательным условием

<sup>4</sup> Химченко А. И. О взаимосвязи вопросов обеспечения информационного суверенитета Российской Федерации и формирования цифровой среды доверия // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 4 (92). С. 90.

<sup>5</sup> СЗ РФ. 2011. № 49 (ч. V). Ст. 7284.

<sup>6</sup> СЗ РФ. 2018. № 1 (ч. I). Ст. 66.

<sup>7</sup> СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.



для работы с биометрическими данными при этом было наличие базовой банковской лицензии.

В дальнейшем положениями Федерального закона от 29.12.2020 № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»<sup>8</sup> были внесены временные поправки, направленные на развитие биометрических технологий, а отдельными нормативными актами в течение 2021 г. производилась детальная настройка соответствующего механизма биометрической идентификации (см., например, постановление Правительства РФ от 24.12.2021 № 2459 «О внесении изменений в постановление Правительства Российской Федерации от 8 июня 2011 г. № 451»<sup>9</sup>, постановление Правительства РФ от 23.10.2021 № 1815<sup>10</sup>, приказ Минцифры России от 10.09.2021 № 930<sup>11</sup>).

Новый этап в регулировании отношений, возникающих при осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных с помощью ЕБС начался с принятием Федерального закона от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации»<sup>12</sup> (далее — Закон).

Законом были закреплены понятия «аутентификация», «единая биометрическая система», «единая система идентификации и аутентификации», «идентификация», в том числе новые, такие как «вектор единой биометрической системы», «идентификатор», «мобильное приложение единой биометрической системы», «оператор регионального сегмента единой биометрической системы», «организации, осуществляющие аутентификацию на основе биометрических персональных данных физических лиц», «региональный сегмент единой биометрической системы».

Устанавливается, что ЕБС используется для осуществления идентификации и (или) аутентификации физических лиц государственными органами, органами местного самоуправления, Центральным банком РФ, банками, иными кредитными организациями, некредитными финансовыми организациями, субъектами национальной платежной системы, лицами, оказывающими профессиональные услуги на финансовом рынке, иными организациями, индивидуальными предпринимателями, нотариусами, а также в иных правоотношениях в случаях, установленных законодательством РФ.

При обработке биометрических персональных данных в единой биометрической системе, в том числе в ее региональных сегментах, их взаимодействии с иными информационными системами устанавливается необходимость применять организационные и технические меры по обеспечению безопасности персональных данных.

<sup>8</sup> СЗ РФ. 2021. № 1 (ч. I). Ст. 18.

<sup>9</sup> СЗ РФ. 2022. № 1 (ч. II). Ст. 166.

<sup>10</sup> СЗ РФ. 2021. № 44 (ч. III). Ст. 7423.

<sup>11</sup> Зарегистрирован в Минюсте России 28.10.2021 № 65621.

<sup>12</sup> URL: <http://pravo.gov.ru>, 29.12.2022.

В инфраструктуре ЕБС используются данные:

- изображение лица человека, полученное с помощью фотовидеоустройств;
- запись голоса человека, полученная с помощью звукозаписывающих устройств.

Также Законом устанавливается, что отказ физического лица от прохождения идентификации и (или) аутентификации с использованием его биометрических персональных данных не может служить основанием для отказа ему в оказании государственной, муниципальной или иной услуги, выполнении государственных, муниципальных функций, продаже товаров, выполнении работ или отказа в приеме на обслуживание. Законом также закрепляется набор прав гражданина, зарегистрированного на едином портале государственных услуг (ЕПГУ), в части персональных данных.

Законом установлен запрет на идентификацию и (или) аутентификацию физических лиц с использованием биометрических персональных данных, при которых необходима их трансграничная передача, за исключением аутентификации, осуществляемой аккредитованными госорганами или Центральным банком РФ в определенных случаях.

Кроме того, положениями Закона определен порядок размещения сведений в ЕБС и в единой системе идентификации и аутентификации (ЕСИА); региональных сегментах ЕБС; функции уполномоченного органа, осуществляющего регулирование в сфере идентификации и аутентификации физических лиц на основе биометрических данных, полномочия федеральных органов исполнительной власти и Центрального банка РФ, функции оператора ЕБС.

Также определен порядок осуществления идентификации и аутентификации с использованием ЕБС, использования ЕБС и ЕСИА при предъявлении документов, удостоверяющих личность физического лица.

Закреплен порядок осуществления идентификации и (или) аутентификации при проходе на территории организаций, обработке биометрических персональных данных вне ЕБС, аутентификации с использованием информационных систем организаций на основе биометрических персональных данных физических лиц, взаимодействия с ЕБС. Определены вопросы аккредитации организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц и государственного контроля (надзора) в сфере идентификации и (или) аутентификации.

При этом в Законе не урегулирован вопрос доступности инфраструктуры ЕБС для граждан с ограниченными физическими возможностями, в частности порядок действий инвалидов в ситуации, когда нет физической возможности сдачи образца голоса.

Отдельного внимания заслуживает вопрос признания юридической силы и правовых последствий аутентификации с использованием регионального сегмента ЕБС, поскольку в соответствии со ст. 11 Закона действия по идентификации и (или) аутентификации физического лица с использованием ЕБС и ЕСИА с соблюдением требований Закона, приравниваются к действиям по предъявлению документов, за исключением региональных сегментов ЕБС. Вопрос актуален в связи с использованием регионального сегмента ЕБС в рамках предоставления государственных и муниципальных услуг.



В целях определения стратегических направлений развития и совершенствования цифровых технологий идентификации и аутентификации на основе биометрических персональных данных в Российской Федерации, а также в целях обеспечения недискриминационного доступа к сервисам единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, постановлением Правительства РФ от 29.12.2022 № 2511<sup>13</sup> был образован Координационный совет по развитию цифровых технологий идентификации и аутентификации на основе биометрических персональных данных. К его полномочиям были отнесены определение стратегических направлений развития биометрических технологий в Российской Федерации и развития единой биометрической системы, а также подготовка предложений по их внедрению в различные сферы правоотношений.

*Новые решения. Мобильная электронная подпись «Госключ».* Активное распространение дистанционной модели работы, увеличение доли дистанционных сервисов и услуг в традиционном деловом обороте, а также их усложнение и масштабирование требуют разработки соответствующих актуальному уровню сервисов современных инфраструктурных решений.

Одним из таких решений является приложение «Госключ», представляющее собой мобильный формат подписания юридически значимых документов посредством использования электронной подписи.

«Госключ» реализует следующий технологический цикл:

- выпуск сертификата электронной подписи;
- отображение документа пользователю на экране мобильного телефона или планшета с возможностью детально изучить этот документ перед подписанием;
- подписание документов с помощью свежевывущенного сертификата электронной подписи или уже созданного пользователем ранее.

С использованием приложения генерируется сертификат усиленной неквалифицированной электронной подписи (Унэп) и усиленной квалифицированной электронной подписи (УКЭП), выбор которого зависит от вида получаемой услуги.

Для использования сервиса необходимы подтвержденная учетная запись на «Госуслугах», биометрический загранпаспорт нового поколения, смартфон с NFC-модулем.

Перед внедрением сервиса в постоянную эксплуатацию в соответствии с постановлением Правительства РФ от 15.07.2021 № 1207 в период с 20.07.2021 по 31.07.2022 проводился эксперимент по использованию усиленной электронной подписи при предоставлении услуг и осуществлении иных действий с использованием федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»<sup>14</sup>.

<sup>13</sup> URL: <http://pravo.gov.ru>, 31.12.2022.

<sup>14</sup> СЗ РФ. 2021. № 30. Ст. 5784.

В настоящее время посредством мобильного приложения «Госключ» может быть реализован следующий пользовательский функционал:

- дистанционная регистрация юридического лица или ИП. Порядок получения услуги описан в письме ФНС России от 22.07.2022 № КВ-4-14/9486@ «О реализации подписания документов в мобильном приложении Госключ»<sup>15</sup>;
- в рамках суперсервиса «Мое жилье» возможность отправки заявлений в Росреестр на исправление технической ошибки в данных ЕГРН (опечатка, грамматическая или арифметическая ошибка, допущенная органом регистрации прав при внесении сведений) полностью онлайн<sup>16</sup>;
- дистанционное заключение договора по купле-продаже транспортного средства полностью онлайн, с использованием мобильного приложения «Госключ», при этом он будет иметь ту же юридическую значимость, что и подписанный на бумаге<sup>17</sup>;
- дистанционное заключение договора с оператором мобильной связи;
- дистанционное заключение договора на платное обучение;
- кадровый электронный документооборот.

В рамках развития проекта для общественного обсуждения был опубликован проект<sup>18</sup> постановления Правительства, устанавливающий правовой статус Единой цифровой платформы подписания документов («Госключ») как подсистемы федеральной государственной информационной системы Единый портал государственных и муниципальных услуг (функций) (ЕПГУ).

Проект предусматривает закрепление как подсистемы ЕПГУ функционала платформы подписания, включающего возможность подписания заявителями, завершившими процедуру регистрации в единой системе идентификации и аутентификации (ЕСИА) заявлений, договоров и иных документов, подписание которых в электронной форме допускается в соответствии с законодательством РФ. Такие документы могут быть сформированы посредством ЕПГУ или получены из иных информационных систем, входящих в инфраструктуру электронного правительства.

Стоит отметить, что использование подобных решений может стать одним из эффективных механизмов повышения доверия в цифровой среде. Например, посредством мобильного приложения «Госключ» была реализована верификация аккаунта через ЕПГУ с отображением соответствующего статуса после прохождения процедуры подтверждения личности на платформе «Авито». Индикация статуса верификации повысила трафик через подтвержденные аккаунты<sup>19</sup>, снизилась вероятность мошенничества и недобросовестных действий, что способствует повышению доверия пользователей.

*Перспективные решения (видеопоток).* Развитие дистанционных сервисов и услуг обуславливает активный поиск возможностей расширения механизмов

<sup>15</sup> Официальные документы. № 29, 09.08.2022 (еженедельное приложение к газете «Учет, налоги, право»).

<sup>16</sup> URL: <https://digital.gov.ru> (дата обращения: 14.09.2022).

<sup>17</sup> URL: <https://гибдд.рф/> (дата обращения: 12.07.2022).

<sup>18</sup> URL: <https://regulation.gov.ru/projects#npa=134129/> (дата обращения: 06.12.2022).

<sup>19</sup> URL: <https://https://www.kommersant.ru/doc/5707565/> (дата обращения: 08.12.2022).



удаленной идентификации. Так, дорожная карта Банка России по развитию финансирования субъектов малого и среднего предпринимательства<sup>20</sup> предусматривает рассмотрение возможности проведения банками процедуры удаленной идентификации клиента посредством технологий видеопотока с проведением пилотирования инициативы в «регулятивной песочнице» Банка России.

Анализ международного опыта показывает, что регуляторы отдельных стран — участниц Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) уже допускают проведение идентификации посредством применения технологий видеопотока<sup>21</sup>.

Развитие технологий идентификации посредством видеопотока имеет большой потенциал для реализации в географически труднодоступных местах, а также повышения ее доступности для граждан с ограниченными физическими возможностями.

Процесс идентификации по видеопотоку может быть построен по модели идентификации при личном обращении — демонстрации паспорта и СНИЛС в процессе видеосеанса. Дополнительным методом повышения доверия к проводимой процедуре могут стать проверка на применение программ искажения изображения, применение маркировки для соответствующих операций при мониторинге, а также установление лимита возможных операций.

### Заключение

Стремительные процессы цифровой трансформации общественных отношений и сопутствующее развитие дистанционных сервисов и услуг требуют комплекса соответствующих правовых, технологических и методологических решений по развитию инфраструктуры идентификации. Создание, развитие и эксплуатация соответствующих инфраструктурных решений являются фундаментальным вопросом формирования среды доверия и залогом продуктивного и безопасного применения современных средств взаимодействия в цифровом пространстве.

<sup>20</sup> Дорожная карта Банка России по развитию финансирования субъектов малого и среднего предпринимательства, утв. приказом Банка России от 13.09.2018 № ОД-2387.

<sup>21</sup> Химченко А. И. Вопросы формирования цифровой среды доверия как структурного элемента в цифровизации государственного управления // Правовое государство: теория и практика. 2022. № 3 (69). С. 159—164.

## БИБЛИОГРАФИЯ

1. *Наумов В. Б.* Задача обеспечения тайны идентификации в информационном праве // Мониторинг правоприменения. — 2019. — № 3 (32). — С. 70—75.
2. *Полякова Т. А., Минбалеев А. В.* Понятие и правовая природа «цифровой зрелости» // Государство и право. — 2021. — № 9. — С. 107—116.
3. *Полякова Т. А., Минбалеев А. В., Кроткова Н. В.* Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. — 2020. — № 5. — С. 75—87.
4. Формирование системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе : монография / под общ. ред. Т. А. Поляковой ; Институт государства и права РАН. — М. ; Саратов : Амирит, 2022. — 332 с.
5. *Химченко А. И.* Вопросы формирования цифровой среды доверия как структурного элемента в цифровизации государственного управления // Правовое государство: теория и практика. — 2022. — № 3 (69). — С. 159—164.
6. *Химченко А. И.* О взаимосвязи вопросов обеспечения информационного суверенитета Российской Федерации и формирования цифровой среды доверия // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2022. — № 4 (92).
7. *Polyakova T. A., Naumov V. B., Minbaleev A. V.* Trust in the law during the digital transformation // Государство и право. — 2022. — № 11. — С. 139—147.





**Арина Сергеевна  
СЕЛЮК,**

ассистент кафедры  
информационного права  
и цифровых технологий  
Университета имени  
О.Е. Кутафина (МГЮА)  
[arina\\_selyuk@mail.ru](mailto:arina_selyuk@mail.ru)  
125993, Россия, г. Москва,  
ул. Садовая-Кудринская, д. 9

## Защита персональных данных в цифровом пространстве

**Аннотация.** Защита персональных данных представляет собой одну из наиболее важных задач на современном этапе развития государства. Эта необходимость определяется цифровизацией, переходом большинства видов деятельности человека в цифровое пространство, а также увеличением численности кибератак и утечек персональных данных в цифровой среде. Цель исследования заключалась в анализе причин и условий повышенных рисков в отношении персональных данных, анализе действующего законодательства РФ в части системы защиты персональных данных в цифровой среде, анализе соответствующего опыта зарубежных стран. В статье определены основные проблемы защиты персональных данных в цифровом пространстве, а также основные направления, требующие совершенствования для обеспечения защиты персональных данных. **Ключевые слова:** персональные данные, цифровая среда, Интернет, цифровизация, киберпреступность, фишинг.

DOI: 10.17803/2311-5998.2023.102.2.110-119

**ARINA S. SELYUK,**

Assistant of the Department of information law  
and digital technologies  
of the Kutafin Moscow State Law University (MSAL)  
[arina\\_selyuk@mail.ru](mailto:arina_selyuk@mail.ru)  
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

### Protection of Personal Data in the Digital Space

**Abstract.** The protection of personal data is one of the most important tasks at the present stage of the development of states. This need is determined by digitalization, the transition of most human activities into the digital space, as well as an increase in the number of cyber-attacks and leaks of personal data in the digital environment. The purpose of the study was to analyze the causes and conditions of increased risks in relation to personal data, to analyze the current legislation of the Russian Federation regarding the system of personal data protection in the digital environment, to analyze the experience of foreign countries in relation to this issue. The article draws conclusions about the main problems of personal data protection in the digital space, and also identifies the main areas that require improvement to ensure the protection of personal data.

**Keywords:** personal data, digital environment, Internet, digitalization, cybercrime, phishing.

Права человека — ценностный ориентир для большинства демократических государств, в том числе и для России. Сегодня понятие личных прав, которые должны быть гарантированы государством и защищены соответствующими государственными институтами, значительно расширен. Конституция РФ в ст. 23 устанавливает, что каждому гарантируется право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей части и доброго имени<sup>1</sup>.

Какие-либо произвольные ограничения указанных прав недопустимы, за исключением установленных законодательством случаев. Понятие права на неприкосновенность частной и личной жизни включает в себя и возможность пользоваться и распоряжаться своими персональными данными<sup>2</sup>. С переходом к цифровой экономике, расширением сети Интернет, цифровизации общества вопросы охраны и защиты персональных данных, в частности их защита в цифровой среде, становятся все более актуальными, что обусловлено сложностями самой цифровой среды, под которой все чаще понимается информационно-телекоммуникационная сеть Интернет.

Понятие персональных данных закреплено в Федеральном законе «О персональных данных» № 152-ФЗ от 27.07.2006 (далее — Закон о персональных данных): «персональные данные — это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»<sup>3</sup>. При этом доктринальные источники определяют персональные данные как особый институт охраны права на неприкосновенность частной жизни, как информационный ресурс ограниченного доступа<sup>4</sup>.

Закон о персональных данных определяет персональные данные как конфиденциальную информацию, что следует из положений о доступе к такой информации, особенностей ее распространения. Закон устанавливает обязанности операторов персональных данных по соблюдению требований к их сбору, обработке и распространению, а также закрепляет необходимость формирования системы защиты персональных данных в Российской Федерации.

Однако заложенная российским законодателем система защиты и оборота персональных данных в условиях цифровизации сталкивается с проблемами самой цифровой среды — сети Интернет.

Сегодня, как отмечают многие исследователи, происходит цифровая трансформация (цифровая революция), реализуемая в трех основных этапах:

- ИТ (интернет вещей);
- Big Data (большие данные);
- AI (искусственный интеллект)<sup>5</sup>.

<sup>1</sup> Конституция Российской Федерации // URL: [http://pravo.gov.ru/proxy/ips/?doc\\_itself=&nd=102027595&ysclid=ld7mdb65j8554953653#10](http://pravo.gov.ru/proxy/ips/?doc_itself=&nd=102027595&ysclid=ld7mdb65j8554953653#10) (дата обращения: 17.01.2023).

<sup>2</sup> Сычева М. И. Проблемы правового регулирования защиты персональных данных в сети Интернет // Международный журнал гуманитарных и естественных наук. 2022. № 10–3 (73). С. 175.

<sup>3</sup> Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Российская газета. 29.07.2006. № 165.

<sup>4</sup> Бачило И. Л. Информационное право : учебник для магистров 3-е изд., перераб. и доп. М. : Юрайт, 2015.

<sup>5</sup> Сибел Т. Цифровая трансформация. Как выжить и преуспеть в новую эпоху. М. : Манн, Иванов и Фербер, 2021. С. 5—15.



На современном этапе развития можно однозначно сказать о применимости трех уровней, так как в большинстве стран мира модернизируется законодательство, а также рассматриваются статус и положение искусственного интеллекта, особенности его применения в финансовых услугах и цифровом пространстве.

Цифровая среда представляет собой информационное пространство, в котором информация может распространяться неограниченно, предполагается простота копирования информации, возможность хранения информации без материального носителя. И основная сложность — невозможность наложить какие-либо юрисдикционные границы на цифровую среду. Соответственно, наиболее важным аспектом данной проблемы выступает необходимость согласованного международного подхода к регулированию оборота персональных данных в цифровой среде.

Эти вопросы в доктрине нередко поднимаются исследователями. Справедливой и обоснованной представляется позиция, согласно которой в современных реалиях цифровое пространство нерегулируемо расширяется, что ведет к господству «цифровой» эры, где право на защиту персональных данных должно быть приравнено к фундаментальным правам и свободам человека<sup>6</sup>.

В последние годы нарастает тенденция к фиксации случаев утечек персональных данных граждан в сеть Интернет, когда любой злоумышленник может воспользоваться конкретной информацией о гражданине. При этом не имеет значения — были ли использованы данные гражданина для совершения противоправных действий (например, кражи денежных средств со счета по составам мошенничества) либо же была совершена кража персональных данных без их последующего использования. Чаще всего такие данные собираются в специальную базу данных и впоследствии хранятся с целью их возможной будущей перепродажи.

Кража данных представляет собой незаконную передачу или хранение личной, конфиденциальной и финансовой информации<sup>7</sup>.

В 2022 г. фиксировалось рекордное количество утечек персональных данных из крупнейших компаний, осуществляющих свою деятельность в удаленном формате («Яндекс.Еда», Delivery Club, «Гемотест», СДЭК)<sup>8</sup>. Базы персональных данных содержали в себе информацию о пользователях, адресе их проживания, телефонных номерах, а также некоторую банковскую информацию. Данные Роскомнадзора также подтверждают, что с сентября 2022 г. было получено порядка 100 уведомлений от компаний об утечках персональных данных пользователей<sup>9</sup>.

Увеличение случаев утечек персональных данных по большей части неразрывно связано с тенденциями к построению информационного общества,

<sup>6</sup> *Абрамова А. Г.* Международно-правовая защита персональных данных в сети Интернет: общие положения // Регион и мир. 2020. Т. 11. № 5. С. 52.

<sup>7</sup> Что такое кража данных и как ее избежать? // URL: <https://www.kaspersky.ru/resource-center/threats/data-theft?ysclid=ld7atap1ar727360244> (дата обращения: 17.01.2023).

<sup>8</sup> 14 компаний, откуда утекли данные пользователей в 2022 году // URL: <https://www.sravni.ru/text/14-kompanij-otkuda-utekli-dannye-polzovatelej-v-2022-godu/> (дата обращения: 18.01.2023).

<sup>9</sup> В Роскомнадзор с сентября поступило порядка 100 уведомлений от компаний об утечках данных // URL: <https://tass.ru/ekonomika/16838265> (дата обращения: 19.01.2023).

повсеместной цифровизацией, а также распространением финансовых технологий, что получило еще более ускоренное развитие в результате пандемии и перехода компаний на предоставление услуг в онлайн-формате. Конечно, переход к предоставлению услуг онлайн дает немало преимуществ для потребителей и компаний — простоту получения услуг для одних, капитализацию и расширение масштабов бизнеса для других.

Однако широкие возможности в рамках предоставления удаленно услуг и товаров неуклонно ведут к коммерциализации персональных данных, а также их краже. При этом законодательство не успевает за развитием способов кражи персональных данных, что позволяет говорить о наличии пробелов в регулировании защиты персональных данных. Это также подтверждается данными о состоянии преступности в Российской Федерации за январь — ноябрь 2022 г.

Так, согласно данным МВД России, было зарегистрировано более 470 тысяч преступлений с использованием информационных технологий, при этом раскрыто менее 130 тысяч<sup>10</sup>. Соответственно, наблюдается низкая степень раскрываемости преступлений в сфере использования информационных технологий.оборот персональных данных в сети Интернет позволяет относить посягательства на целостность такой информации к категории преступлений, совершенных посредством использования информационных технологий.

Поэтому справедливым будет указать и тот факт, что подобные преступления, а равно противоправные действия в отношении персональных данных (т.е. их кража), обладают высокой степенью латентности.

Таким образом, можно выделить следующие тенденции противоправной деятельности в отношении персональных данных:

- потерпевшие (лица, чьи персональные данные были украдены, распространены без получения соответствующего согласия) зачастую могут не знать о факте краже их персональных данных. К примеру, без должного освещения СМИ случаев утечки персональных данных крупных фирм граждане не смогут узнать о том, что их персональные данные утекли в Сеть;
- низкая степень раскрываемость киберпреступлений в отношении персональных данных, так как для органов следствия наиболее сложными и проблемными являются методы расследования таких преступлений, а также поиск виновного лица. Данные обстоятельства осложняются тем, что если кража персональных данных выступает в качестве основной задачи для преступников, то чаще формируются преступные группы или сообщества, а также используются технические средства для сокрытия цифровых следов;
- фиксация и анализ цифровых следов, которые могут обнаружить органы следствия;
- отсутствие необходимой нормативной базы для эффективного обеспечения защиты персональных данных в цифровой среде.

В рамках национального правового поля все чаще выдвигаются инициативы по установлению штрафов для компаний за утечку персональных данных. Подобная

<sup>10</sup> Краткая характеристика состояния преступности в Российской Федерации за январь — ноябрь 2022 года // URL: <https://мвд.рф/reports/item/34307225/> (дата обращения: 18.01.2023).



инициативы высказало в декабре 2022 г. Минцифры России, однако законопроект не нашел одобрения среди субъектов бизнеса, так как штрафные санкции, предлагаемые государством, являются для них несоразмерными<sup>11</sup>.

В значительной степени сложности таких инициатив связаны с критерием повторности утечек персональных данных, за которые, согласно предложениям Минцифры, предусматривается более жесткая юридическая ответственность, так как уже после первой утечки персональных данных информация о пользователях будет храниться в цифровой среде, что не позволяет корректно определить, был ли факт повторной утечки или же распространение персональных данных основано на первой зафиксированной утечке.

Однако все же российское законодательство модернизируется с учетом современных реалий. В Федеральном законе от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон “О персональных данных”» закреплены положения о необходимости получения согласия на обработку персональных данных отдельно от иных согласий, которые могут запрашиваться со стороны компании, а также необходимость указания в данном согласии пункта о том, что лицо, соглашаясь с условиями, также согласно на распространение персональных данных. Без такого условия оператор персональных данных не обладает правом на распространение персональных данных<sup>12</sup>.

Основная проблема данного нововведения заключается в том, что указанные положения не имеют обратной силы, соответственно, даже при условии отзыва согласия на обработку и распространение персональных данных полученные ранее оператором персональные данные уже находятся в базе, а следовательно, могут выступать предметом преступных посягательств. Также отсутствуют и сам механизм, и требования для отзыва согласия на прекращение использования и распространения персональных данных.

Помимо этого, в сентябре 2022 г. также вступили в силу поправки, которые направлены на усиление системы защиты персональных данных путем закрепления обязанности оператора персональных данных сообщать уполномоченным органам об утечках персональных данных в течение суток, а в течение трех суток — о результатах внутренней проверки факта утечки персональных данных.

В современных условиях повышенных киберрисков национальное законодательство также пытается на них реагировать. Так, было принято постановление Правительства РФ от 16.01.2023 № 24 «Об утверждении Правил принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан»<sup>13</sup>. Данный акт устанавливает следующие ситуации запрета трансграничной передачи персональных данных:

<sup>11</sup> Минцифры задумало ввести штрафы за утечки данных до 500 млн рублей // URL: [https://www.rbc.ru/technology\\_and\\_media/26/12/2022/63a8f2999a79471e4e7c3968?ysclid=ld7atg60px644919802](https://www.rbc.ru/technology_and_media/26/12/2022/63a8f2999a79471e4e7c3968?ysclid=ld7atg60px644919802) (дата обращения: 19.01.2023).

<sup>12</sup> Российская газета. 11.01.2021. № 1.

<sup>13</sup> URL: <http://publication.pravo.gov.ru/document/view/0001202301170011> (дата обращения: 20.01.2023).

- если органами власти иной юрисдикции не принимаются меры по защите передаваемых персональных данных;
- юридическое лицо, которое относится к иной юрисдикции, входит в список запрещенных на территории России организаций;
- юридическое лицо иной юрисдикции относится к категории нежелательных организаций на территории России;
- трансграничная передача персональных данных не соответствует целям их сбора.

Что касается цифрового пространства, то в Российской Федерации имеется соответствующая нормативная основа для обеспечения защиты персональных данных в сети Интернет. Так, защита лиц от мошеннических действий в Интернете реализуется в соответствии с Федеральным законом «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ (далее — Закон об информации)<sup>14</sup>. Данный акт не только раскрывает понятие информационно-телекоммуникационной сети (т.е. сети Интернет), но и регулирует вопросы системы сертификации, разработки программ по защите информации, а также внедрения усовершенствованных систем аутентификации пользователей на различных сервисах.

Однако указанные акты — Закон о персональных данных и Закон об информации не формируют необходимой и совершенной системы защиты, которая отвечала бы требованиям развития самих информационных технологий (в том числе в контексте развития средств и способов воздействия со стороны злоумышленников на персональные данные), а также требованиям полной информационной безопасности каждого пользователя. В этой связи справедливым является мнение, согласно которому разработка инновационных методов защиты — это наиболее приоритетное направление развития для всего мира<sup>15</sup>.

В современных условиях существует несколько моделей реализации умысла по краже персональных данных:

- 1) социальная инженерия. Чаще всего социальная инженерия реализуется в форме фишинга, когда злоумышленник представляется доверенным лицом и путем обмана (в том числе создания поддельных сайтов, рассылки) осуществляет кражу данных непосредственно у лица (субъекта персональных данных). Наиболее распространена в составах мошенничества;
- 2) использование ненадежных способов защиты персональных данных. В данном случае можно говорить не только о фактах пробелов в системе информационной безопасности компании, но и об использовании ненадежных способов защиты самим клиентом (например, использование простых паролей и др.), что может быть обусловлено низким качеством информационно-просветительской работы по вопросам защиты персональных данных;

<sup>14</sup> Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» // Российская газета. 29.07.2006. № 165.

<sup>15</sup> Шарыпова Т. Н., Пунга К. В. Интернет-мошенничество: защита персональных данных от фишинга // Modern Science. 2022. № 5–3. С. 216.



- 3) использование для обработки персональных данных технологий искусственного интеллекта<sup>16</sup>. Это позволяет быстрее и эффективнее осуществлять обработку персональных данных, но при этом искусственный интеллект также создает повышенную уязвимость системы;
- 4) кадровые риски. Данная модель реализуется посредством использования должностным лицом своих полномочий по доступу к базе персональных данных и их последующей кражи.

Относительно последней модели реализации умысла по краже персональных данных необходимо отметить, что в практике российских судов нередко встречаются споры, касающиеся того, что должностное лицо информационной компании или компании по предоставлению связи, имея, согласно своим должностным полномочиям, доступ к персональным данным пользователей, осуществляет воздействие на эти данные, кражу или же использует эти данные без получения соответствующего согласия со стороны граждан<sup>17</sup>.

Соответственно, формирование системы защиты персональных данных в первую очередь должно обеспечиваться посредством внутренних механизмов защиты (например, использования высокотехнологичного программного обеспечения, создания внутренних должностных инструкций, стандартов). Такие внутренние меры по защите персональных данных должны коррелироваться с правовыми основами, которые также закрепляют стандарты для обеспечения эффективной защиты персональных данных в цифровой среде.

В контексте формирования в России эффективной правовой среды для защиты персональных данных, а также учета существенных характеристик цифрового пространства (трансграничность и отсутствие возможности для установления юрисдикции в отношении сети Интернет), интересно рассмотреть зарубежного опыта защиты персональных данных. На данном уровне регулирования имеются достаточно интересные практики по защите персональных данных в Европейском союзе во взаимосвязи с Международным союзом электросвязи (МСЭ).

В ЕС был принят регламент GDPR, целью которого является укрепление прав субъектов персональных данных<sup>18</sup>. Данный акт предполагает установление ответственности за несоблюдение правил хранения и обработки персональных данных, раскрывает терминологическую основу — понятия персональных данных, обработки персональных данных, ограничения персональных данных, контроллера, процессора персональных данных.

<sup>16</sup> Минбалеев А. В., Филоненкова В. А. Проблемы защиты персональных данных и цифрового профиля человека в сети Интернет в условиях пандемии // Вестник Южно-Уральского государственного университета. Серия : Право. 2020. Т. 20. № 3. С. 89.

<sup>17</sup> См., например: приговоры Советского районного суда г. Владивостока № 1-277/2020 от 30.07.2020 по делу № 1-277/2020 // URL: <https://sudact.ru/regular/doc/4AyuDmz7J9oX/?ysclid=Id7r658k9780709119> ; Октябрьского городского суда № 1-243/2020 от 29.07.2020 по делу № 1-243/2020 // URL: <https://sudact.ru/regular/doc/eLKpELsMEF5w/?ysclid=Id7r7grw9p48969269> ; Шиманского районного суда № 1-2/2019 1-2/2020 1-30/2018 от 05.11.2020 по делу № 1-2/2019 // URL: <https://sudact.ru/regular/doc/r4h59Cvexoln/?ysclid=Id7r88hq5t802523738> (дата обращения: 20.01.2023).

<sup>18</sup> URL: <https://gdpr.eu> (дата обращения: 20.01.2023).

Сравнивая данные положения с национальным законодательством, хочется отметить, что законодательство ЕС более детально раскрывает субъектный состав при обороте персональных данных. Более того, регламент GDPR закрепляет такие основополагающие принципы для сферы обработки персональных данных, как законность, справедливость и прозрачность, сбор и обработка для законных целей, адекватность и релевантность персональных данных целям обработки, хранение персональных данных в соответствующей форме.

Принципы, закрепленные GDPR, не являются абстрактными, а приближены к реальным и практическим условиям. Интересным подходом ЕС является установление такой правовой категории, как «право на забвение», т.е. возможность удаления данных пользователя из поисковой выдачи по требованию субъекта персональных данных, в том числе путем отзыва согласия на обработку персональных данных.

В рамках ЕС различаются понятия сбора и использования персональных данных. Если обращаться к практике МСЭ, то можно отметить, что в первую очередь организация ориентируется на стандартизацию и выдачу рекомендаций относительно защиты персональных данных, а также применения законодательства, в том числе GDPR.

В зарубежных странах защита персональных данных в значительной степени реализуется на внутреннем уровне — посредством предоставления пользователям пользовательских соглашений, в которых указываются права и обязанности сторон<sup>19</sup>. Более того, на многих интернет-платформах (в том числе в социальных сетях) реализуются собственные программы по защите пользователей от кражи персональных данных (Facebook, YouTube, различные поисковые системы и браузеры). Представляется, что некоторая степень саморегулирования в контексте защиты персональных данных пользователей имеет место, так как основная задача информационных порталов и платформ — это предоставление защищенной системы, которая функционирует на законодательных стандартах обеспечения безопасности пользовательских данных.

Логичным является вопрос определения правовой и функциональной возможности создания условий для «абсолютной» защиты персональных данных. Теоретически эта возможность может быть реализована только при условии, что существуют технические способы такой защиты<sup>20</sup>. Однако представляется, что все же невозможно реализовать эффективную и постоянную систему защиты — и техническим организациям (разработчикам софта, ПО), и законодателю необходимо будет реагировать на любые технические изменения, в том числе на механизмы и способы воздействия со стороны преступников на информацию. Более того, трансграничность сети Интернет предполагает установление общих международных стандартов для формирования систем защиты персональных данных, что на сегодняшний день труднореализуемо.

<sup>19</sup> Гонтарь Л. О. Защита персональных данных в условиях развития интернет-компаний: международно-правовое регулирование vs саморегулирование // Труды по интеллектуальной собственности. 2021. Т. 37. № 1–2. С. 134.

<sup>20</sup> Дмитриева Е. Г. Проблемы защиты персональных данных в цифровом мире и пути их решения // Право и бизнес. 2021. № 3.



Таким образом, подводя итог, можно сказать, что проблема защиты персональных данных является одной из наиболее актуальных в современных условиях. Для России ее актуальность связана с увеличением количества преступных воздействий на персональные данные, отсутствием необходимого уровня технологической независимости, что неоднократно отмечалось на протяжении 2022 г. Центральным банком РФ, а также со сложностями в разработке отечественного программного обеспечения и технологий после ухода с российского рынка большинства иностранных компаний, в том числе информационных и технологических.

Предполагается, что формирование системы защиты персональных данных в цифровой среде должно осуществляться на двух уровнях: государственном (путем принятия нормативных правовых актов) и на уровне организаций. При этом его должен сопровождать следующий комплекс мер:

- 1) реализация государством просветительской функции в части защиты персональных данных<sup>21</sup> в целях ознакомления граждан с положениями законодательства, основными рисками утечки персональных данных и способами самостоятельной защиты своих персональных данных;
- 2) развитие частных инициатив по защите персональных данных, что прямо коррелируется с необходимостью построения независимой экономики и технологической независимости в России. Это также предполагает и применение дополнительных мер — налоговых, административных для снижения давления на субъекты, занимающиеся разработкой программного обеспечения и информационных систем для защиты персональных данных пользователей;
- 3) формирование внутренних должностных инструкций и стандартов, а также проведение просветительских мероприятий относительно юридической ответственности за нарушения уголовного и административного законодательства в отношении персональных данных с использованием своего должностного положения;
- 4) формирование способов и механизмов внесудебной защиты персональных данных в случае обнаружения утечек;
- 5) уведомление граждан о факте утечек, что дополняло бы обязанность операторов персональных данных сообщать уполномоченным органам о факте утечки персональных данных;
- 6) формирование системы внешнего расследования случаев утечки персональных данных.

<sup>21</sup> Герасимова Н. А. Проблемы защиты персональных данных в сети Интернет // Актуальные проблемы науки и практики : Гатчинские чтения — 2020 : сборник научных трудов по материалам VII Международной научно-практической конференции. Гатчина, 22 мая 2020 г. Гатчина : Государственный институт экономики, финансов, права и технологий, 2020. Т. 2. С. 80.

## БИБЛИОГРАФИЯ

1. *Абрамова А. Г.* Международно-правовая защита персональных данных в сети Интернет: общие положения // Регион и мир. — 2020. — Т. 11. — № 5. — С. 51—58.
2. *Бачило И. Л.* Информационное право : учебник для магистров. — 3-е изд., перераб. и доп. — М. : Юрайт, 2015. — 564 с.
3. *Герасимова Н. А.* Проблемы защиты персональных данных в сети Интернет // Актуальные проблемы науки и практики : Гатчинские чтения — 2020 : сборник научных трудов по материалам VII Международной научно-практической конференции. Гатчина, 22 мая 2020 г. — Гатчина : Государственный институт экономики, финансов, права и технологий, 2020. — Т. 2. — С. 78—80.
4. *Гонтарь Л. О.* Защита персональных данных в условиях развития интернет-компаний: международно-правовое регулирование vs саморегулирование // Труды по интеллектуальной собственности. — 2021. — Т. 37. — № 1–2. — С. 116—140.
5. *Дмитриева Е. Г.* Проблемы защиты персональных данных в цифровом мире и пути их решения // Право и бизнес. — 2021. — № 3.
6. *Минбалеев А. В., Филоненкова В. А.* Проблемы защиты персональных данных и цифрового профиля человека в сети Интернет в условиях пандемии // Вестник Южно-Уральского государственного университета. — Серия : Право. — 2020. — Т. 20. — № 3. — С. 89—94.
7. *Сибел Т.* Цифровая трансформация. Как выжить и преуспеть в новую эпоху. — М. : Манн, Иванов и Фербер, 2021.
8. *Сычева М. И.* Проблемы правового регулирования защиты персональных данных в сети Интернет // Международный журнал гуманитарных и естественных наук. — 2022. — № 10–3 (73). — С. 175—178.
9. *Шарыпова Т. Н., Пунга К. В.* Интернет-мошенничество: защита персональных данных от фишинга // Modern Science. — 2022. — № 5–3.





**Кирилл Сергеевич  
ЕВСИКОВ,**

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

## К вопросу о правовом регулировании интернет-голосования

**Аннотация.** В статье рассмотрены особенности регулирования интернет-голосования. Исследование позволяет говорить, что органы публичной власти часто стремятся ограничить доступ граждан к данному способу участия в управлении делами государства, ссылаясь на технические и юридические барьеры. Рассмотренный в статье зарубежный опыт и опыт дистанционного электронного голосования в нашей стране позволяет опровергнуть ссылку на наличие значимых технических барьеров для интернет-голосования. Барьеры правового характера, как показывают результаты исследования, также могут быть преодолены путем изменения соответствующих правовых норм.

Одновременно отмечается, что интернет-голосование востребовано не только в публично-правовой, но и в частноправовой сферах. В связи с этим обоснована гипотеза о необходимости открытия доступа к технологии интернет-голосования, сертифицированного государством, для субъектов частного права. Реализация этого предложения будет способствовать росту доверия к информационным технологиям, повышению компетенций у широкого круга лиц и, как следствие, гармонизации цифровой трансформации избирательного процесса с существующей правовой концепцией.

Зарубежный опыт показал, что интернет-голосование сталкивается с множеством правовых барьеров. Юридическая наука при этом должна формировать пути преодоления подобных коллизий. Вариант устранения барьеров проанализирован в статье на примере института тайного голосования. Аналогичным образом Российская Федерация сможет преодолеть «цифровой» неолуддизм в области цифровизации государственного управления вообще и в сфере интернет-голосования в частности.

**Ключевые слова:** интернет-голосование, тайное голосование, цифровая трансформация избирательной системы, цифровизация государственного управления, цифровое голосование, цифровое государство, цифровое право, «цифровой» неолуддизм, электронная демократия, электронное голосование, электронное государство.

DOI: 10.17803/2311-5998.2023.102.2.120-128

**KIRILL S. EVSIKOV,**

*Associate professor of the Department of information law and digital technologies  
of the Kutafin Moscow State Law University (MSAL),  
Cand. Sci. (Law), Associate professor  
aid-ltd@yandex.ru  
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993*

### On the Issue of Legal Regulation of I-Voting

**Abstract.** *The article discusses the specific features of legislative regulation of i-voting. The study shows that public authorities often seek to restrict citizens' access to this method of participation in government referring to technical and legal barriers to its use. The foreign experience considered in the article and the experience of remote e-voting in our country allows us to refute the reference to the presence of significant technical barriers to i-voting. Legal barriers, as the results of the study show, can also be overcome by changing the relevant legal norms.*

*At the same time, it is noted that i-voting is in demand not only in public law, but also in private law. In this regard, the hypothesis of the need to open access to i-voting technology for subjects of private law is substantiated. The implementation of this proposal will help to increase confidence in the information system, increase the competencies of a wide range of people, and as a result, harmonize the digital transformation of the electoral process with the existing legal culture.*

*The studied experience has shown that in the course of digital transformation, i-voting will face many technical and legal problems. At the same time, legal science should form an understanding of these difficulties, as well as proposals for their neutralization and overcoming. This is the only way for the Russian Federation to defeat «digital neo-luddism» in the field of digitalization of public administration in general and in the field of i-voting in particular.*

**Keywords:** *digital neo-Luddism, digital law, digital voting, digital government, e-democracy, e-government, electoral system digital transformation, e-voting, i-voting, public administration digitalization, secret ballot.*

**3**аконы представляют собой совокупность юридически значимых решений, принятых путем голосования, которое проходит либо на референдуме, либо в парламенте, состав которого также определяется голосованием. В Российской Федерации жители многоквартирного дома голосуют за выбор управляющей компании, компаньоны — за создание юридического лица, присяжные заседатели — за вердикт, жители муниципального образования — за решение вопросов местного значения. Конституция РФ принята всенародным голосованием 12.12.1993, а изменения одобрены в ходе общероссийского голосования 01.07.2020<sup>1</sup>.

<sup>1</sup> URL: <http://www.pravo.gov.ru>.



Голосование окружает нас повсеместно, а принятые в ходе него решения становятся юридическими фактами, ведущими к появлению, изменению или прекращению общественных отношений во всех сферах общественной жизни. Это делает голосование одним из важнейших объектов правового регулирования для информационного права, структура которого сегодня имеет устойчивую тенденцию к расширению<sup>2</sup>.

Социум воспринимает голосование как наиболее справедливую форму формирования публичного интереса. Это подтверждается количеством решений в частно-правовой сфере, принимаемых путем голосования, а также количеством споров, рассматриваемых в судах о признании недействительными решений собраний. В Гражданском кодексе РФ регулированию данной сферы отведена отдельная глава<sup>3</sup>, а в базе данных ГАС «Правосудие» и коммерческих справочных правовых системах на начало 2023 г. содержится более 100 000 судебных актов, принятых судами общей юрисдикции и арбитражными судами по данной категории дел.

В публично-правовой сфере голосование используется повсеместно<sup>4</sup>, но не часто, что объясняется наличием объективных препятствий. К их числу можно отнести затраты на проведение голосования, а также сложность его организации. В настоящее время эти проблемы легко разрешаются путем внедрения цифровых технологий, которые существенно расширяют возможности для принятия коллективного решения (системы распределенных реестров, квантовая криптография, цифровые платформы и т.д.). Данный вывод подтвержден анализом зарубежного опыта и изучением экспериментов по дистанционному электронному голосованию (ДЭГ), проведенному в Российской Федерации в 2019 и 2021 гг.

Эксперимент с ДЭГ проходил в двух формах — одна применялась в Москве, другая — в шести субъектах РФ, участвовавших в апробации интернет-голосования<sup>5</sup>. Формы существенно различались как в организационном, так и в правовом плане. Например, в Москве использовался региональный портал государственных услуг, а в других субъектах — единый портал государственных и муниципальных услуг. Правила голосования также различались, например, в Москве у избирателя была возможность изменять результат голосования в течение периода для голосования, а в других субъектах РФ заполнить электронный бюллетень можно было только один раз<sup>6</sup>. Это лишь часть различий, которые вместе с низким

<sup>2</sup> Полякова Т. А., Минбалеев А. В., Кроткова Н. В. Развитие науки информационного права и правового обеспечения информационной безопасности: формирование научной школы информационного права (прошлое и будущее) // Государство и право. 2021. № 12. С. 97—108.

<sup>3</sup> Гражданский кодекс РФ (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 16.04.2022). Глава 9.1 // СЗ РФ. 1994. № 32. Ст. 3301.

<sup>4</sup> Гриценко Г. А. Механизм легитимации государственной власти в современной России (теоретико-правовой аспект) : дис. ... канд. юрид. наук. М., 2012. 182 с.

<sup>5</sup> Постановление ЦИК России от 20.07.2021 № 26/225-8 (ред. от 03.09.2021) «О Порядке дистанционного электронного голосования на выборах, назначенных на 19 сентября 2021 года» // Вестник ЦИК России. 2021. № 13.

<sup>6</sup> Гриценко Е. В. Право на хорошее управление в условиях цифровой трансформации // Сравнительное конституционное обозрение. 2022. № 4. С. 15—36.

уровнем цифровых компетенций у населения и органов публичной власти привели к подаче более 30 исков о признании недействительными результатов выборов.

Следует отметить, что иски оппозиции на процедуру интернет-голосования являются мировым трендом. В Германии после подобного иска Федеральный конституционный суд признал неконституционным электронное голосование, использованное на выборах в Бундестаг 16-го созыва. Данное решение не привело к роспуску избранного парламента, так как отсутствовали факты, указывающие на то, что машины для голосования работали неправильно или ими можно было манипулировать<sup>7</sup>.

В настоящее время цифровая трансформация избирательного процесса в Германии не проводится, хотя исследования показывают, что 56 % немцев хотели бы голосовать через Интернет<sup>8</sup>. Учитывая наличие такой потребности, законодательство страны допускает использовать системы онлайн-голосования на неполитических выборах, например в советы университетов<sup>9</sup>. Аналогичные ограничения существуют и в большинстве других европейских стран. Как справедливо отмечают некоторые авторы, страны ЕС искусственно притормаживают внедрение многих цифровых технологий, мотивируя это заботой о правах человека<sup>10</sup>.

Правовое регулирование правоотношений, возникающих в сети Интернет, различается в разных странах<sup>11</sup>, что отражено и в законодательстве об интернет-голосовании. Конституционный совет Франции, рассматривая соответствующий иск, признал интернет-голосование допустимым способом реализации избирательных прав граждан<sup>12</sup>. Современные цифровые технологии могут принести

<sup>7</sup> Leitsätze zum Urteil des Zweiten Senats vom 3. März 2009 — 2 BvC 3/07, 2 BvC 4/07 // URL: [https://www.bundesverfassungsgericht.de/shareddocs/entscheidungen/de/2009/03/cs20090303\\_2bvc000307.html](https://www.bundesverfassungsgericht.de/shareddocs/entscheidungen/de/2009/03/cs20090303_2bvc000307.html) (дата обращения: 20.01.2023).

<sup>8</sup> Kaspersky-Studie: So steht Deutschland zum Thema Online-Wahlen // URL: <https://www.kaspersky.de/blog/kaspersky-studie-so-steht-deutschland-zum-thema-online-wahlen/13493> (дата обращения: 20.01.2023).

<sup>9</sup> Bätge F., Weiler T. (2019) Elektronische Wahlen und Abstimmungen (Electronic Voting) // T. Klenk, F. Nullmeier, G. Wewer (eds) Handbuch Digitalisierung in Staat und Verwaltung. Springer VS, Wiesbaden. URL: [https://doi.org/10.1007/978-3-658-23669-4\\_25-1](https://doi.org/10.1007/978-3-658-23669-4_25-1).

<sup>10</sup> Холодная Е. В. О правовом обеспечении прав человека при использовании цифровых технологий на территории ЕС // Роль права в обеспечении благополучия человека : сборник докладов XI Московской юридической недели: XX Международная научно-практическая конференция «Кутафинские чтения» ; XXII Международная научно-практическая конференция юридического факультета Московского государственного университета имени М.В.Ломоносова : в 5 ч. М., 2022. С. 351—354.

<sup>11</sup> Минбалева А. В. Основы правового регулирования сети Интернет // Право и кибербезопасность. 2014. № 1. С. 20—26.

<sup>12</sup> Loi relative à la représentation des Français établis hors de France // Décision № 2013-673 DC du 18 juillet 2013 // URL: <https://www.conseil-constitutionnel.fr/decision/2013/2013673dc.htm> (дата обращения: 20.01.2023).



социуму и вред, и благо, разница лишь в организационных и правовых методах их использования<sup>13</sup>.

Технология всегда нейтральна, что видно на примере Франции. Многие страны используют голосование по почте, не ставя под сомнение результаты своих выборов, во Франции этот способ голосования признан небезопасным<sup>14</sup>. Одновременно в стране допускается голосование по доверенности (Code électoral)<sup>15</sup>, что считается антиконституционным в других странах.

Информационная безопасность систем интернет-голосования является важной составляющей национального информационного суверенитета страны<sup>16</sup>. Данная процедура важна, так как все риски информационной безопасности в глобальной цифровой среде не могут быть исключены ни одним государством<sup>17</sup>. Во Франции уполномоченный орган в области защиты данных принял рекомендации, касающиеся данного вопроса<sup>18</sup>. В документе указано, что система интернет-голосования должна пройти независимую экспертизу, проверяющую:

- исходный код программного обеспечения;
- механизмы пломбирования, используемые на различных этапах голосования;
- используемые механизмы шифрования, в частности для шифрования избирательных бюллетеней на избирательном участке.

Во Франции интернет-голосование применимо не только на всеобщих выборах, но и активно используется в частноправовой сфере. Например, в статьях с R723-16 по R723-21 Торгового кодекса Франции (Code de commerce)<sup>19</sup> определен порядок интернет-голосования на выборах судей арбитражных судов. В 2020 г. определены порядок и условия проведения интернет-голосования на выборах

<sup>13</sup> Минбалеев А. В., Евсиков К. С. Информационные технологии противодействия коррупции // Журнал Сибирского федерального университета. Серия : Гуманитарные науки. 2021. Т. 14. № 11. С. 1674—1689.

<sup>14</sup> Note de synthèse // URL: <https://www.senat.fr/lc/lc107/lc1070.html> (дата обращения: 20.01.2023).

<sup>15</sup> Code electoral // URL: [https://www.legifrance.gouv.fr/codes/texte\\_lc/legitext000006070239?dateversion=24%2f09%2f2021&nomcode=uer\\_fa%3d%3d&page=1&pagesize=10&query=internet&searchfield=all&searchtype=all&tab\\_selection=code&typepagination=default&typerecherche=date](https://www.legifrance.gouv.fr/codes/texte_lc/legitext000006070239?dateversion=24%2f09%2f2021&nomcode=uer_fa%3d%3d&page=1&pagesize=10&query=internet&searchfield=all&searchtype=all&tab_selection=code&typepagination=default&typerecherche=date) (дата обращения: 20.01.2023).

<sup>16</sup> Ефремов А. А. Информационное пространство как сфера реализации государственного суверенитета // Вестник Воронежского государственного университета. Серия : Право. 2017. № 1 (28). С. 22—30.

<sup>17</sup> Полякова Т. А., Минбалеев А. В., Бойченко И. С. Проблемы правового обеспечения информационной безопасности в процессе использования цифровых технологий в глобальной цифровой среде // Вестник Академии права и управления. 2018. № 3 (52). С. 32—36.

<sup>18</sup> Délibération № 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique // NOR: CNIA1000012X. JORF № 0272. du 24 novembre 2010. Texte № 29.

<sup>19</sup> Code de commerce // URL: [https://www.legifrance.gouv.fr/codes/texte\\_lc/legitext000005634379?init=true&page=1&query=code+de+commerce&searchfield=all&tab\\_selection=all](https://www.legifrance.gouv.fr/codes/texte_lc/legitext000005634379?init=true&page=1&query=code+de+commerce&searchfield=all&tab_selection=all) (дата обращения: 20.01.2023).

членов консультационных органов вооруженных сил и представителей военно-служащих в командовании<sup>20</sup>.

В приказе министра внутренних дел Франции от 04.02.2021 «О проведении электронного голосования через Интернет для выборов членов консультационной сети в национальной жандармерии»<sup>21</sup> также подробно урегулирована аналогичная процедура. Опыт Франции представляет большой интерес. Он показывает, что наличие правовых и технологических препятствий для внедрения интернет-голосования является мифом. Это подтверждает и отечественный опыт использования цифровых технологий в условиях пандемии<sup>22</sup>.

Несмотря на указанные примеры, исследование подтверждает, что в большинстве стран «цифровую трансформацию» избирательного процесса искусственно ограничивают. В качестве аргумента противники данного процесса приводят нормы права, которые препятствуют внедрению современных информационных технологий. Данная ситуация не является уникальной. В условиях повсеместной цифровой трансформации многие области жизнедеятельности подверглись существенной модернизации, которая вошла в диссонанс с существующими нормами права<sup>23</sup>.

В различных сферах общественной жизни эта проблема решается по-разному. Например, в области безопасности дорожного движения создаются экспериментальные правовые режимы, которые позволяют эксплуатировать беспилотные транспортные средства на ограниченной территории без нарушения действующих правил дорожного движения и иных нормативных правовых актов<sup>24</sup>.

Использование цифровых технологий в голосовании также вошло в противоречие с некоторыми традиционными правовыми механизмами. Например, в отечественном и зарубежном праве высказано множество опасений насчет соблюдения принципа тайного голосования через сеть Интернет. Не вызывает сомнений, что

<sup>20</sup> Décret № 2020–1329 du 2 novembre 2020 relatif aux conditions et modalités de la mise en œuvre du vote électronique par internet pour l'élection des membres des organismes consultatifs et de concertation des militaires et des représentants du personnel militaire auprès du commandement // Journal officiel «Lois et Décrets» № 0267 du 3 novembre 2020.

<sup>21</sup> Arrêté du 4 février 2021 relatif au déroulement du vote électronique par internet pour l'élection des membres de la chaîne de concertation au sein de la gendarmerie nationale // Journal officiel «Lois et Décrets» № 0034 du 9 février 2021.

<sup>22</sup> *Добробаба М. Б., Минбалеев А. В.* Пандемия как новый импульс развития системы регулирования отношений, применяемых в сфере искусственного интеллекта, применяемого в государственном управлении // Роль и значение права в условиях пандемии : монография по итогам Международного онлайн-симпозиума / под общ. ред. В. В. Блажеева, М. А. Егоровой. М., 2021. С. 167—177.

<sup>23</sup> *Минбалеев А. В., Берестнев М. А., Евсиков К. С.* Регулирование использования искусственного интеллекта в добывающей промышленности // Известия Тульского государственного университета. Науки о Земле. 2022. № 2. С. 509—525.

<sup>24</sup> Постановление Правительства РФ от 09.03.2022 № 309 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по эксплуатации высокоавтоматизированных транспортных средств» // СЗ РФ. 2022. № 12. Ст. 1817.



при голосовании с использованием сети Интернет у государства могут возникнуть сложности с обеспечением тайны голосования. Но это не исключает возможность обеспечения свободы волеизъявления иными способами.

Данный вывод подтверждается анализом запретительных мер, принимаемых разными странами в сфере использования информационных технологий избирателями. Например, в некоторых странах, а также в некоторых субъектах федераций установлены запреты на селфи с заполненным бюллетенем для голосования, в части стран это разрешено на законодательном уровне, но в большинстве стран не урегулировано<sup>25</sup>. При этом ни в одной стране мира нет прецедентов, когда результаты голосования были бы оспорены из-за использования гражданами смартфонов на избирательном участке.

Важно отметить, что Российская Федерация идет по пути внедрения цифровых технологий в избирательную систему, что отражено в действующем законодательстве. Например, ранее ДЭГ не регулировалось Федеральным законом от 12.06.2002 № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации»<sup>26</sup>. В 2022 г. данный нормативный акт дополнен статьей 64.1 «Дистанционное электронное голосование», состоящей из 20 частей<sup>27</sup>. Хотя эта статья не урегулировала все вопросы, связанные с интернет-голосованием, но ее принятие — значимый шаг в совершенствовании правового регулирования цифровой трансформации избирательной системы Российской Федерации.

Подводя итог вышеизложенному, следует отметить, что использование интернет-голосования соответствует запросам информационного общества. Их удовлетворение является одной из ключевых задач цифрового государства<sup>28</sup>. Изученный зарубежный опыт позволяет говорить, что органы публичной власти не стремятся обеспечить доступ граждан к новому способу участия в управлении делами государства, ссылаясь на технические и юридические проблемы.

Эксперименты с ДЭГ, проведенные в России, а также примеры интернет-голосования за рубежом позволяют опровергнуть данные доводы. Как показало наше исследование, проблемы правового характера могут быть разрешены путем изменения правовых концепций и принятия новых правовых гарантий реализации гражданами избирательных прав.

Одновременно следует отметить, что интернет-голосование востребовано не только в публично-правовой, но и в частноправовой сфере. В связи с этим необходимо рекомендовать предоставление доступа к цифровым платформам для

<sup>25</sup> Евсиков К. С. Правовой режим изображения бюллетеня для голосования, отмеченного избирателем // Информационное право. 2022. № 3. С. 14—18.

<sup>26</sup> Федеральный закон от 12.06.2002 № 67-ФЗ (ред. от 28.06.2022) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» // СЗ РФ. 2002. № 24. Ст. 2253.

<sup>27</sup> Федеральный закон от 14.03.2022 № 60-ФЗ (ред. от 14.07.2022) «О внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2022. № 12. Ст. 1787.

<sup>28</sup> Полякова Т. А., Минбалеев А. В., Бойченко И. С. Цифровая трансформация: вызовы праву и векторы научных исследований // Информационное право. 2020. № 2. С. 46—48.

голосования, сертифицированным государством, для использования их субъектами частного права при принятии ими коллективных юридически значимых решений. Реализация этого предложения будет способствовать повышению доверия к информационным системам, повышению компетенций у широкого круга лиц и цифровой трансформации избирательного процесса в Российской Федерации.

## БИБЛИОГРАФИЯ

1. *Гриценко Е. В.* Право на хорошее управление в условиях цифровой трансформации // Сравнительное конституционное обозрение. — 2022. — № 4. — С. 15—36.
2. *Гриценко Г. А.* Механизм легитимации государственной власти в современной России (теоретико-правовой аспект) : дис. ... канд. юрид. наук. — М., 2012. — 182 с.
3. *Добробаба М. Б., Минбалеев А. В.* Пандемия как новый импульс развития системы регулирования отношений, применяемых в сфере искусственного интеллекта, применяемого в государственном управлении // Роль и значение права в условиях пандемии : монография по итогам Международного онлайн-симпозиума / под общ. ред. В. В. Блажеева, М. А. Егоровой. — М., 2021. — С. 167—177.
4. *Евсиков К. С.* Механизмы реализации конституционного права граждан на участие в управлении делами государства // Журнал российского права. — 2019. — № 6. — С. 36—49.
5. *Евсиков К. С.* Правовой режим изображения бюллетеня для голосования, отмеченного избирателем // Информационное право. — 2022. — № 3. — С. 14—18.
6. *Ефремов А. А.* Информационное пространство как сфера реализации государственного суверенитета // Вестник Воронежского государственного университета. — Серия : Право. — 2017. — № 1 (28). — С. 22—30.
7. *Минбалеев А. В.* Основы правового регулирования сети Интернет // Право и кибербезопасность. — 2014. — № 1. — С. 20—26.
8. *Минбалеев А. В., Берестнев М. А., Евсиков К. С.* Регулирование использования искусственного интеллекта в добывающей промышленности // Известия Тульского государственного университета. — Науки о Земле. — 2022. — № 2. — С. 509—525.
9. *Минбалеев А. В., Евсиков К. С.* Информационные технологии противодействия коррупции // Журнал Сибирского федерального университета. — Серия : Гуманитарные науки. — 2021. — Т. 14. — № 11. — С. 1674—1689.
10. *Полякова Т. А., Минбалеев А. В., Бойченко И. С.* Проблемы правового обеспечения информационной безопасности в процессе использования цифровых технологий в глобальной цифровой среде // Вестник Академии права и управления. — 2018. — № 3 (52). — С. 32—36.
11. *Полякова Т. А., Минбалеев А. В., Бойченко И. С.* Цифровая трансформация: вызовы праву и векторы научных исследований // Информационное право. — 2020. — № 2. — С. 46—48.



12. Полякова Т. А., Минбалеев А. В., Кроткова Н. В. Развитие науки информационного права и правового обеспечения информационной безопасности: формирование научной школы информационного права (прошлое и будущее) // Государство и право. — 2021. — № 12. — С. 97—108.
13. Холодная Е. В. О правовом обеспечении прав человека при использовании цифровых технологий на территории ЕС // Роль права в обеспечении благополучия человека : сборник докладов XI Московской юридической недели: XX Международная научно-практическая конференция «Кутафинские чтения» ; XXII Международная научно-практическая конференция юридического факультета Московского государственного университета имени М.В.Ломоносова : в 5 ч. — М., 2022. — С. 351—354.
14. Bätge F., Weiler T. (2019) Elektronische Wahlen und Abstimmungen (Electronic Voting) // Klenk T., Nullmeier F., Wewer G. (eds.) Handbuch Digitalisierung in Staat und Verwaltung. — Springer VS, Wiesbaden. — [https://doi.org/10.1007/978-3-658-23669-4\\_25-1](https://doi.org/10.1007/978-3-658-23669-4_25-1).

## Правоотношения в цифровой сфере

### Правовые характеристики качества патентов в сфере информационных технологий: постановка проблемы

**Аннотация.** Патенты являются важным элементом экономического роста, который способствует инновациям за счет создания новых научных и технологических знаний. Влияние патентов на стимулирование инноваций и экономический рост бесспорен. При этом подчеркивается роль охраны результатов интеллектуальной деятельности для повышения конкурентоспособности и роста заявок. В результате количество патентов по применению новых технологий и привлечению новых участников внутри системы (т.е. высокотехнологичных юридических лиц, научно-исследовательских институтов, стартапов и сетей) выросло в геометрической прогрессии, что ставит под угрозу будущее функционирование патентной системы. Патенты по-прежнему все чаще используются субъектами предпринимательской деятельности и государственными исследовательскими организациями для защиты новых изобретений, IT-решений, технологий, которые порождают новые волны инноваций и способствуют изменению действующего национального гражданского законодательства Российской Федерации.  
**Ключевые слова:** качество патента, новые технологии, предпринимательская деятельность, информационные технологии, инновации, результаты интеллектуальной деятельности, патентная система.



**Ольга Викторовна  
СУШКОВА,**

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

DOI: 10.17803/2311-5998.2023.102.2.129-136

**OLGA V. SUSHKOVA,**

Associate Professor of the Department of information law and digital technologies,  
Associate Professor of the Department of business and corporate law  
of the Kutafin Moscow State Law University (MSAL),  
Cand. Sci. (Law), Associate Professor  
[ovsushkova@mail.ru](mailto:ovsushkova@mail.ru)  
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

#### **Legal Characteristics of the Quality of Patents in the Sphere of Information Technologies: Statement of the Problem**

**Abstract.** Patents are an important element of economic growth that promotes innovation through the creation of new scientific and technological knowledge. The impact of patents on stimulating innovation and economic

© Сушкова О. В., 2023

*growth is undeniable. At the same time, the role of protecting the results of intellectual activity is emphasized in order to increase competitiveness and increase applications. As a result, the number of patents for applying new technologies and attracting new participants within the system (i.e. high-tech entities, research institutions, start-ups and networks) has grown exponentially, jeopardizing the future functioning of the patent system. Patents are still increasingly used by business entities and government research organizations to protect new inventions, IT solutions, technologies that generate new waves of innovation and contribute to changing the current national civil legislation of the Russian Federation.*

**Keywords:** *patent quality, new technologies, entrepreneurial activity, information technologies, innovations, results of intellectual activity, patent system.*

Исследователи утверждают<sup>1</sup>, что в последние годы инновационные тенденции и функционирование патентной системы подвергались сомнению с учетом различных факторов, как экзогенных, так и эндогенных. Как изложено в пояснительной записке к проекту федерального закона № 873108-7, «данные изменения позволят расширить круг специалистов, владеющих практически навыками проведения информационного поиска и оценки патентоспособности, анализа патентной и иной документации в специализированных областях науки и техники, предоставят эксперту Роспатента возможность уменьшить объем подготовительной работы и лучше понять сущность заявленного изобретения, а также повысить качества патента за счет привлечения отраслевых специалистов для определения уровня техники и оценки патентоспособности технического решения до начала проведения экспертизы заявки по существу»<sup>2</sup>.

Новые технологии и научные достижения (например, биотехнологии, связанные с компьютерами, нанотехнологии) воспринимаются как основные экзогенные силы.

Эти технологии поставили множество вопросов относительно объема патентоспособных объектов и вызвали у законодателей в области права интеллектуальной собственности (далее — ИС)<sup>3</sup> необходимость рассмотреть регулирование новых видов технологий и знаний<sup>4</sup>. Например, несколько патентных ведомств

<sup>1</sup> Дуэль А. Ноу-хау. Роспатент привлечет к работе вузы. Экспертиза на стороне // Российская газета. 06.08.2020.

<sup>2</sup> Проект федерального закона № 873108-7 «О внесении изменений в Гражданский кодекс Российской Федерации» (редакция, внесенная в Государственную Думу, текст по состоянию на 27.12.2019) // URL: <https://sozd.duma.gov.ru/>, 27.12.2019.

<sup>3</sup> Гражданский кодекс РФ (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 05.12.2022) // СЗ РФ. 2006. № 52 (ч. 1). Ст. 5496.

<sup>4</sup> С 01.01.2023 вступила в силу новая, 12-я редакция МКТУ (Международной классификации товаров и услуг для регистрации знаков, принятая в г. Ницце 15.06.1957). В Классификатор внесены изменения. В частности, в классе 9 появились такие товары, как «файлы цифровые загружаемые, аутентифицированные невзаимозаменяемыми токенами (NFT)», «роботы человекоподобные с искусственным интеллектом для пригото-

(включая Европейское патентное ведомство) заняли ведущую роль в расширении круга объектов, для которых патентную охрану можно получить в случае добавления, например, биотехнологии в качестве патентоспособного объекта в учреждениях ИС.

Качество выдаваемых патентов считается в основном эндогенным фактором, который ставит под сомнение способность патентной системы стимулировать инновации и распространять технологии.

Существуют **различные определения качества патента**. Одни ученые смотрят на эту проблему шире, соотнося ее в принципе с несколькими патентами, которые соответствуют критериям патентоспособности (новизна, изобретательский уровень и промышленная применимость)<sup>5</sup>, другие же утверждают<sup>6</sup> как пользователи патентной системы (заявители, патентообладатели), что качество патента связано с затратами на патентование, своевременностью экспертизы и работоспособностью продукции, поставляемой конечным потребителям.

В исследовании больше будет сделан акцент на вопросах качества патентов, которые относятся к процессу поиска и экспертизы, а также возможности патентования заявки на выполнение требований патентоспособности.

Первые комплексные исследования в этом направлении начались в США. Однако патентная система не может исключать риски и негативные последствия патентов низкого качества. Сложные патентные отношения (взаимосвязь оборота объектов ИС, удостоверяемых патентами) с другими важными сферами, такими как политика и нормативное регулирование в области конкуренции (Федеральный закон «О защите конкуренции»<sup>7</sup>), политика технологических стандартов (Федеральный закон «О стандартизации в Российской Федерации»<sup>8</sup>), международная торговля и политика в сфере здравоохранения, сделали политику в отношении прав ИС решающей.

Патенты низкого качества, не соответствующие критериям патентоспособности, могут нанести серьезный ущерб инновационному процессу, заставив общественность платить сверхконкурентные цены за продукты (из-за высоких лицензионных отчислений). Они также могут налагать ненужные ограничения на последующие инновации, что приводит к уменьшению стимулов для развития

ления напитков», «роботы человекоподобные программируемые пользователем ненастроенные», «роботы человекоподобные, обладающие функциями общения и обучения, для оказания помощи и развлечения людей». В классе 39 появились «услуги аренды автомобиля по подписке». В класс 41 добавили среди прочего «предоставление онлайн-изображений, не загружаемых».

<sup>5</sup> *Ивлиев Г. П.* О целесообразности введения в Российской Федерации процедуры оппозиции при регистрации промышленных образцов // ИС. Промышленная собственность. 2020. № 8. С. 5—10.

<sup>6</sup> *Мартасов Д. В.* Экономическая эффективность ноу-хау и его практическое использование // Российская юстиция. 2019. № 9. С. 63—65.

<sup>7</sup> Федеральный закон от 26.07.2006 № 135-ФЗ (ред. от 29.12.2022) «О защите конкуренции» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3434.

<sup>8</sup> Федеральный закон от 29.06.2015 № 162-ФЗ (ред. от 30.12.2020) «О стандартизации в Российской Федерации» // СЗ РФ. 2015. № 27. Ст. 3953.



технологий и создает «патентные заросли»<sup>9</sup>, где появляются перекрывающиеся патенты.

Чтобы преодолеть это, мы попытаемся найти априорные способы определения стоимости патента в первые годы его существования. Для построения прогностических показателей мы разделили наши данные на два этапа, а именно на ранний и зрелый этапы развития технологии, чтобы объяснить влияние качества патента. Мы применили анализ социальных сетей для анализа сетевой структуры ссылок на патенты как инновационной сети.

*Анализ социальных сетей* — это метод исследования, направленный на выявление действующих лиц и наборов отношений, составляющих структуру системы, причем отношения можно определить как «предоставление информации» и «получение информации»<sup>10</sup>. Недавно анализ социальных сетей использовался для анализа взаимосвязей между ссылками на патенты и стратегическим альянсом, а также для изучения распространения технологий или патентов среди организаций<sup>11</sup>. В текущем исследовании патенты рассматриваются как связи или взаимодействие между двумя патентами, которые определяются прямым и обратным цитированием. Анализ сети цитирования патентов позволяет изучить патенты с точки зрения макроэкономики, чтобы распознать положение каждого патента в сети и его характеристики в сети.

В этом исследовании делается попытка использовать положение патентов для прогнозирования их патентного качества.

**Качество патентов.** Патенты — это «суррогат» научно-исследовательского потенциала юридического лица, деятельность которого направлена на исследование технологических инноваций<sup>12</sup>. Они являются результатом инвестиций в НИОКР<sup>13</sup> и становятся ценными нематериальными активами<sup>14</sup>. Эта неосязаемость

<sup>9</sup> *Ворожевич А. С.* Принцип эстоппеля в патентном праве: основания и практика применения // Закон. 2020. № 4. С. 88—106 ; *Shapiro C.* Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard-Setting // Innovation Policy and the Economy / eds. A. B. Jaffe [et al.]. 2001. Vol. 1. P. 119—150. MIT Press ; *Blakeney M.* Biotechnological Patenting and innovation // Patents and Technological Progress in a Globalized World / ed. by M. J. Adelman, R. Brauneis [et al.]. Berlin, 2009. P. 234 ; *Stack A. J.* International Patent law: Cooperation, harmonization and institutional analysis of WPO. Cheltenham, 2011. P. 24.

<sup>10</sup> *Monge P. R., Contracto N. S.* Theories of communication networks. New York : Oxford University Press, 2003. С. 334.

<sup>11</sup> *Cantner U., Graf H.* The network of innovators in Jena: An application of social network analysis // Research Policy. 2006. № 35 (4). P. 463—480.

<sup>12</sup> *Сушкова О. В.* Гражданско-правовой режим инноваций в научно-технической сфере (на примере деятельности высших учебных заведений) : дис. ... канд. юрид. наук, М. : РПА Минюста России, 2010. С. 153.

<sup>13</sup> Гражданский кодекс РФ (часть вторая) от 26.01.1996 № 14-ФЗ (с изм. и доп., вступ. в силу с 01.01.2022) // СЗ РФ. 1996. № 5. Ст. 410.

<sup>14</sup> Приказ Минфина России от 15.11.2019 № 181н «Об утверждении федерального стандарта бухгалтерского учета государственных финансов «Нематериальные активы»» (зарегистрировано в Минюсте России 16.12.2019 № 56822) // URL: <http://www.pravo.gov.ru>, 17.12.2019.

затрудняет измерение стоимости патента, а поскольку исследователи склонны использовать качество патента для отражения стоимости патента, для измерения качества патента, было предложено множество показателей. Эти показатели можно классифицировать в зависимости от того, связаны они с показателями цитирования, объемом патента или решениями о сроке их действия / продлении или нет.

Ссылки на патенты считаются полезными показателями с точки зрения достоверности и надежности<sup>15</sup>. Показатели, связанные с цитированием, включают связи между наукой и технологиями, текущие индексы влияния и общее количество цитирований. *Ссылки на науку и технологии* — это количество ссылок на патент в других научных работах. Чем чаще патент цитируется в научных статьях или чем чаще в патенте цитируется влиятельная статья, тем больше влияние патента на научные разработки или его связь между наукой и технологиями.

Наиболее широко используемым показателем качества патентов является число цитирований патентов. Патентные ссылки включают в себя предыдущие и прямые ссылки. Обратное цитирование относится к цитатам, которые патент цитирует в патентном документе. Прямое цитирование происходит, когда основной патент цитируется в последующих патентных заявках. Упреждающий подсчет цитирования широко используется в исследованиях качества патентов.

Как правило, количество цитирований отражает внутреннее качество патента. Изменения в количестве цитирований патентов за определенный период времени отражают тенденции в цитировании. Изменения в количестве цитируемых патентов можно рассматривать как пассивный показатель качества патентов, поскольку конкретный правопреемник не может полностью контролировать количество патентов, на которые делается ссылка; скорее, он контролируется всеми соответствующими патентами.

Качество патента может быть измерено решением о продлении, потому что в патентной системе правопреемники должны платить пошлину за поддержание патентных прав. Плата за поддержание патента может увеличиваться; правопреемник должен изучить и оценить качество и ценность патентов, чтобы определить, оправдывают ли выгоды, предоставляемые патентом, стоимость платы за его поддержание в силе. Плата за поддержание патента в силе может быть тяжелым бременем для юридических лиц, поэтому срок действия патента рассматривается как субъективный или активный показатель качества патента, который оценивается правопреемниками. Юридические лица могут принять как положительное, так и отрицательное решение об уплате пошлины за поддержание патента в силе.

**Количество цитирований патентов и решения о продлении** — два широко используемых показателя качества патентов. Число цитирований патентов отражает *объективную оценку* изобретателей соответствующих технологий; решение о продлении отражает *субъективную оценку* патентообладателя. Поскольку патенты связаны друг с другом прямым и обратным цитированием, на качество патентов могут влиять связи между патентами. Поэтому мы применили анализ социальных сетей для дальнейшего изучения влияния структуры сети цитирования патентов на качество патентов.

<sup>15</sup> Meyer M. What is special about patent citations? Differences between scientific and patent citations // *Scientometrics*. 2000. № 49. P. 93—123.



**Анализ социальных сетей** впервые был использован для анализа отношений между людьми, включая экономические, политические и аффективные связи<sup>16</sup>. Каждое лицо (или действующее лицо) в социальной сети обозначает узел; отношения между двумя акторами образуют связи (или «ребра»), а социальные сети строятся из связей, соединяющих акторов. Связи между акторами — это каналы передачи ресурсов<sup>17</sup>. Структура сети, позиции в сети и взаимосвязанность связей являются основными проблемами исследователей социальных сетей. Анализ социальных сетей широко применяется в исследованиях сообществ и взаимосвязанных управлений. *Прямые и обратные ссылки на патенты образуют сеть цитирования патентов.*

Одни исследователи использовали анализ социальных сетей для выяснения отношений цитирования патентов, а также для анализа цитирований и совместных инноваций<sup>18</sup>. Другие исследователи применяли теорию социальных сетей для анализа многоэтапного цитирования, выявляя взаимосвязь между «семействами патентов», библиографическую связь и т.д.<sup>19</sup>

Однако характеристики позиции в сети редко изучаются в сетях цитирования патентов. Положение в сети часто изучается, чтобы объяснить важность актора внутри и за пределами группы, которая является частью более крупной сети. Предполагается, что актор может занимать две взаимодополняющие, но важные позиции: посредничество и закрытие.

*Посредничество* относится к обмену информацией или ресурсами между двумя группами или двумя субъектами, чтобы разъединенные группы или субъекты могли общаться и обмениваться информацией и ресурсами.

*Закрытие* важно для группы. Закрытие уменьшает вариации внутри группы, что повышает доверие и сотрудничество. Каждый участник сети создает свою репутацию и имеет доверие, чтобы он мог тесно связать себя с другими участниками и сформировать закрытую сеть. Актор может не только передавать информацию и ресурсы другим группам, но и одновременно строить тесные отношения с другими акторами в той же группе в закрытой сети.

Центральное место в посредничестве представляет положение актора на кратчайшем пути между двумя другими акторами. Это подразумевает, что актор может контролировать взаимодействие между двумя несмежными акторами. Кроме того, такое положение представляет актора, который имеет возможность контролировать ресурсы или информацию, передаваемую другим акторам в сети, что позволяет актору передавать информацию и ресурсы другим акторам или группам. Промежуточность может отражать передачу технологических знаний, что способствует появлению новых технологий<sup>20</sup>.

<sup>16</sup> Wasserman S., Faust K. Social network analysis: Methods and applications. New York : Cambridge University Press, 1994. P. 135.

<sup>17</sup> Копина А. А. Правовые основы налогообложения акторов цифровой экономики // *Налоги*. 2022. № 1. С. 23—28.

<sup>18</sup> Sternitzke C., Bartkowski A., Schramm R. Visualizing patent statistics by means of social network analysis tools // *World Patent Information*. 2008. № 30 (2). P. 115—131.

<sup>19</sup> Van Wartburg I., Teichert T., Rost K. Inventive progress measured by multi-stage patent citation analysis // *Research Policy*. 2005. № 34 (10). P. 1591—1607.

<sup>20</sup> См.: Мохов А. А. Инновационная биомедицина — миф или реальность? // *Медицинское право*. 2021. № 6. С. 13—18 ; Минбалеев А. В. Основные проблемы и перспективы раз-

Патенты, занимающие посредническую позицию, являются технологической базой для последующих технологий; они открывают новые технологические уклады и ведут к дальнейшему развитию. Патенты, занимающие посредническую позицию на ранней стадии конкретной технологической области, играют ключевую роль в передаче соответствующих знаний или информации между двумя патентами. Более того, патенты на посреднические услуги можно рассматривать как стратегический инструмент для быстрого блокирования входа конкурентов на рынок, поскольку эти патенты занимают важное место в связи с родственными патентами.

Следовательно, патенты с более высокой промежуточной центральностью в сети цитирования патентов могут прогнозировать более высокое качество патентов. Как предварительное цитирование, так и решения о продлении являются важными показателями качества патентов.

Поскольку технологии постоянно меняются, разные технологические этапы могут иметь разные характеристики в сети цитирования патентов. В этом исследовании, сказано выше, были проанализированы две разные стадии развития технологий: ранняя стадия и зрелая стадия. Предполагалось, что сети цитирования патентов различаются на ранней и зрелой стадиях, что отражает траекторию развития технологии.

Таким образом, патентная позиция может играть разные роли по мере развития сети цитирования патентов, а технологические этапы могут оказывать большое влияние на качество патентов.

## БИБЛИОГРАФИЯ

1. *Ворожевич А. С.* Принцип эстоппеля в патентном праве: основания и практика применения // Закон. — 2020. — № 4. — С. 88—106.
2. *Ершова И. В.* Модернизация сферы образования: инновация & эксперимент // Право и бизнес. — 2022. — № 1. — С. 25—29.
3. *Ивлиев Г. П.* О целесообразности введения в Российской Федерации процедуры оппозиции при регистрации промышленных образцов // ИС. Промышленная собственность. — 2020. — № 8. — С. 5—10
4. *Копина А. А.* Правовые основы налогообложения акторов цифровой экономики // Налоги. — 2022. — № 1. — С. 23—28.
5. *Мартасов Д. В.* Экономическая эффективность ноу-хау и его практическое использование // Российская юстиция. — 2019. — № 9. — С. 63—65.
6. *Минбалева А. В.* Основные проблемы и перспективы развития LegalTech в России в условиях цифровизации // Юрист. — 2022. — № 9. — С. 43—48.
7. *Мохов А. А.* Инновационная биомедицина — миф или реальность? // Медицинское право. — 2021. — № 6. — С. 13—18.

вития LegalTech в России в условиях цифровизации // Юрист. 2022. № 9. С. 43—48 ;  
*Ершова И. В.* Модернизация сферы образования: инновация & эксперимент // Право и бизнес. 2022. № 1. С. 25—29.



8. Сушкова О. В. Гражданско-правовой режим инноваций в научно-технической сфере (на примере деятельности высших учебных заведений) : дис. ... канд. юрид. наук. — М. : РПА Минюста России, 2010.
9. *Blakeney M.* Biotechnological Patenting and innovation // *Patents and Technological Progress in a Globalized World* / ed. by M. J. Adelman, R. Brauneis [et al.]. — Berlin, 2009.
10. *Cantner U., Graf H.* The network of innovators in Jena: An application of social network analysis // *Research Policy*. — 2006. — № 35 (4). — P. 463—480.
11. *Meyer M.* What is special about patent citations? Differences between scientific and patent citations // *Scientometrics*. — 2000. — № 49. — P. 93—123.
12. *Monge P. R., Contractor N. S.* Theories of communication networks. — New York : Oxford University Press, 2003.
13. *Shapiro C.* Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard-Setting // *Innovation Policy and the Economy* / eds A. B. Jaffe [et al.]. — 2001. — Vol. 1. — P. 119—150, MIT Press.
14. *Stack A. J.* International Patent law: Cooperation, harmonization and institutional analysis of WPO. — Cheltenham, 2011.
15. *Sternitzke C., Bartkowski A., Schramm R.* Visualizing patent statistics by means of social network analysis tools // *World Patent Information*. — 2008. — № 30 (2). — P. 115—131.
16. *Van Wartburg I., Teichert T., Rost K.* Inventive progress measured by multi-stage patent citation analysis // *Research Policy*. — 2005. — № 34 (10). — P. 1591—1607.
17. *Wasserman S., Faust K.* Social network analysis: Methods and applications. — New York : Cambridge University Press, 1994.

## О целесообразности совершенствования системы правового регулирования информационных отношений в сфере библиотечного дела в контексте киберправа

**Аннотация.** Предпринята попытка анализа новых институциональных образований в системе информационного права — интернет-права, киберправа, цифрового права. На основе изучения подходов различных авторов представлено соотношение данных категорий. Обосновано, что цифровое право является приоритетным для правового регулирования принципиально новых общественных отношений, складывающихся по поводу применения сквозных цифровых технологий, в то время как совершенствование системы правового регулирования с позиций киберправа представляется более перспективным в качестве направления совершенствования правовой регламентации традиционных информационных институтов, не способных к быстрой цифровой трансформации.

По результатам исследования автором сделан вывод о том, что одним из традиционных информационных институтов, совершенствование системы правового регулирования которого целесообразно рассматривать в контексте киберправа, является институт правового регулирования информационных отношений в сфере библиотечного дела. Утверждается, что данный подход позволит адаптировать правовое регулирование библиотечно-информационной деятельности к цифровой среде на период внедрения в библиотечную практику сквозных цифровых технологий при соблюдении баланса предоставления библиотечно-информационных услуг в традиционной и электронной формах.

**Ключевые слова:** информационное право, интернет-право, киберправо, киберпространство, сквозные цифровые технологии, цифровое право, библиотека, правовое регулирование библиотечного дела, цифровая трансформация библиотечного дела.



**Татьяна Викторовна ПАШНИНА,**

доцент кафедры  
государственно-правовых  
дисциплин  
Уральского филиала  
Российского  
государственного  
университета правосудия  
(РГУП),  
кандидат юридических наук  
[pashninatv\\_chel@mail.ru](mailto:pashninatv_chel@mail.ru)  
454135, Россия,  
г. Челябинск,  
ул. Энергетиков, д. 63

DOI: 10.17803/2311-5998.2023.102.2.137-145

**TATYANA V. PASHNINA,**

*Associate Professor of the Department of state  
and legal disciplines of the Ural branch  
of the Russian State University of justice (RSUJ), Cand. Sci. (Law)*

*pashninatv\_chel@mail.ru*

*63, ul. Energetikov, Chelyabinsk, Russia, 454135*

**On the Expediency of Improving  
the System of Legal Regulation of Information Relations  
in the Field of Librarianship in the Context of Cyber Law**

**Abstract.** *An attempt is made to analyze new institutional formations in the system of information law — «Internet law», «cyber law», «digital law». Based on the study of the approaches of various authors, the ratio of these categories is presented. It is proved that digital law is a priority for the legal regulation of fundamentally new public relations emerging over the use of end-to-end digital technologies, while improving the system of legal regulation from the standpoint of cyber law seems more promising as a direction for improving the legal regulation of traditional information institutions that are incapable of rapid digital transformation.*

*According to the results of the study, the author concludes that one of the traditional information institutions, the improvement of the system of legal regulation of which it is advisable to consider in the context of cyber law, is the institute of legal regulation of information relations in the field of librarianship. It is argued that this approach will make it possible to adapt the legal regulation of library and information activities to the digital environment for the period of introduction of end-to-end digital technologies into library practice, while maintaining a balance of providing library and information services in traditional and electronic forms*

**Keywords:** *information law, internet law, cyber law, cyberspace, end-to-end digital technologies, digital law, library, legal regulation of librarianship, digital transformation of librarianship.*

**Б**ытие человека XXI в. подвергается стремительной, временами турбулентной трансформации, делясь в процессе нее на пласт реальный и пласт виртуальный. Проникновение во все слои общества и сферы жизнедеятельности интернет- и иных новых информационных, а затем — пришедших им на смену сквозных цифровых технологий изменило окружающую человека действительность, породив новое ее измерение — цифровое, виртуальное, киберпространство. И это прочно вошло в жизнь социума и отразилось на системе отраслей российского права, вынужденных приспособляться к новой цифровой реальности и осуществлять правовую регламентацию отношений по поводу объектов, ранее данным отраслям не известных<sup>1</sup>.

<sup>1</sup> См., например: Правовое регулирование цифровых технологий в России и за рубежом. Роль и место правового регулирования и саморегулирования в развитии цифровых

Наиболее серьезные изменения сквозные цифровые технологии и новое измерение пространства привнесли в отрасль информационного права, в своем классическом виде сформировавшуюся и получившую статус самостоятельной отрасли российского права в конце прошлого века.

Рассматривая процесс эволюции отрасли информационного права, А. В. Минбалеев справедливо отмечает то обстоятельство, что цифровая трансформация оказывает на нее значительное влияние, проявляющееся, в частности, в том, что «важной проблемой в развитии информационного права сегодня видится постоянное расширение его предмета, происходящего за счет появления новых отношений, связанных с развитием данных в цифровой форме, а также ряда классов новейших цифровых технологий»; «трансформируется и правовой категориальный аппарат, который меняется под техническим воздействием и обуславливается техническими процессами цифровизации»; «в информационном праве происходит постоянное появление новых институтов, связанных с правовыми режимами отдельных видов информации, информационных технологий и других информационных объектов»<sup>2</sup>.

В настоящее время в информационном праве институционализируются такие новые правовые категории, как цифровое право, интернет-право, право информационных технологий, киберправо (право киберпространства), и т.д.

И если первая категория получила широкое концептуальное осмысление в научных исследованиях последних лет<sup>3</sup>; вторая и третья, в силу «привязанности» к конкретным технологиям, не несут в себе значительной дискуссионности, понятие «киберправо», хотя и появилось в научных источниках около 20 лет назад<sup>4</sup>, не получило столь широкого распространения и глубокого теоретического осмысления<sup>5</sup> и, как следствие, четкой дифференциации от близких категорий.

Обосновывая различия и соотношение перечисленных выше понятий, М. А. Рожкова отмечает: «В зарубежной юриспруденции *интернет-право* изначально рассматривалось... как некая совокупность разнонаправленных правовых норм и институтов, относящихся к различным отраслям (областям) права и регулирующих отношения, которые так или иначе связаны с Интернетом. Такое

---

технологий : монография / под ред. А. В. Минбалеева. Саратов : Амирит, 2019. 207 с. ; Цифровая трансформация: вызовы праву и векторы научных исследований : монография / под общ. ред. А. Н. Савенкова ; отв. ред. Т. А. Полякова, А. В. Минбалеев. М. : РГ-Пресс, 2021 ; Механизмы и модели регулирования цифровых технологий / А. В. Минбалеев, А. В. Мартынов, Г. Г. Камалова [и др.]. М. : Проспект, 2023.

<sup>2</sup> Минбалеев А. В. Проблемы цифрового права : учебное пособие. Саратов : Амирит, 2022. С. 12, 14—15.

<sup>3</sup> См., например: Цифровое право / А. Дюфло, Л. В. Андреева, В. В. Блажеев [и др.]. М. : Проспект, 2020 ; Минбалеев А. В. Проблемы цифрового права : учебное пособие. Саратов : Амирит, 2022.

<sup>4</sup> Jambholkar L. Cyber law. Issues and perspectives // The Indian j. of intern. law. 2000. Vol. 40. № 3. P. 559—562.

<sup>5</sup> См., например: Леонтьев А. Н. Киберправо : учебное пособие / ВолгГТУ. Волгоград, 2021 ; Мажорина М. В. Цифровые платформы и международное частное право, или Есть ли будущее у киберправа? // Lex russica. 2019. № 2. С. 107—120.



понимание сохраняется и поныне»<sup>6</sup>. «Киберправо, право киберпространства, компьютерное право представляют собой не самостоятельные отрасли права, а совокупности разноплановых правовых норм и институтов, относящихся к различным отраслям (областям) права, объединение которых производится в каждом случае в соответствии с субъективными критериями и поставленными задачами»<sup>7</sup>. «Цифровое право следует понимать как совокупность правовых норм и институтов, регулирующих разнообразные отношения, связанные с внедрением и использованием цифровых технологий, но эти нормы не объединены единым методом регулирования и относятся к различным отраслям права»<sup>8</sup>.

Таким образом, можно сделать вывод о том, что цифровое право является наиболее технологически прогрессивным институтом в системе информационного права, поскольку его генезис связан с необходимостью правового регулирования отношений по применению сквозных цифровых технологий. Интернет-право преимущественно акцентировано на нормативной регламентации применения одной технологии — Интернета. По отношению же к правовой природе киберправа до сих пор среди исследователей не найден консенсус: в то время как ряд авторов фактически ставят знак равенства между киберправом и интернет-правом<sup>9</sup>, другие исследователи считают киберправо сферой законодательства, регулирующей

<sup>6</sup> По поводу *права информационных технологий* М. А. Рожкова утверждает: «Важно обратить внимание на следующее: в определенный момент стало очевидным, что влияние технологий на право не ограничивается исключительно интернетом — значимыми для права могут оказаться разнообразные информационные технологии... В этих условиях получило развитие «право информационных технологий». Но опять-таки речь шла не о новой самостоятельной отрасли права, а о совокупности разноотраслевых правовых норм и институтов, регулирующих отношения, так или иначе связанные с применением различных информационных технологий, включая, разумеется, Интернет» (Рожкова М. А. Цифровое право (Digital Law) — что это такое и чем оно отличается от киберправа / интернет-права / компьютерного права? // Закон.ру. 15.03.2020. URL: [https://zakon.ru/blog/2020/3/15/cifrovoe\\_pravo\\_digital\\_law\\_-\\_chto\\_eto\\_takoe\\_i\\_chem\\_ono\\_otlichaetsya\\_ot\\_kiberpravainternet-pravakompy](https://zakon.ru/blog/2020/3/15/cifrovoe_pravo_digital_law_-_chto_eto_takoe_i_chem_ono_otlichaetsya_ot_kiberpravainternet-pravakompy) (дата обращения: 18.01.2023)).

<sup>7</sup> Исследователь отмечает: «Интернет-право, киберправо и проч. основываются на миксе из, во-первых, традиционных правовых институтов, которые в целом не меняются под воздействием интернета, но нуждаются в некоторых дополнительных нормах или толковании применительно к Интернету (таких, как, например, заключение договора посредством e-mail, купля-продажа товаров посредством Интернета и проч.), и, во-вторых, новых правовых институтов и положений, появившихся и развившихся именно в связи с Интернетом (в частности, законодательство об информационной безопасности, телекоммуникациях и т.д.)» (Рожкова М. А. Указ. соч.).

<sup>8</sup> Рожкова М. А. Указ. соч.

<sup>9</sup> См., например: Рассолов И. М. Право и Интернет. Теория кибернетического права : монография. 3-е изд. М. : Норма, 2022. 304 с.

правоотношения в цифровой сфере, в частности в Интернете<sup>10</sup>, т.е. институтом, сочетающим признаки и интернет-права, и права цифрового<sup>11</sup>.

Полагаем, что в институте киберправа, наряду с регулированием отношений, складывающихся по поводу использования отдельных сквозных технологий (робототехники, систем искусственного интеллекта), сохраняются нормы, регламентирующие применение менее современных технологий (в первую очередь Интернета). Это делает целесообразным признание киберправа в качестве направления совершенствования правового регулирования традиционных информационных институтов, не способных к быстрой цифровой трансформации, а также отличает его как от категории интернет-права, так и от понятия цифрового права.

Одним из таких традиционных информационных институтов является институт библиотечного дела, чья система правового регулирования изменяется крайне медленно и нуждается в адаптации к новой цифровой действительности.

Необходимо отметить, что современная система нормативных установлений в части регулирования библиотечной сферы сформировалась вскоре после вступления в силу действующей Конституции РФ<sup>12</sup>, с момента принятия двух базовых для библиотечной отрасли законов — Федеральных законов от 29.12.1994 № 78-ФЗ «О библиотечном деле»<sup>13</sup> и № 77-ФЗ «Об обязательном экземпляре документов»<sup>14</sup>.

Система правового регулирования информационных отношений в сфере библиотечного дела находится в процессе институционализации и в настоящее время включает: конституционные нормы, закрепившие основные информационные права и права граждан в сфере культуры, подзаконные акты, определяющие направления их реализации; общепризнанные принципы и нормы международного права, гарантирующие свободный доступ к информации; базовые нормы информационного законодательства, включающие правовые нормы, регулирующие библиотечное дело; иные отраслевые нормы федерального законодательства, касающиеся охраны библиотечной информации, в том числе нормы об ответственности за нарушение законодательства в области информации, культуры и сохранения культурного наследия; нормы законодательства субъектов РФ, подзаконных актов органов публичной власти в области библиотечного дела; а также

<sup>10</sup> Глушко И. Что нужно знать бизнесу о киберправе // Контур. Журнал. 07.04.2021. URL: <https://kontur.ru/articles/6059>.

<sup>11</sup> Так, например, С. С. Горохова обосновывает, что киберправо регулирует общественные отношения, связанные с правовым регулированием в сфере информационных технологий, поддерживающих работу искусственных интеллектуальных систем, роботов и объектов робототехники, т.е. де-факто рассматривает киберправо как часть категории цифрового права. См.: Горохова С. С. Идентификация искусственных интеллектуальных систем в правовом поле: основы киберправа // Юридические исследования. 2020. № 6. С. 1—11.

<sup>12</sup> Конституция РФ (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // URL: <http://www.pravo.gov.ru>, 04.07.2020.

<sup>13</sup> СЗ РФ. 1995. № 1. Ст. 2.

<sup>14</sup> СЗ РФ. 1995. № 1. Ст. 1.



локальные правовые акты библиотек; документы по стандартизации; декларативные, рекомендательные и модельные акты<sup>15</sup>.

В системе правового регулирования оборота библиотечной информации на сегодняшний день наблюдается тенденция к преобладанию подзаконного регулирования, выступающего средством адаптации сферы библиотечного дела к реалиям современного цифрового пространства, геополитическим и технологическим вызовам.

Особое место занимает распоряжение Правительства РФ от 13.03.2021 № 608-р (ред. от 15.12.2021) «Об утверждении Стратегии развития библиотечного дела на период до 2030 года»<sup>16</sup>, в котором среди проблем российских библиотек названо отсутствие полноценного доступа к сети Интернет. Подчеркивая необходимость цифровой трансформации библиотечной системы страны, базовый стратегический документ библиотечной сферы в числе механизмов (средств) достижения данной цели называет обеспечение библиотек качественным широкополосным доступом к сети Интернет; внедрение модели открытой библиотеки (OPEN+); разработку системы «одного окна» для доступа библиотек к единой ресурсной базе; разработку и внедрение методов автоматической классификации и предметизации полнотекстовых ресурсов с использованием методов искусственного интеллекта.

Таким образом, по отношению к сфере библиотечного дела в ближайшей и средней перспективе речь идет не о полной цифровой трансформации, а лишь о внедрении отдельных сквозных технологий, наряду с широким применением «традиционных» информационных технологий (в первую очередь широкополосного Интернета).

Рассматривая картину цифровизации библиотечного дела в целом, необходимо отметить, что в последнее десятилетие в сфере библиотечного дела наряду с традиционными средствами (формами) информатизации и цифровизации (Интернетом, электронными каталогами и базами данных, электронными библиотеками, оцифровкой аналоговых информационных ресурсов), получившими широкое применение, начинают внедряться и сквозные цифровые технологии, не получившие повсеместного внедрения в силу комплекса объективных и субъективных причин (в первую очередь финансового и кадрового характера).

В числе наиболее перспективных для библиотечной отрасли технологий эксперты называют Big Data, технологии облачных вычислений, робототехники, искусственного интеллекта<sup>17</sup>. Последние две технологии в библиотечной сфере нередко применяются параллельно (примеры: роботизированная система доставки книг BookBot библиотеки Университета Хантера (США, штат Северная

<sup>15</sup> О системе правового регулирования информационных отношений в сфере библиотечного дела подробно см.: *Минбалеев А. В., Пашнина Т. В.* Правовое регулирование оборота библиотечной информации // Вестник ЮУрГУ. Серия : Право. 2017. № 4. С. 89—95.

<sup>16</sup> СЗ РФ. 2021. № 12. Ст. 2072. См. также: распоряжение Правительства РФ от 07.07.2021 № 1828-р «Об утверждении плана мероприятий по реализации Стратегии развития библиотечного дела в РФ на период до 2030 года» // СЗ РФ. 2021. № 29. Ст. 5689.

<sup>17</sup> См., например: *Тикунова И. П.* Цифровизация как тренд библиотечного развития // Труды ГПНТБ СО РАН. 2021. № 3. С. 31—37.

Каролина); проект робототехники (САРМ) Библиотеки Университета Джона Хопкинса<sup>18</sup>).

В целом институт правового регулирования библиотечного дела демонстрирует достаточную инертность по отношению к внешней среде. Изменения в базовый библиотечный закон вносились и вносятся точно (касательно НЭБ, книжных памятников и т.д.), зачастую надолго отставая от практики фактического регулирования данных вопросов нормами рекомендательного характера<sup>19</sup>.

Принятие основополагающего стратегического документа сферы библиотечного дела заняло около 15 лет<sup>20</sup>. Все это свидетельствует о том, что прохождение отрасли библиотечного дела процесса цифровой трансформации и достижение показателей цифровой зрелости займет весьма продолжительное время. При этом согласно положениям Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы<sup>21</sup> библиотека обязана сохранять возможность получения российскими гражданами услуг в нецифровой традиционной форме.

Таким образом, на данном этапе развития библиотечного дела, не связанном с широким внедрением в библиотечную практику сквозных цифровых технологий, представляется целесообразной трансформация системы правового регулирования оборота библиотечной информации в контексте не цифрового права, а права киберпространства (киберправа), позволяющего как осуществлять правовое регулирование применения отдельных наиболее перспективных для сферы библиотечного дела сквозных цифровых технологий (в первую очередь робототехники и технологий искусственного интеллекта), так и сохранить традиционные

<sup>18</sup> *Kaijun Yu, Ruiyi Gong, Longjie Sun, Chunguo Jiang. The Application of Artificial Intelligence in Smart Library // International Conference on Organizational Innovation: Advances in Economics, Business and Management Research. 2019. Vol. 100. P. 708—713. URL: <https://www.atlantis-pess.com/proceedings/icoi-19/125919402> (дата обращения: 18.01.2023).*

<sup>19</sup> Например, приказ Министерства культуры РФ № 1905 «Об утверждении правил предоставления и размещения общедоступными библиотеками находящейся в их фондах информационной продукции, содержащей информацию, запрещенную для распространения среди детей в соответствии с частью 2 статьи 5 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»» (URL: [www.pravo.gov.ru](http://www.pravo.gov.ru), 27.07.2020) был принят 06.12.2019. Однако созданный национальной библиотечной ассоциацией документ рекомендательного характера по данному вопросу применялся с 2013 г. — это Рекомендации Российской библиотечной ассоциации по реализации норм Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» в общедоступных библиотеках России, осуществляющих обслуживание пользователей до 18-летнего возраста (утверждены на Всероссийском библиотечном конгрессе: XVIII Ежегодной конференции Российской библиотечной ассоциации в Пензе 14 мая 2013 г.) (Рос. библ. ассоциация. URL: <http://www.rba.ru/content/about/doc/recom.php>).

<sup>20</sup> См.: Пашнина Т. В., Минбалева А. В. О Стратегии развития библиотечного дела в Российской Федерации на период до 2030 года // Информационное право. 2020. № 4. С. 33—36.

<sup>21</sup> Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.



объекты и способы регулирования в рамках сложившихся правоотношений в библиотечно-информационной сфере.

Данный подход позволит адаптировать правовое регулирование библиотечно-информационной деятельности к цифровой среде на период внедрения в библиотечную практику сквозных цифровых технологий при соблюдении баланса предоставления библиотечно-информационных услуг в традиционной и электронной формах.

### БИБЛИОГРАФИЯ

1. *Глушко И.* Что нужно знать бизнесу о киберправе // *Контур. Журнал.* — URL: <https://kontur.ru/articles/6059>, 07.04.2021 (дата обращения: 18.01.2023).
2. *Горохова С. С.* Идентификация искусственных интеллектуальных систем в правовом поле: основы киберправа // *Юридические исследования.* — 2020. — № 6. — С. 1—11.
3. *Леонтьев А. Н.* Киберправо : учебное пособие. — Волгоград : ВолгГТУ, 2021. — 80 с.
4. *Мажорина М. В.* Цифровые платформы и международное частное право, или Есть ли будущее у киберправа? // *Lex russica.* — 2019. — № 2. — С. 107—120.
5. Механизмы и модели регулирования цифровых технологий / А. В. Минбалеев, А. В. Мартынов, Г. Г. Камалова [и др.]. — М. : Проспект, 2023. — 264 с.
6. *Минбалеев А. В.* Проблемы цифрового права : учебное пособие. — Саратов : Амирит, 2022. — 233 с.
7. *Минбалеев А. В., Пашнина Т. В.* Правовое регулирование оборота библиотечной информации // *Вестник ЮУрГУ.* — Серия : Право. — 2017. — № 4. — С. 89—95.
8. *Пашнина Т. В., Минбалеев А. В.* О Стратегии развития библиотечного дела в Российской Федерации на период до 2030 года // *Информационное право.* — 2020. — № 4. — С. 33—36.
9. Правовое регулирование цифровых технологий в России и за рубежом. роль и место правового регулирования и саморегулирования в развитии цифровых технологий : монография / под ред. А. В. Минбалеева. — Саратов : Амирит, 2019. — 207 с.
10. *Рассолов И. М.* Право и Интернет. Теория кибернетического права : монография. — 3-е изд. — М. : Норма, 2022. — 304 с.
11. *Рожкова М. А.* Цифровое право (Digital Law) — что это такое и чем оно отличается от киберправа / интернет-права / компьютерного права? // URL: [https://zakon.ru/blog/2020/3/15/cifrovoe\\_pravo\\_digital\\_law\\_-\\_chto\\_eto\\_takoe\\_i\\_chem\\_ono\\_otlichaetsya\\_ot\\_kiberpravainternet-pravakompy](https://zakon.ru/blog/2020/3/15/cifrovoe_pravo_digital_law_-_chto_eto_takoe_i_chem_ono_otlichaetsya_ot_kiberpravainternet-pravakompy) (дата обращения: 18.01.2023).
12. *Тикунова И. П.* Цифровизация как тренд библиотечного развития // *Труды ГПНТБ СО РАН.* — 2021. — № 3. — С. 31—37.
13. Цифровая трансформация: вызовы праву и векторы научных исследований : монография / под общ. ред. А. Н. Савенкова ; отв. ред. Т. А. Полякова, А. В. Минбалеев. — М. : РГ-Пресс, 2021. — 344 с.

14. Цифровое право / А. Дюфло, Л. В. Андреева, В. В. Блажеев [и др.]. — М. : Проспект, 2020. — 640 с.
15. *Jambholkar L.* Cyber law. issues and perspectives // *The Indian j. of intern. law.* — 2000. — Vol. 40. — № 3. — P. 559—562.
16. *Kaijun Yu, Ruiyi Gong, Longjie Sun, Chunguo Jiang.* The Application of Artificial Intelligence in Smart Library // *International Conference on Organizational Innovation: Advances in Economics, Business and Management Research.* — 2019. — Vol. 100. — P. 708—713. — URL: <https://www.atlantis-press.com/proceedings/icoi-19/125919402>.





**Валентин Николаевич  
ШЕЛЬМЕНКОВ,**

преподаватель кафедры  
информационного права  
и цифровых технологий  
Университета имени  
О.Е. Кутафина (МГЮА)  
[vnshelmenkov@msal.ru](mailto:vnshelmenkov@msal.ru)  
125993, Россия, г. Москва,  
ул. Садовая-Кудринская, д. 9

## Основные принципы обработки правовой информации в информационных правовых системах

**Аннотация.** Одно из основных свойств права — его системность. Массив правовой информации не является простым набором текстовых документов. Правовые документы по своей природе связаны между собой. Следовательно, обработка правовой информации заключается в обнаружении и раскрытии этих связей и построении на их основе целостной, внутренне обоснованной системы. В статье раскрываются основные принципы обработки правовой информации в информационных правовых системах.

**Ключевые слова:** правовая информация, обработка правовой информации, система, информационная правовая система.

DOI: 10.17803/2311-5998.2023.102.2.146-152

**VALENTIN N. SHELMEKOV,**

lecturer of the Department of information law  
and digital technology

of the Kutafin Moscow State Law University (MSAL)

[vnshelmenkov@msal.ru](mailto:vnshelmenkov@msal.ru)

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

### Basic principles of processing legal information in information legal systems

**Abstract.** One of the main properties of law is its consistency. The array of legal information is not a simple set of text documents. Legal documents by their very nature are interconnected. Therefore, the processing of legal information consists in the detection and disclosure of these links and the construction of a holistic, internally sound system based on them.

**Keywords:** legal information, legal information processing, system, legal information system.

**П**ринципы — это основные исходные положения какой-либо теории, учения, мировоззрения. То есть принцип — это одно из наиболее общих понятий науки, и это понятие обозначает не все, а лишь некоторые сведения, совокупность каких-то данных, знаний. Принципы права представляют собой руководящие идеи, характеризующие содержание права, его сущность и назначение в обществе<sup>1</sup>.

Право строится и функционирует на определенных принципах, выражающих его сущность и социальное назначение, главные свойства и особенности. Принципами права должны руководствоваться все участники информационных отношений — органы законодательной, исполнительной, судебной власти, организации и граждане. Соблюдение принципов может служить мерилom правового и социального характера государства, эффективности защиты информационных прав и законных интересов человека и гражданина<sup>2</sup>.

Центральным этапом в процессе обращения информации в информационной системе является обработка информации. В зависимости от общего назначения системы на данном этапе проводится систематизация собранной информации, реализуются поисковые, логические или другие аналитические процедуры<sup>3</sup>.

Что касается правовых документов, то здесь речь может идти о внешних и внутренних связях. Внешние связи заданы самой структурой национальной правовой системы. Например, в отношении каждого конкретного постановления Правительства РФ можно говорить, что данный документ входит в различные подсистемы: подсистему актов федеральных органов власти; подсистему актов высших органов исполнительной власти; подсистему актов, издаваемых в форме постановлений; подсистему актов, изданных за определенный интервал времени; подсистему актов, изданных по определенной тематике, и т.д.

Таким образом, каждый документ является уникальной точкой пересечения различных реквизитов. При этом все реквизиты, рассматриваемые по отдельности, являются элементами более общих систем, характеризующих формальную сторону права. В свою очередь, формальные признаки определяют юридическую силу правовых документов, т.е. саму специфику их существования и применения.

Например, тот факт, что некий документ является постановлением Правительства РФ, обязывает правоприменителя соотнести этот документ, с одной стороны, с федеральными законодательными актами, которым данное постановление не должно противоречить, а с другой — с актами министерств и ведомств, которые сами, в свою очередь, не должны противоречить актам Правительства РФ.

То, что Правительство РФ выразило свою волю в форме постановления, а не распоряжения, свидетельствует о нормативном, а не о распорядительном характере акта. Дата издания данного документа также может иметь правовое значение в свете известного принципа *lex posterior derogat lex priori*.

Обработка правовой информации немислима без учета указанной выше специфики. Следовательно, подключение правовых документов к банку данных является в первую очередь включением их в специально подготовленную информационную среду, которая должна базироваться на действующей правовой системе нашего государства. Можно сказать, что данная информационная среда сама по себе является выражением национальной правовой системы.

<sup>2</sup> Чубукова С. Г. О принципах информационного права // Российское право в Интернете. 2000. № 3. С. 8.

<sup>3</sup> Чубукова С. Г., Элькин В. Д. Основы правовой информатики (юридические и математические вопросы информатики) : учебное пособие / под ред. М. М. Рассолова, В. Д. Элькина. М., 1999.



Есть базовые признаки правовой информации: вид, номер документа, дата и др. К статусным реквизитам относится и информация о юридической силе, или о степени важности данного документа в общей иерархии правовых документов. Данная иерархия находит свое отражение в одном из способов представления списков документов, содержащихся в информационном банке — в так называемой «сортировке по юридической силе», когда в начале списка представлены документы, обладающие большей юридической силой (важностью). Разработка такой таблицы является одним из ключевых аспектов создания и поддержания в актуальном состоянии информационно-правовой среды.

Важным компонентом информационно-правовой среды является классификация тематического содержания правовых документов.

Данная проблематика реализуется в двух направлениях. Во-первых, каждый правовой документ должен найти свое место в отраслевой структуре правовой информации. Такая структура организована по иерархическому признаку, обеспечивая тем самым логическое движение от общего к частному. На верхнем уровне классификации выделены основные отрасли национального законодательства: основы государственно-правового устройства, гражданское право, трудовые отношения, уголовное право и т.д. На следующих уровнях представлены подотрасли и институты соответствующих отраслей.

Разработку такой структуры следует вести на основе Классификатора правовых актов, утвержденного Указом Президента РФ от 15.03.2000 № 511<sup>4</sup>, а также анализа имеющегося массива правовой информации, дифференцированного по различным видам, опираясь на новейшие исследования в области теории классификации информации.

Помимо иерархической классификации, систематизация правовой информации должна предусматривать и ситуационный подход. Логическое движение от общего к частному не исчерпывает всех возможных вариантов работы с правовой информацией. Довольно часто правовой вопрос формулируется исключительно как частная проблема, как точка пересечения различных аспектов, не поддающихся простому отраслевому анализу.

Например, пользователя может интересовать тема технического осмотра транспортных средств. При этом данный конкретный пользователь может слабо представлять место этой темы в общей отраслевой структуре правовой информации. Для этого в информационной среде должен быть предусмотрен обширный набор элементарно сформулированных практических ситуаций, собранных в простую алфавитную структуру, которая позволяет найти прямой ответ на четко сформулированный запрос.

Создание такой структуры основывается на изучении реальных потребностей пользователей правовой информации, прогнозировании этих потребностей на основе анализа содержания нормативных актов и разнообразных аналитических материалов по правовой тематике.

Все указанные выше компоненты информационной правовой среды описывают внешние связи между документами. Эти компоненты образуют форму, в которую вливается поток правовой информации.

<sup>4</sup> Указ Президента РФ от 15.03.2000 № 511 «О классификаторе правовых актов» // СЗ РФ. 2000. № 12. Ст. 1260.

Помимо этого, при создании информационной правовой среды необходимо учитывать и наличие внутренних связей между документами. Система обработки информации должна быть пригодна для обнаружения и отображения этих связей.

Специфика правовой информации заключается в том, что довольно часто эти внутренние связи имеют прямое юридическое значение, оказывают влияние на правовой статус документа, определяют характер его применения.

Речь идет в первую очередь о связи между подзаконным актом и актом, во исполнение которого он принят. Например, если Министерство финансов своим приказом утверждает форму налоговой декларации, то в этом случае реализуется некое полномочие данного органа исполнительной власти, предусмотренное путем прямого предписания в Налоговом кодексе РФ. В приказе содержится ссылка на соответствующие нормы НК РФ, а в самом НК РФ обнаруживается норма, которая была исполнена посредством издания данного приказа.

Таким образом, между двумя документами установилась правовая связь. Подобные вертикальные связи возникают также между судебными актами и нормами, на основании которых приняты эти акты; между проектами законов о внесении изменений и теми законами, которые планируется изменить; между комментариями и комментируемыми актами и т.п.

Эти связи могут быть выражены с разной долей явности. Например, тот же Налоговый кодекс РФ содержит упоминание таможенной декларации, не указывая при этом ни конкретного акта, которым она утверждена, ни порядка издания этого акта, так как этот вопрос регулируется смежной отраслью законодательства. Довольно часто в правовых актах содержится общая отсылка — «в соответствии с федеральными законами» или «согласно действующему законодательству» и т.п. В этом случае обнаружение таких связей берут на себя обработчики правовой информации.

Кроме того, большую роль в обработке правовой информации играет внесение изменений и дополнений, создание новых редакций правовых актов. Эту роль также выполняют обработчики правовой информации, напрямую реализовывая связь между изменяющим и изменяемым документом.

Нередко разные акты содержат близкий предмет регулирования, при этом отдельные нормы не всегда могут быть вполне согласованы между собой. В этом случае внутренние связи между документами позволяют обнаружить возможные противоречия и пробелы в законодательстве.

Компьютерные технологии позволяют отображать внутренние связи между документами в форме гипертекстовых ссылок, обеспечивающих мгновенный переход от одного документа к нужному фрагменту другого документа.

Обратное применение данной технологии дает очень ценный результат — информационно-правовые системы, базирующиеся на принципе «полного гипертекста», при котором отображаются все явные и неявные ссылки, позволяют находить все документы, которые ссылаются на интересующую пользователя правовую норму.

Иными словами, если у пользователя имеется потребность в изучении определенной статьи кодекса или пункта закона, ему предоставляется возможность построить список всех документов, в которых упоминается данная статья или пункт. Накладывая на эту возможность функцию видовой дифференциации,



можно достичь желаемого результата при поиске, например, судебной практики по интересующей нас правовой норме или комментариев к заинтересовавшему нас судебному решению и т.п.

Указанные выше возможности по отображению внутренних связей между документами основываются на кропотливой и повседневной аналитической работе по их выявлению. Для проведения такой работы необходимо задействовать большой штат профессиональных квалифицированных специалистов с широким кругозором, хорошо ориентирующихся в действующем законодательстве. Результаты такой работы отражают и общее состояние юридической техники в национальной правовой системе.

Помимо такого, чисто юридического подхода к обнаружению внутренних связей между документами, возможен и иной — лингвосемантический подход, которым не должны пренебрегать разработчики современных информационно-правовых систем. Достигнутый уровень развития знаний в области лингвистики и семантики позволяет рассматривать текст любого документа как сложную структуру, поддающуюся математическому, статистическому анализу. А это, в свою очередь, является предпосылкой для использования компьютерных средств обработки информации. Во многих новейших программных приложениях, связанных с поиском информации, используются различные технологии учета степени «похожести документов».

Такие технологии позволяют отбирать из всего массива информации те документы, которые более других похожи на определенный прототип. В итоге обеспечивается возможность сортировки найденных документов по степени релевантности, степени соответствия. При этом в качестве критерия схожести используется именно текстовая близость документов, определяемая на основе неких универсальных математически выраженных критериев.

Применение таких средств в отношении правовой информации открывает новые перспективы. Сложный профессиональный анализ внутренних связей между документами, помимо всех преимуществ «человеческого фактора», парадоксальным образом содержит и недостатки, которые присущи этому фактору. Любая субъективность нуждается в объективном подкреплении.

Кроме того, субъективный профессиональный взгляд в большей степени ориентируется на вертикальные связи между документами («закон — подзаконный акт», «норма — ее разъяснение», «изменяющий документ — изменяемый документ» и т.д.), охватить же горизонтальные связи между большим массивом документов человеку достаточно сложно. Если, например, обратиться к судебной практике, то, с одной стороны, необходимо отметить огромное разнообразие тем, а с другой — большое число документов по отдельным темам (достаточно вспомнить об обширной практике по спорам, связанным с возмещением экспортного НДС).

Также возникает проблема с выделением точки близости различных документов. Ведь если продолжать говорить о судебных актах, то они с точки зрения содержания представляют собой целый конгломерат различных тем. И если связь между двумя документами устанавливает эксперт, то он неизбежно обращает большее внимание только на те темы, которые интересны именно ему в силу тех или иных профессиональных или жизненных причин. И то, что было интересно в данном документе одному эксперту, может быть не интересно другому.

Не всегда помогают и ссылки в судебных актах на одни и те же нормы. Применяя одну и ту же правовую норму, суд может рассматривать ее с разных сторон применительно к специфике фактической стороны данного дела. В этом случае вертикальная связь с общей нормой еще не гарантирует горизонтальной близости судебных актов, которые на нее ссылаются.

В связи с этим и возникает потребность в обнаружении текстуально близких документов. Причем актуальна она в большей степени именно в отношении судебных актов и компактных разъяснительных материалов в форме «вопрос — ответ», которая очень популярна и востребована, поскольку отображает наиболее сложные и злободневные проблемы правоприменительной практики, различные, подчас противоположные, профессиональные суждения. Поэтому, если пользователь нашел некое разъяснение, то вполне предсказуемым будет желание найти дополнительные материалы по тому же вопросу, подтверждающие или опровергающие имеющееся мнение.

Для судебной практики технология поиска похожих документов позволяет решать задачу, которая реально стоит не только перед потенциальными участниками споров, которым бывает полезно спрогнозировать судебные перспективы, но и в первую очередь перед судебными инстанциями. Более того, эта задача закреплена на нормативном уровне. Если же учесть, что ежегодно в арбитражной системе рассматривается порядка миллиона дел, выявить это единообразие без использования современных информационно-поисковых систем становится практически невозможно.

Что касается нормативных актов, то проблема поиска похожих документов также может быть актуальна. Ее решение позволило бы выявлять пересекающееся, дублирующее правовое регулирование, что сократило бы вероятность возникновения противоречий в действующем законодательстве, т.е. могло бы стать эффективным инструментом в правотворческой деятельности.

Достижение положительных результатов в отношении судебной практики и аналитических материалов открывает перед нами новые направления исследований в этой сфере. Здесь могут выявиться специфические сложности. Вряд ли может возникнуть реальная потребность искать документ, похожий на Налоговый кодекс или Закон о рекламе. Каждый нормативный акт уникален. Скорее речь должна идти о похожих нормах, а не о похожих документах. Но в то же время большое терминологическое разнообразие в изложении близких по своему содержанию норм обязывает нас углублять исследования в области построения понятийных тезаурусов и онтологий, позволяющих выявлять текстуальную близость между документами по более сложным параметрам. И здесь наши разработки находятся в общем контексте развития лингвосемантических технологий русскоязычного сегмента данной области гуманитарных знаний.

Горизонтальные и вертикальные внутренние связи между документами выполняют свои специфические функции в организации информационно-правовой среды. И если различные типы горизонтальных связей являются плодом работы специалистов-юристов, занимающихся текущей обработкой правовой информации, то выявление вертикальных связей по принципу текстуальной схожести достигается посредством компьютерной обработки информации с применением систем лингвосемантического анализа.



Таким образом, можно заключить, что обработка правовой информации должна основываться на общем принципе учета и выявления внешних и внутренних связей между документами для создания тем самым сложно организованной информационно-правовой среды.

#### БИБЛИОГРАФИЯ

1. Теория государства и права / отв. ред. В. Д. Перевалов. — М. : Норма, 2006.
2. Чубукова С. Г. О Принципах информационного права // Российское право в Интернете. — 2000. — № 3. — С. 8—13.
3. Чубукова С. Г., Элькин В. Д. Основы правовой информатики (юридические и математические вопросы информатики) : учебное пособие / под ред. М. М. Рассолова, В. Д. Элькина. — М., 1999.

## О некоторых юридически значимых особенностях технологий облачных вычислений

**Аннотация.** В статье исследуются основные юридические подходы в отношении определения правовой сущности технологий облачных вычислений, анализируются их устойчивые признаки и преимущества, а также аккумулируются риски и угрозы применения. Отмечается, что в Российской Федерации правовое обеспечение сферы технологий облачных вычислений недостаточно, в том числе отсутствует дефинитивный аппарат, не снята актуальность принятия специального закона об информационной безопасности, разделы которого должны быть посвящены правовым основам кибербезопасности при использовании технологий облачных вычислений, что заложило бы основу для комплексного подхода к правовому управлению безопасностью между различными участниками цифровой среды. Поэтому исследование правовой природы и признаков технологий облачных вычислений с выделением видовых характеристик, а также выявление угроз и рисков в процессе их применения представляется перспективным направлением для дальнейшего развития механизма правового регулирования сферы цифровых технологий.

**Ключевые слова:** объект права; информационные технологии; сквозные технологии; цифровые технологии; облачные вычисления; технологии облачных вычислений.



**Елена Викторовна  
ХОЛОДНАЯ,**

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

DOI: 10.17803/2311-5998.2023.102.2.153-161

**ELENA V. KHOLODNAYA,**

Associate Professor of the Department  
of information law and digital technologies  
of the Kutafin Moscow State Law University (MSAL),  
Cand. Sci. (Law), Associate Professor  
[evholodnaya@msal.ru](mailto:evholodnaya@msal.ru)

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

### About some Legally Significant Features of Cloud Computing Technologies

**Abstract.** The article examines the main legal approaches to determining the legal essence of cloud computing technologies, analyzes their stable features and advantages, and accumulates risks and threats of application. It is noted that in the Russian Federation, legal support for the sphere of cloud computing technologies is insufficient, including the absence of a definitive apparatus, the relevance of the adoption of a special law on information security, sections of which should be devoted, inter alia, to the legal foundations of

© Холодная Е. В., 2023

*cybersecurity when using cloud computing technologies, laying the foundation for an integrated approach to legal security management, has not been removed between different participants of the digital environment. Therefore, the study of the legal nature and features of cloud computing technologies with the allocation of specific characteristics, as well as the identification of threats and risks in the process of using cloud computing technologies seems to be a promising direction for the further development of the mechanism of legal regulation of the digital technology sphere.*

**Keywords:** *object of law; information technologies; end-to-end technologies; digital technologies; cloud computing; cloud computing technologies.*

Сетевые информационные системы превратились в устойчивый признак повседневной жизни благодаря быстрой цифровой трансформации и взаимосвязанности информационного общества<sup>1</sup>. При этом отмечается, что говорить о цифровой трансформации, например частного сектора, можно в том случае, если не менее 75 % бизнес-структур используют для своей деятельности вычислительные облачные сервисы, большие данные, искусственный интеллект<sup>2</sup>.

Так, теория облачных вычислений предложена еще в 1970-х гг. Джозефом Ликлайдером (J. C. R. Licklider) при разработке сети ARPANET (Advanced Research Projects Agency Network), суть которой сводилась к тому, что каждый субъект будет подключен к сети как ресурсу для получения не только данных, но и программного обеспечения. Другой ученый — Джон Маккартни (John McCarthy) предположил, что вычислительные мощности будут предоставляться пользователям как услуга (сервис). Как отмечают специалисты, в 1999 г. компания Salesforce.com первая предоставила доступ к своему программному приложению через сайт по принципу «программное обеспечение как услуга» (SaaS), далее идея развилась в создание облачного веб-сервиса компанией Amazon в 2002 г. для хранения и вычисления данных и популяризировалась через облачные технологии Google и др.<sup>3</sup>

На сегодняшний день технологии облачных вычислений — это перспективное направление развития цифровых технологий, представляющее собой метод распределенной обработки данных, при котором технологические ресурсы и программный инструментарий предоставляются пользователю виртуально в аренду.

Облачные технологии можно понимать и как способ хранения, обработки и использования цифровых данных на удаленных компьютерах (серверах), доступ к которым осуществляется через информационно-телекоммуникационные сети. С помощью технологий облачных вычислений создается специализированная

<sup>1</sup> Amelin R., Channov S., Dobrobaba M., Kalinina L., Kholodnaya E. Transformation of legal personality in the context of the development of modern digital technologies // International Journal of Computer Science and Network Security. 2022. Vol. 22. № 11. С. 294—302.

<sup>2</sup> Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance) // URL: <https://eur-lex.europa.eu> (дата обращения: 17.01.2023).

<sup>3</sup> Облачные вычисления, краткий обзор или статья для начальника // URL: <https://habr.com/ru/post/111274/> (дата обращения: 18.01.2023).

виртуальная рабочая среда в Интернете или в корпоративной компьютерной сети с предоставлением пользователю цифровых возможностей для решения разнообразных задач<sup>4</sup>.

При этом пользователи могут использовать практически неограниченную вычислительную мощность по запросу, не прибегая к финансовым вложениям для удовлетворения своих потребностей и получая доступ к своим данным из любого места с подключением к Интернету или локальной сети с использованием веб-технологий.

Таким образом, технологии облачных вычислений имеют потенциал для сокращения расходов пользователей на ИТ за счет сокращения капитальных и операционных затрат, увеличения коэффициента использования оборудования и позволяют наращивать производительность за счет возможностей для совместного использования цифровой инфраструктуры между различными пользователями<sup>5</sup>.

Сегодня модели облачных сервисов классифицируют на следующие основные виды: инфраструктура как услуга (IaaS); платформа как услуга (PaaS); программное обеспечение как услуга (SaaS); сеть как услуга (NaaS)<sup>6</sup>.

Модели развертывания технологий облачных вычислений в зависимости от доступа подразделяются:

- на частные (private cloud), пользователями такого облака является ограниченный круг лиц, как правило, это сотрудники и контрагенты компании-потребителя. Такое облако может быть доступно только внутри локальной сети предприятия и (или) посредством VPN-соединений;
- публичные (public cloud), в которых облачные сервисы и ИТ-ресурсы распределяются между всеми и любыми пользователями;
- гибридные (hybrid cloud), которые могут сочетать инфраструктуру, платформу и приложения от разных поставщиков услуг, а также предоставлять сервисы, часть из которых доступна для ограниченного круга пользователей, часть — для сообщества, а некоторые и публично;
- общественные (community cloud), пользователями такого облака являются участники сообщества, связанного определенными регламентными соглашениями;
- модель интерклауд (intercloud) — подразумевает глобальное «облако облаков» как совокупность групп взаимосвязанных серверов узлов сети, взаимодействующих посредством «сети сетей» Интернет и др.<sup>7</sup>

Существует точка зрения, что технологии облачных вычислений — это развивающаяся парадигма, связанная с повсеместным распространением и быстрым

<sup>4</sup> Жигалов Н. Ю. Облачные вычислительные технологии в судебно-экспертной деятельности // Российский следователь. 2018. № 4. С. 11—14.

<sup>5</sup> Информационно-технологическое обеспечение юридической деятельности (LegalTech). М. : Проспект, 2022. 368 с.

<sup>6</sup> Облачные вычисления (мировой рынок) // URL: [https://www.tadviser.ru/index.php/статья:облачные\\_вычисления\\_\(мировой\\_рынок\)](https://www.tadviser.ru/index.php/статья:облачные_вычисления_(мировой_рынок)) (дата обращения: 19.01.2023).

<sup>7</sup> Беккер М. Я., Гатчин Ю. А., Кармановский Н. С., Терентьев А. О., Федоров Д. Ю. Информационная безопасность при облачных вычислениях: проблемы и перспективы // URL: <https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-pri-oblachnyh-ychisleniyah-problemy-i-perspektivy/viewer> (дата обращения: 19.01.2023).



развитием этой технологии и соответствующих услуг<sup>8</sup>. Вычислительные ресурсы технологий облачных вычислений включают в себя: сети, серверы и другую инфраструктуру, операционные системы, программное обеспечение, хранилища, приложения и службы. На сегодняшний день не существует общепринятого юридического определения технологий облачных вычислений или облачных сервисов. Поэтому особенно важным представляется поиск ключевых устойчивых характеристик этой цифровой технологии для возможностей создания максимально эффективного механизма правового регулирования отношений, возникающих в связи с их применением.

К таким константам технологии облачных вычислений относят:

- сетевой удаленный доступ. Характеризует возможность получения услуг через сети и механизмы использования разнородных технических платформ (мобильных телефонов, рабочих станций, планшетов и т.п.) пользователей. Суть в том, что пользователи могут получить доступ к виртуальной среде и данным с любого технического устройства, подключенного к сети;
- измеримость сервиса с позиции используемых цифровых ресурсов. Позволяет пользователю оплачивать услуги по факту запроса. Данный признак позволяет снизить, например, государственные расходы и увеличить общественные выгоды;
- мультиаренду облачных сервисов. Характеризуется тем, что ресурсы облака могут быть распределены между несколькими изолированными друг от друга пользователями, но при этом каждый достигает эффекта производительности от работы на своем техническом устройстве;
- самостоятельное обслуживание по запросу без взаимодействия с администратором облачного сервиса. Сокращает временные издержки и усилия по получению цифровых услуг;
- эластичность пула. Характеризует возможность увеличивать или уменьшать доступные ресурсы в зависимости от рабочей нагрузки и спроса;
- масштабируемость облачных сервисов. Характеризует возможности гибкого распределения вычислительных ресурсов независимо от их территориального расположения при колебаниях запросов. Иными словами, данный признак расширяет возможности пользователя при его разнообразии географического местоположения или низком потенциале собственных ресурсов.

Исходя из перечисленных признаков, к преимуществам технологий облачных вычислений можно отнести:

- доступность данных с любого технического устройства, подключенного к информационно-телекоммуникационной сети;
- сохранность данных при выходе из строя конечного оборудования пользователя;
- актуальность данных и программного обеспечения при регулярных обновлениях сервисов;
- среду для хранения больших данных;

<sup>8</sup> European Parliament resolution of 16 February 2017 on the European Cloud Initiative (2016/2145(INI)) // URL: <https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3A52017IP0052&qid=1673960581825> (дата обращения: 17.01.2023).

- независимость от вида операционной системы;
- многопользовательский доступ для совместной работы с данными и приложениями;
- виртуализацию вычислительных ресурсов, что снижает энергетические, эксплуатационные и материальные расходы, повышает коэффициент использования технического оборудования и сетевой инфраструктуры и др.

Также исходя из характерных признаков, можно выделить и недостатки технологий облачного вычисления:

- создание «иллюзии неограниченных ресурсов»;
- зависимость пользователя от выделенных линий и широкополосных соединений;
- зависимость пользователя от распределенных информационных систем поставщика облачных сервисов;
- неизвестность для пользователя месторасположения сервера, хранящего данные;
- неизвестность для пользователя состава цепочки субподрядчиков облачных услуг и непрозрачность распределения между ними прав и обязанностей и др.

Так, согласно исследованию Европейского агентства по сетевой и информационной безопасности (ENISA) основными рисками, связанными применением технологий облачных вычислений, являются<sup>9</sup>:

- потеря управления и контроля над безопасностью со стороны пользователя облачных сервисов;
- блокировки непрерывности обслуживания, например при переносе данных и услуг обратно во внутреннюю ИТ-среду — форматы данных и интерфейсы сервисов в облаке не имеют единых стандартов;
- сбой изоляции (механизмов, разделяющих хранилище, память и маршрутизацию между соарендаторами);
- репутационный ущерб одного облачного пользователя, что из-за недобросовестной практики службы безопасности поставщика услуг может повлиять на репутацию других пользователей в облаке;
- виртуализация облачных услуг, которая означает, что реальная операционная платформа поставщика услуг скрыта от пользователей;
- небезопасное или неполное удаление данных, когда неясно, как пользователь может убедиться, что данные действительно были удалены и др.

Сказанное актуализирует вопросы кибербезопасности — по обеспечению защиты данных, противодействию рискам их утечки, определению юрисдикции и юридической ответственности поставщиков облачных сервисов и гарантий надлежащего качества облачных услуг, аутентификации и идентификации и др. Основными мировыми моделями по решению поставленных задач являются принятие как стратегических актов, так и специальных законов по регулированию отношений в области применения технологий облачных вычислений.

В США в 2011 г. была разработана Федеральная стратегия использования облачных вычислений, определившая планы внедрения технологий облачных

<sup>9</sup> Cloud Security Guide for SMEs // URL: <https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes> (дата обращения: 19.01.2023).



вычислений в государственные органы и правила, которым должны соответствовать сервисы<sup>10</sup>. Правительством США сертифицированы облачные сервисы, разработанные компанией Google для нужд государства. США является мировым лидером по производству облачных сервисов.

Однако юридическая практика государства об экстерриториальном применении иностранных законов в отношении данных, хранящихся в облачных сервисах за рубежом, вызывает озабоченность в отношении возможных злоупотреблений и нарушений прав и свобод человека<sup>11</sup>, что, например, вытекает из дела «США против Microsoft» (Microsoft Warrants, 2014 г.), по которому суд постановил, что местонахождение данных не имеет существенного значения для исполнения требования суда США (судебного приказа) на раскрытие содержания электронной почты и других записей в конкретной учетной записи электронной почты MSN в соответствии с Законом США о хранении сообщений<sup>12</sup> и др.

Также Закон 2018 г. «Об уточнении правомерности использования хранящихся за рубежом данных» (The Clarifying Lawful Overseas Use of Data Act (Cloud Act)) упрощает правоохранительным органам США доступ к данным пользователей Интернета (электронной переписке, документам и иным данным, хранящимся онлайн) вне зависимости от того, в какой стране они хранятся.

В ЕС особо отмечается, что пользователи облачных сервисов должны быть уверены в надежности защиты сервисов и конфиденциальности данных: данные должны быть всегда доступны для них и недоступны неавторизованным пользователям. На особом контроле — риски безопасности технологий облачных вычислений, которые связаны как с многопользовательским доступом к данным, так и с общими ресурсами. К ним относят: контроль доступа, хранение и защиту данных, переносимость данных, целостность данных и виртуализацию.

Фактически пользователь передает контроль над безопасностью поставщику облачных услуг, что затрудняет оценку достаточной степени соответствия требованиям безопасности. Поэтому в связи с распространенностью, с одной стороны, и высокой чувствительностью к указанным рискам — с другой, в отношении технологий облачных вычислений на уровне ЕС принят ряд инициатив с упором на обеспечение кибербезопасности данных сервисов<sup>13</sup>.

<sup>10</sup> Federal Cloud Computing Strategy // URL: <https://cloud.cio.gov/strategy/> (дата обращения: 19.01.2023).

<sup>11</sup> См. подробнее: Карцхия А. А. «Облачные» технологии: российское и зарубежное законодательство и практика правоприменения // Мониторинг правоприменения. 2018. № 2 (27). С. 36—41; Викторова Н. Г., Шухов Ф. Г. Цифровая экономика: развитие облачных технологий в России и за рубежом // Век качества. 2019. № 2. С. 81—90. URL: <http://www.agequal.ru/pdf/2019/219006.pdf> (дата обращения: 19.01.2023).

<sup>12</sup> Hurley Lawrence, Volz Dustin (February 27, 2018). U.S. Supreme Court wrestles with Microsoft data privacy fight. // Reuters. Retrieved. April 2, 2018 — via The Globe and Mail.

<sup>13</sup> European Parliament resolution of 16 February 2017 on the European Cloud Initiative (2016/2145(INI)) // URL: <https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a52017ip0052&qid=1673960581825> (дата обращения: 15.01.2023); Executive summary of the Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the potential of cloud computing in Europe' // URL: <https://eur-lex.europa.eu/>

Стратегия ЕС «Раскрытие потенциала облачных вычислений в Европе» нацелена на создание безопасной системы контрактов, систематизацию существующих стандартов облачных вычислений и создание единой экосистемы для эффективного взаимодействия европейских стран.

Специализированный закон по урегулированию отношений в связи с применением облачных технологий принят, например, в Республике Корея — Закон «О продвижении облачных вычислений и защите пользователей», которым предусмотрена возможность использования частных облачных сервисов в государственном секторе, установлена обязанность провайдера сообщать об утере информации пользователям, ответственность провайдера за ущерб пользователю и др. Другим примером является Закон Чешской Республики 2013 г. о защите персональных данных в облачных сервисах, дополненный в 2019 г.<sup>14</sup>

В России вопросы развития технологий облачных вычислений затрагиваются в стратегических документах как направления развития российских информационных и коммуникационных технологий<sup>15</sup>; принят ряд стандартов по обеспечению информационной безопасности при использовании технологий облачных вычислений<sup>16</sup>; в качестве нормативных регуляторов можно назвать законы об

[legal-content/en/txt/?uri=celex%3a52013xx0903%2801%29&qid=1673945154828#ntc7-c\\_2013253en.01000301-e0007](https://www.legal-content/en/txt/?uri=celex%3a52013xx0903%2801%29&qid=1673945154828#ntc7-c_2013253en.01000301-e0007) (дата обращения: 15.01.2023).

<sup>14</sup> Новый чешский закон об обработке персональных данных 2019 // URL: <https://www.ecovislegal.cz/ru/новинки/новый-чешский-закон-об-обработке-перс/> (дата обращения: 20.01.2023).

<sup>15</sup> См.: Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901; Указ Президента РФ от 14.06.2018 № 334 «О мерах по оптимизации структуры Администрации Президента Российской Федерации» (вместе с Положением об Управлении Президента Российской Федерации по развитию информационно-коммуникационных технологий и инфраструктуры связи) // СЗ РФ. 2018. № 25. Ст. 3646.

<sup>16</sup> ГОСТ Р ИСО/МЭК 19086-4-2020 «Национальный стандарт Российской Федерации. Информационные технологии. Облачные вычисления. Структура соглашения об уровне обслуживания (SLA). Часть 4. Компоненты информационной безопасности и защиты персональных данных» (утв. и введен в действие приказом Росстандарта от 10.11.2020 № 1040-ст). М. : Стандартинформ, 2020; ГОСТ Р ИСО/МЭК 27017-2021 «Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Правила применения мер обеспечения информационной безопасности на основе ИСО/МЭК 27002 при использовании облачных служб» (утв. и введен в действие приказом Росстандарта от 19.05.2021 № 389-ст). М. : Стандартинформ, 2021; ГОСТ ISO/IEC 17788-2016 «Межгосударственный стандарт. Информационные технологии. Облачные вычисления. Общие положения и терминология» (введен в действие приказом Росстандарта от 10.11.2016 № 1665-ст). М. : Стандартинформ, 2019.



информации<sup>17</sup>, о персональных данных<sup>18</sup> и о безопасности критической информационной инфраструктуры<sup>19</sup>.

Однако это не снимает актуальности принятия специального федерального закона об информационной безопасности, разделы которого должны быть посвящены в том числе правовым основам кибербезопасности при использовании технологий облачных вычислений, технологий искусственного интеллекта, больших данных и т.д., что заложит основу для комплексного подхода к правовому управлению безопасностью для различных участников цифровой среды.

В ближайшей перспективе должны быть определены правовые режимы применения технологий облачных вычислений, правосубъектность сторон, установлены правовые принципы деятельности с применением технологий облачных вычислений, касающиеся в том числе организации деятельности по предоставлению облачных сервисов в условиях прозрачной и понятной для пользователя среды, хранения, обработки и предоставления облачных данных на безопасных технологических платформах, мониторинга цифровых рисков и опасностей применения технологий облачных вычислений и др.

## БИБЛИОГРАФИЯ

1. Беккер М. Я., Гатчин Ю. А., Кармановский Н. С., Терентьев А. О., Федоров Д. Ю. Информационная безопасность при облачных вычислениях: проблемы и перспективы // URL: <https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-pri-oblachnyh-vychisleniyah-problemy-i-perspektivy/viewer> (дата обращения: 19.01.2023).
2. Жигалов Н. Ю. Облачные вычислительные технологии в судебно-экспертной деятельности // Российский следователь. — 2018. — № 4. — С. 11—14.
3. Карцхия А. А. «Облачные» технологии: российское и зарубежное законодательство и практика правоприменения // Мониторинг правоприменения. — 2018. — № 2 (27). — С. 36—41.
4. Викторова Н. Г., Шухов Ф. Г. Цифровая экономика: развитие облачных технологий в России и за рубежом // Век качества. — 2019. — № 2. — С. 81—90. — URL: <http://www.agequal.ru/pdf/2019/219006.pdf> (дата обращения: 19.01.2023).
5. Информационно-технологическое обеспечение юридической деятельности (LegalTech). — М. : Проспект, 2022. — 368 с.
6. Новый чешский закон об обработке персональных данных 2019 // URL: <https://www.ecovislegal.cz/ru/новинки/новый-чешский-закон-об-обработке-перс/> (дата обращения: 20.01.2023).

<sup>17</sup> Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

<sup>18</sup> Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) «О персональных данных» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.

<sup>19</sup> Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ. 2017. № 31 (ч. I). Ст. 4736.

7. Облачные вычисления, краткий обзор или статья для начальника // URL: <https://habr.com/ru/post/111274/> (дата обращения: 18.01.2023).
8. Облачные вычисления (мировой рынок) // URL: [https://www.tadviser.ru/index.php/статья:облачные\\_вычисления\\_\(мировой\\_рынок\)](https://www.tadviser.ru/index.php/статья:облачные_вычисления_(мировой_рынок)) (дата обращения: 19.01.2023).
9. *Amelin R., Channov S., Dobrobaba M., Kalinina L., Kholodnaya E.* Transformation of legal personality in the context of the development of modern digital technologies // *International Journal of Computer Science and Network Security*. — 2022. — Vol. 22. — № 11. — С. 294—302.
10. *Hurley Lawrence, Volz Dustin* (February 27, 2018). U.S. Supreme Court wrestles with Microsoft data privacy fight // Reuters. Retrieved. — April 2, 2018 — via The Globe and Mail.



**Сергей Викторович  
КОРОЛЕВ,**

главный научный сотрудник  
сектора международного  
права Института  
государства и права  
Российской академии наук,  
доктор юридических наук,  
профессор  
[sko.05@mail.ru](mailto:sko.05@mail.ru)  
119019, Россия, г. Москва,  
ул. Знаменка, д. 10



**Ирина Сергеевна  
ЛЯЛИНА,**

научный сотрудник  
сектора международного  
права Института  
государства и права  
Российской академии наук,  
кандидат юридических наук  
[irlyalina@yandex.ru](mailto:irlyalina@yandex.ru)  
119019, Россия, г. Москва,  
ул. Знаменка, д. 10

© Королев С. В.,  
Лялина И. С., 2023

## Интернет-право и кибербезопасность КНР

**Аннотация.** История возникновения и последующей трансграничной эволюции интернет-права по всему миру носит в некотором смысле парадоксальный характер. Создатели первой версии Интернета как информационной системы национальной безопасности вряд ли предполагали, что правовое регулирование Интернета, и прежде всего в Западной Европе, подпадет под влияние романо-германской системы права. Речь идет о базовом для континентальной Европы делении национального правопорядка на право публичное (*jus publicum*) и право частное (*jus privatum*). Соответственно, кибербезопасность и прочие публичные потребности Интернета в континентальной Европе стали предметом регулирования публичного интернет-права. Напротив, специфика и защита индивидуальных прав пользователей и предпринимателей в интернет-пространстве стали предметом регулирования частного интернет-права. В контексте такой дифференциации интернет-пространства особый интерес представляет опыт КНР, где соотношение публичной потребности и частного интереса в силу специфики китайской цивилизации невозможно интерпретировать в духе западноевропейского дуализма.

**Ключевые слова:** интернет, интернет-право, кибербезопасность, публичное интернет-право, частное интернет-право.

DOI: 10.17803/2311-5998.2023.102.2.162-167

**SERGEY V. KOROLEV,**

Chief scientific researcher, the Department of international law,  
Institute of State and Law of Russian Academy of Sciences,  
Dr. Sci. (Law), full professor  
[sko.05@mail.ru](mailto:sko.05@mail.ru)

10, ul. Znamenka, Moscow, Russia, 119019

**IRINA S. LYALINA,**

Scientific researcher, the Department of international law,  
Institute of state and law of Russian Academy of Sciences, Cand. Sci. (Law)  
[irlyalina@yandex.ru](mailto:irlyalina@yandex.ru)

10, ul. Znamenka, Moscow, Russia, 119019

### Internet law and cybersecurity of the PRC

**Abstract.** The history of the emergence and subsequent cross-border evolution of Internet law around the world is, in a sense, paradoxical. The creators of the first version of the Internet as a national security information system hardly imagined that the legal regulation of the Internet, primarily in

*Western Europe, would fall under the influence of the Romano-Germanic legal system. We are talking about the basic division of the national legal order for continental Europe into public law (jus publicum) and private law (jus privatum). Accordingly, cybersecurity and other public needs of the Internet in continental Europe have become the subject of public Internet law. On the contrary, the specifics and protection of the individual rights of users and entrepreneurs in the Internet space have become the subject of regulation of private Internet law. In the context of such differentiation of the Internet space, the experience of the PRC is of particular interest, where the ratio of public need and private interest, due to the specifics of Chinese civilization, cannot be interpreted in the spirit of Western European dualism.*

**Keywords:** internet, internet law, cybersecurity, public internet law, private internet law.

Интернет-право Китайской Народной Республики (КНР) находится в постоянной динамике. Основными факторами этой динамики, на наш взгляд, являются трансграничный характер Интернета, с одной стороны, и национальная специфика — с другой. В принципе, в любой стране мира правовое регулирование отражает оба указанных аспекта, при этом трансграничный характер Интернета можно назвать объективным фактором, а национальную специфику — субъективным. Именно последний аспект отвечает за то, насколько интернет-право той или иной страны является национальным и в конечном итоге — суверенным<sup>1</sup>.

Интернет как феномен возник первоначально исключительно как инструмент Пентагона или — в нейтральных терминах — как инструмент национальной безопасности США. Другими словами, Интернет — это прежде всего предмет публичного права. В момент зарождения Интернета ничто не предвосхищало дифференциацию интернет-права на публичное и частное, как, например, в современной Германии<sup>2</sup>. Отсюда — сквозная проблематика любого национального интернет-права, а именно соотношение публичного интернет-права и субъективных интернет-прав.

Китайский подход к этой проблематике имеет, по нашему убеждению, особое значение для тех стран, которые отказались идти в фарватере специфических эскапад западного либерализма. Несмотря на всю ультрасовременность и технологичность, китайское киберпространство и, соответственно, интернет-право КНР органично интегрированы в традицию того, что Фридрих Карл фон Савиньи назвал бы «китайским народным духом» (der chinesische Volksgeist)<sup>3</sup>.

Одной из древнейших манифестаций китайского народного духа является, скорее, тривиальное убеждение в том, что в природе (мироздании) существует

<sup>1</sup> См.: Fletcher P. Governing in the Internet Age in the National Interest. Melbourne : Monash University publishing, 2022. 96 p.

<sup>2</sup> См.: Paschke M. Medienrecht. 3. Aufl. Heidelberg, Dordrecht etc.: Springer Verlag, 2009. 548 S.

<sup>3</sup> См.: Lahusen B. Alles Recht geht vom Volksgeist aus: Friedrich Carl von Savigny und die moderne Rechtswissenschaft. Weilerswist : Dittich Verlag, 2019. 185 S.



порядок, и совсем нетривиальное следствие из этого, что естественный порядок вещей и социальный порядок взаимодействуют. С отрицательной стороны это означает, что социальный *непорядок* неизбежно посягает и на естественный порядок вещей.

Следует отметить *проактивный*, а не реактивный характер взаимодействия естественного порядка и социального порядка. Речь идет не просто об имитации естественных (космических) принципов в повседневном взаимодействии людей, речь идет об *убеждении*, что правильное (гармоничное) взаимодействие оказывает благоприятное влияние на окружающий мир. И наоборот: социальные распри, социальная рассогласованность, вражда оказывают пагубное воздействие на естественный порядок вещей<sup>4</sup>.

По крайней мере, с середины первого тысячелетия до н.э. и вплоть до начала XX в. социокультурную парадигму китайской цивилизации определяло взаимодействие двух традиций — конфуцианской и легистской. Центральной категорией конфуцианства является термин *ли*. Его пиктографические истоки двойственны: согласно одной версии древнейшая пиктографическая версия иероглифа *ли* восходит к обозначению разметки и размежевания полей. Так, правая часть иероглифа состоит из знаков «поле» и «почва»<sup>5</sup>. Отсюда терминологическое значение иероглифа *ли* как космического структурирующего начала или алгоритма.

С идеей алгоритма связана конкурирующая интерпретация пиктографических истоков термина *ли* как культового, церемониального действия с сосудом. Другими словами, согласно этой версии графическую основу обоих иероглифов термина *ли* составляет изображение ритуального сосуда<sup>6</sup>. В древнейших памятниках («Шу цзин» и «Ши цзин») категория *ли* обозначала обряды, дающие возможность преодолеть политические конфликты и отражающие единство мира, а также храмовые и дворцовые ритуалы, формы поведения сановников по отношению к народу. Конфуций (VI—V вв. до н.э.), теоретически осмыслив понятие *ли*, превратил его в самую общую характеристику правильного общественного устройства и поведения человека по отношению к другим и к себе: «Правитель [должен] руководить подданными посредством *ли*»<sup>7</sup>.

Школа законников, или легистская традиция, возникла как радикальный антипод конфуцианской традиции. Центральной категорией легизма является термин *фа*. Его первоначальное аморфное значение можно передавать и словом «образец», и словом «правило», и словом «метод»<sup>8</sup>. Благодаря своей «методологической» коннотации, термин *фа* в долегистском прочтении не противостоит, а дополняет значение слова *ли* в качестве «ритуала, благонравия». Слово *фа* состоит из двух иероглифов (*shui* = вода) и (*qu* = идти). «Вода» символизирует фундаментальный принцип жизни. Глагол «идти» в данном контексте означает удаляться от зла, т.е. от плохих нравов. Технический вид слово *фа* приобретает посредством добавления еще одного иероглифа, именно иероглифа *лю*, что

<sup>4</sup> Escarra J. Le droit chinois. [1936]. P. 8 // URL: <http://classiques.uqac.ca/>.

<sup>5</sup> URL: <http://philosophy.niv.ru/doc/dictionary/chinese-philosophy/articles/92/ceremonii.htm>.

<sup>6</sup> Китайская философия : энциклопедический словарь / под ред. М. Л. Титаренко. М. : Мысль, 1994. С. 194.

<sup>7</sup> Китайская философия : энциклопедический словарь. С. 194.

<sup>8</sup> Китайская философия : энциклопедический словарь. С. 415.

означает «дисциплинировать, контролировать». Соответственно, термин *фалю* приобретает неустранимую легистскую коннотацию.

По необходимости прозападная юридическая терминология в социокультурном контексте Китая имеет как бы два уровня, а именно верхний уровень юридического формализма и глубинный уровень, отражающий неизбежные конфуцианские и легистские коннотации любого формально нейтрального термина. Вместе с тем нельзя проводить резкую грань между двумя указанными традициями китайского миро- и правосознания. Этому препятствует уже базовый символ китайской мифологии, а именно *инь-ян* как символ женского и мужского начала.

На уровне правосознания и конфуцианская, и легистская традиции черпают свою силу и аргументы во всеобъемлющем китайском номинализме (= школа *мин цзя*)<sup>9</sup>. На наш взгляд, попытки искать аналогию в схоластическом номинализме Запада будут сомнительны, по крайней мере, по двум обстоятельствам. Во-первых, китайский номинализм является иероглифическим, а не фонологическим, как в схоластике: одно дело мыслить иероглифами, т.е. образами, другое дело — пытаться найти фонологическое обоснование наших представлений о мироздании. Во-вторых, китайский номинализм — это прежде всего социальная практика. Она базируется на конфуцианской доктрине «исправления имен». Практика же «исправления имен» представляет собой совершенно «бесплезное» занятие с точки зрения западного (фонологического) номинализма.

Соответственно, дополнительной аргументации потребует и попытка найти аналогию между китайским *номинализмом*, с одной стороны, и западным *формализмом* в духе идеологии юридического позитивизма — с другой. Ясно, что любой китайский иероглиф имеет собственную уникальную *форму*. Однако эта форма лишь фиксирует материальную, и — в западных терминах — «магическую» природу иероглифа, его сводимость к пиктографическому источнику (изображению огня, дерева, женщины, лошади и т.д.).

С китайским номинализмом по понятным причинам тесно переплетается конфуцианская теория «исправления имен». Ее обычно рассматривают в контексте социальной этики. Однако не менее интересна прагматическая коннотация этой теории, например в области права. В принципе, каждый китайский юрист проявляет и утверждает свою компетенцию как раз тем, насколько он владеет *юридической* техникой «исправления имен». Согласно китайскому номинализму однажды произнесенное слово приобретает собственную инерцию или даже динамику. Правильный социальный порядок *полностью* зависит от динамизма принципов, категорий, образов, на которых он зиждется, вот почему некоторые слова не следует ни произносить, ни переносить на бумагу<sup>10</sup>.

Возвращаясь в контексте заявленной темы к современному взаимодействию конфуцианства и легизма, можно утверждать, что термин «интернет-право» в *объективном* смысле, скорее, опирается на легистскую традицию *фа* (= закон в духе римской максимы: *dura lex sed lex*)<sup>11</sup>. Напротив, термин «интернет-право» в *субъективном* смысле, скорее, опирается на конфуцианскую традицию *ли* (= мораль, благонравие). Соответственно, традиция *фа* отражает одновременно жесткость

<sup>9</sup> URL: [https://www.thezensite.com/zenessays/philosophical/classical\\_chinese\\_logic.pdf](https://www.thezensite.com/zenessays/philosophical/classical_chinese_logic.pdf).

<sup>10</sup> URL: [http://classiques.uqac.ca/ Escarra J. Le droit chinois. \[1936\]. P. 22.](http://classiques.uqac.ca/ Escarra J. Le droit chinois. [1936]. P. 22.)

<sup>11</sup> Лат. «закон суров, но это закон».



внешнего социального регулирования. Конфуцианская традиция *ли* отражает добровольное соблюдение нравственных норм без внешнего принуждения.

В этом контексте особый интерес представляет взаимодействие в киберпространстве КНР того, что китайские юристы и политологи, пишущие по-английски, передают терминами *law* и *right*. Дело в том, что китайские «аналоги» этих терминов нельзя считать формальными потому, что практически любой *специальный* термин представляет собой комплекс из нескольких, как минимум двух, иероглифов.

Английский термин *a right* китайцы также «озвучивают» двояко. В банальном, т.е. нетехническом, смысле «правомочия» употребляется слово *quan*. Однако для придания этому слову технического смысла добавляется иероглиф *li* (не путать с конфуцианским омофоном «ли» в значении «мораль»). В результате технический термин *quanli* приобретает значение «правомочие + сила», или же «правомочие + власть». В этой комбинации также четко прослеживается легистский след внешнего социального регулирования.

Другими словами, социокультурная матрица китайского правосознания отторгает, например, всю парадигму западной теории естественных прав, по крайней мере, от Гоббса<sup>12</sup>, Локка<sup>13</sup> и до Руссо<sup>14</sup>. В китайском правосознании нет места для парадигмы так называемых естественных прав человека, поскольку эта парадигма плохо совместима с конфуцианской традицией *ли* как внутреннего, добровольного присоединения к общепринятым нормам нравственного поведения.

Подведем итоги и рассмотрим специфику взаимодействия объективного интернет-права в смысле *фалю* и субъективных интернет-прав в смысле *чуанли* на примере дела о мошенничестве и дела о защите личного достоинства. Судебное разбирательство по делу Ли Динг Синг от 1993 г. можно рассматривать в контексте приоритета объективного интернет-права в смысле *фалю* по отношению к институту субъективных интернет-прав в смысле *чуанли*. В октябре 1993 г. ответчик Ли Динг Синг приобрел акции компании «Цзиансу Саншан Индастри» и просчитался, так как компания оказалась весьма убыточной. Для восполнения финансовых потерь ответчик организовал рекламную компанию в СМИ, в которой распространил ложную информацию о деталях приобретения компании. В результате стоимость ее акций существенно возросла. При публичном слушании суд постановил, что ответчик сфабриковал и распространил ложную биржевую информацию. Ли Динг Синг был приговорен к двухгодичному тюремному заключению и штрафу в размере 10 тысяч юаней<sup>15</sup>.

Напротив, дело «Си Хонг против “Женьминь Жибао”», скорее, символизирует приоритет субъективных интернет-прав в смысле *чуанли* по отношению к объективному интернет-праву в смысле *фалю*. В данном деле *фалю* как формальная совокупность правил, регулирующая медийное и интернет-пространство КНР, явно уходит на второй план по сравнению с тем, что китайское правосознание

<sup>12</sup> См.: *Bobbio N.* Hobbes and the Natural Law Tradition. Translated by D. Gobetti. Chicago ; London : The University of Chicago press, 1993. 229 p.

<sup>13</sup> См.: *Simmons A. J.* The lockean Theory of Rights. Princeton : Princeton University press, 1992. 387 p.

<sup>14</sup> См.: *Pezzillo L.* Rousseau et le Contrat social. Paris : PUF, 2000. 128 p.

<sup>15</sup> *Guasong Sh.* Internet Law in China. Oxford etc. : Chandos Publishing, 2012. P. 111.

воспринимает как «правомочие-власть» индивида, т.е. *чуанли*. Фабула дела следующая: 20 июля 1988 г. главный печатный орган КПК «Женьминь Жибао» опубликовал критическую статью по поводу строительства Кашгар Сити. Руководство стройки подверглось критике из-за неумения взять под контроль рабочий персонал. В качестве «образцового лентяя и вечно недовольного жалобщика» был избран реальный рабочий по имени Си Хонг. В защиту своей чести и достоинства Си Хонг подал иск против «Женьминь Жибао». Дело не двигалось с места до 1989 г. Но и в последующие три года ответчик, т.е. центральная партийная газета КНР, игнорировала регулярные вызовы в суд. Лишь в 1992 г. дело было рассмотрено в судебном порядке, но окончательное урегулирование произошло лишь в 1997 г. в рамках (досудебной) медиации<sup>16</sup>.

## Итоговые выводы

1. Китайское правосознание отвергает идею естественных *субъективных* прав. Для менталитета любого китайца, не обязательно юриста, сама идея *принципиальной* первичности субъективного права, например, в духе Томаса Гоббса, невозможна. И базовый термин конфуцианской традиции *ли*, и базовый термин легизма *фа* являются деонтологическими, т.е. сфокусированы на (внутренне или внешне ориентированной) обязанности, а не на личном праве.
2. Соответственно, и в интернет-пространстве можно презюмировать приоритет объективного (национального) интернет-правопорядка в смысле *фалю* над индивидуальными «интернет-правомочиями» в смысле *чуанли*. Обстоятельства рассмотренного дела «Си Хонг против “Женьминь Жибао”» наглядно свидетельствуют о слабом ресурсе *чуанли*, когда дело доходит до символов *фалю*, в данном случае — в виде авторитетнейшей газеты КНР.

## БИБЛИОГРАФИЯ

1. Китайская философия : энциклопедический словарь / под ред. М. Л. Титаренко. — М. : Мысль, 1994.
2. *Bobbio N.* Hobbes and the Natural Law Tradition / translated by D. Gobetti. — Chicago ; London : The University of Chicago Press, 1993.
3. *Escarra J.* Le droit chinois. — [1936].
4. *Fletcher P.* Governing in the Internet Age in the National Interest. — Melbourne : Monash University publishing, 2022.
5. *Guasong Sh.* Internet Law in China. — Oxford etc. : Chandos Publishing, 2012.
6. *Lahusen B.* Alles Recht geht vom Volksgeist aus: Friedrich Carl von Savigny und die moderne Rechtswissenschaft. — Weilerswist : Dittrich Verlag, 2019.
7. *Paschke M.* Medienrecht. — 3. Aufl. — Heidelberg ; Dordrecht etc. : Springer Verlag, 2009.
8. *Pezzillo L.* Rousseau et le Contrat social. — Paris : PUF, 2000.
9. *Simmons A. J.* The lockean Theory of Rights. — Princeton : Princeton University Press, 1992.

<sup>16</sup> *Guasong Sh.* Op. cit. P. 119—120.



**Руслан Тимурович  
БАЙГАРИН,**

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

## Правовые проблемы обеспечения кибербезопасности генетических данных в Российской Федерации

**Аннотация.** В статье рассматриваются проблемные вопросы нормативно-правового регулирования обеспечения кибербезопасности генетических данных. Автором указывается на пробелы в правовой базе, регламентирующей требования по сбору, хранению, обработке и передаче генетических данных как особого вида персональных данных. Исследуются аспекты недостаточной защищенности генетической информации и основные причины и источники угроз для частных и публичных интересов. Предлагаются пути по совершенствованию законодательства в целях противодействия киберрискам в условиях значительного роста объема генетических данных в интернет-пространстве, в частности необходимо утверждение обязательных требований безопасности при работе с генетической информацией, увеличение ответственности за нарушение законодательства в области персональных данных, ограничение круга лиц, имеющих доступ к генетическим базам данных и другие механизмы правового регулирования.

**Ключевые слова:** генетическая информация, безопасность, киберугрозы, геномные исследования, персональные данные, информационно-аналитическая система, база генетической информации.

DOI: 10.17803/2311-5998.2023.102.2.168-176

**RUSLAN T. BAYGARIN,**

Postgraduate student of the Department of information law  
and digital technologies  
of the Kutafin Moscow State Law University (MSAL)  
[ruslanbaygarin@gmail.com](mailto:ruslanbaygarin@gmail.com)  
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

### Legal challenges in ensuring the cybersecurity of genetic data in the Russian Federation

**Abstract.** The article explores problematic issues of legal regulation of genetic data cybersecurity. The author points out gaps in the legal framework regulating the requirements for collection, storage, processing and transfer of genetic data as a special type of personal data. The author investigates the aspects of insufficient protection of genetic information and the main reasons and sources of threats for private and public interests. The author proposed ways to improve the legislation in order to counteract cyber risks

*in conditions of a significant growth of genetic data in the Internet space, in particular, to approve mandatory security requirements when dealing with genetic information, to increase responsibility for violation of legislation in the field of personal data, to limit the range of persons having access to genetic databases and other mechanisms of legal regulation.*

**Keywords:** *genetic information, security, cyber threats, genomic research, personal data, information analysis system, genetic information database.*

Исследования в области обработки генетических данных являются одной из наиболее перспективных и стремительно развивающихся областей человеческого знания. Научные и технологические достижения в области генетики обеспечили существенное повышение качества человеческой жизни, но они также несут в себе и дополнительные риски использования научных знаний во вред человеку, что обязывает совершенствовать государственное регулирование этой сферы общественных отношений.

С появлением так называемой геномики больших данных (Big Data Genomics) использование генетических данных становится все более распространенным явлением, появляются новые участники отношений по использованию генетических данных<sup>1</sup>. По мере того, как объем данных продолжает быстро увеличиваться, возникает все больше вопросов, связанных с разработкой и контролем соблюдения требований по консолидации данных, получаемых в результате гено-инженерной деятельности.

Рост объема генетических данных коррелирует с динамичным развитием интернет-технологий, методов оцифровки данных и способов их хранения, которые применяются в том числе при работе с генетической информацией, что ведет к необходимости разработки комплексных механизмов регулирования этой сферы киберправового поля. Одним из факторов, способствовавших ускорению цифровых процессов и, как следствие, возрастанию роли киберправа, генетических исследований и потребности в регулировании стремительно развивающихся информационных правоотношений, стала пандемия коронавируса (COVID-19).

Разработка конкретных мер, обеспечивающих хранение, обработку и анализ генетических данных в Российской Федерации при соблюдении должного уровня их безопасности, является комплексной задачей, в рамках которой потребуются разрешить как существующие, так и потенциальные правовые проблемы.

Поскольку взаимодействие субъектов и объектов общественных отношений по поводу генетической информации в значительной степени происходит в онлайн-формате, одним из ключевых аспектов при разработке правовых механизмов является обеспечение высокой степени их гибкости и адаптивности применяемых методов.

В первую очередь следует обратить внимание на общие тенденции в рассматриваемой области информационного пространства: рост потребностей в обеспечении конфиденциальности, особенно в отношении защиты финансовых,

<sup>1</sup> Чубукова С. Г. Правовые проблемы защиты генетической информации: субъектный подход // Вестник Университета имени О.Е. Кутафина (МГЮА). 2020. № 5. С. 96—103.



генетических, медицинских данных и сведений о местонахождении; осложнение работы с генетической информацией трансграничной передачей данных; непрерывную потребность организаций в совершенствовании управления собственными киберрисками.

Другой опасной тенденцией, требующей своевременного и эффективного контроля, является усиление интереса киберпреступников к цифровым активам, в частности к персональным, генетическим данным людей<sup>2</sup>.

На сегодняшний день нормативно-правовая база не отражает все особенности генетической информации как объекта информационных правоотношений, а также как особого вида персональных данных, что требует развития и совершенствования российского законодательства.

Генетические данные нуждаются в особой правовой и технической защите. В российском законодательстве имеется пробел в части защиты информации о человеке, полученной из его биоматериала, который содержит генетическую информацию, позволяющую получить о нем дополнительные сведения (о состоянии здоровья, питания, образа жизни, поведенческих особенностях, чувствительности к фармакологическим препаратам или аллергенам и другие индивидуальные характеристики).

В отечественном законодательстве содержится легальное определение геномной информации. В соответствии с Федеральным законом от 03.12.2008 № 242-ФЗ «О государственной геномной регистрации в Российской Федерации»<sup>3</sup> геномная информация представляет собой персональные данные, включающие кодированную информацию об определенных фрагментах дезоксирибонуклеиновой кислоты (ДНК) физического лица или неопознанного трупа, не характеризующих их физиологические особенности.

Такой подход законодателя к генетической информации подвергается критике в юридическом сообществе, так как ДНК является носителем генетической информации не только о конкретном лице, но и о его родственниках и потомках. Другими словами, с молекулой ДНК, помимо ее индивидуальности, связано и другое основополагающее свойство — наследственность и способ передачи наследственной информации, касающейся неопределенного круга лиц<sup>4</sup>.

Само по себе обеспечение кибербезопасности является многогранным процессом. Представляется, что для поддержания должного уровня безопасности данных все устройства, используемые в компаниях и государственных органах, деятельность которых связана с генетической информацией, должны иметь установленное программное обеспечение для защиты от вредоносного ПО, а при удаленной работе критически важно применять виртуальные частные сети. При нарушении сетевого соединения пользователям должен автоматически блокироваться доступ к документам, электронной почте и другим важным программам,

<sup>2</sup> Jeffrey D. Neuburger and Jonathan P. Mollod. Trends in Privacy and Data Security: 2021 // Practical Law. 2021. URL: <https://content.next.westlaw.com/w-034-2241?isplcsc=true&transititiontype=default&contextdata=%28sc.default%29> (дата обращения: 17.01.2023).

<sup>3</sup> СЗ РФ. 2008. № 49. Ст. 5740.

<sup>4</sup> Кубитович С. Н. ДНК как носитель информации неограниченного круга лиц // Вестник экономической безопасности. 2017. № 4. С. 186.

содержащим конфиденциальную информацию. Многофакторная аутентификация также является необходимым атрибутом (особенно при работе с базами генетических данных), позволяющим усложнить процесс взлома систем.

Указанные требования безопасности принимаются на уровне локальных нормативных актов, однако для объективного повышения уровня кибербезопасности следует законодательно закрепить их обязательность при работе с генетической информацией, соответствующие меры ответственности.

Отсутствие серьезных мер ответственности за нарушения порядка проведения работ с генетическими данными фактически приводит к безнаказанному пренебрежению мерами кибербезопасности, а нарушения законодательства о персональных данных происходят повсеместно.

К примеру, в начале 2022 г. стало известно об утечке персональных данных 30 миллионов человек в крупнейшей федеральной медицинской компании «Гемотест», выполняющей лабораторную диагностику<sup>5</sup>. По итогам проверки был обнаружен факт предоставления незаконного доступа к базам данных, что спровоцировало распространение персональных данных пациентов в Интернете.

Согласно официальному ответу представителей лаборатории, произошла хакерская атака: на просторы сети, помимо сведений об оказанных пациентам услугах со стороны лаборатории, также были выгружены гигабайты персональных данных клиентов. Несмотря на отрицание лабораторией вины, суд признал компанию виновной в утечке данных, а также определил сумму штрафа в 60 000 рублей<sup>6</sup>. Очевидно, что данный размер ответственности несопоставим с ущербом, нанесенным широкому кругу лиц, пользовавшихся услугами медицинской компании.

Другой правовой проблемой, стоящей перед законодателем, является сложность соблюдения конфиденциальности и обезличенности генетических данных. Председатель Конституционного Суда РФ В. Д. Зорькин определяет цифровые права в том числе как право на неприкосновенность частной информационной сферы, включая право на конфиденциальность, анонимность (обезличенность) его уже оцифрованной персональной информации<sup>7</sup>.

В некоторых случаях цели геномных исследований не позволяют соблюдать требование по обезличиванию получаемых в результате работы данных. Тем не менее для соблюдения конфиденциальности и защиты частных интересов данные, которые будут передаваться в базы генетической информации, должны быть псевдонимизированы. В европейском Генеральном регламенте о защите

<sup>5</sup> Гемотест начал расследование об утечке данных 30 млн клиентов // URL: [https://www.rbc.ru/society/04/05/2022/6272665b9a794713ec6698dd?f rom=article\\_body](https://www.rbc.ru/society/04/05/2022/6272665b9a794713ec6698dd?f rom=article_body) (дата обращения: 27.01.2023).

<sup>6</sup> Постановление мирового судьи судебного участка № 281 района Вешняки города Москвы от 08.07.2022 по делу 05-0564/287/2022 // URL: <https://mos-sud.ru/287/cases/admin/details/8d9658fc-9304-417c-bf8f-9389ef8772ac?caseNumber=05-0564/287/2022> (дата обращения: 27.01.2023).

<sup>7</sup> Зорькин В. Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума // Российская газета. 2018. Столичный выпуск. № 7578 (115).



персональных данных от 27.04.2016<sup>8</sup> под этой процедурой понимается определенная обработка данных для невозможности ее отнесения к конкретному субъекту данных без использования дополнительной информации. Специальным условием является то, что указанная дополнительная информация должна храниться отдельно с применением технических и организационных мер, предотвращающих ее несанкционированное разглашение<sup>9</sup>.

Представляется, что европейский опыт правового регулирования данных может быть полезен при разработке соответствующих правовых механизмов в национальном законодательстве.

Совсем недавно был принят Федеральный закон от 29.12.2022 № 643-ФЗ «О внесении изменений в Федеральный закон “О государственном регулировании в области генно-инженерной деятельности”»<sup>10</sup>, закрепляющий ряд важных положений в области правового регулирования общественных отношений, возникающих, изменяющихся и прекращающихся в процессе обеспечения оборота генетической информации в Российской Федерации.

Основной объем внесенных изменений касается создания информационно-аналитической системы «Национальная база генетической информации», основными целями которой заявлены обеспечение национальной безопасности, охраны жизни и здоровья граждан, суверенитета в сфере хранения и использования генетических данных. Информационно-аналитическая система также призвана обеспечить обмен генетической информацией между обладателями генетических данных и государственными органами.

Перед законодателем стоит задача разработки положения о Национальной базе генетической информации, детально регулирующего различные аспекты ее работы, в частности формат обработки и состав предоставляемых сведений, а также иные аспекты ее функционирования. С учетом того, что информация, содержащаяся в информационно-аналитической системе, будет общедоступной и предоставляться на безвозмездной основе, возникает вопрос об ограничении круга субъектов, имеющих право на получение содержащейся в ней информации.

Представляется, что при установлении перечня получателей данной информации следует предусмотреть разрешительный порядок доступа к информационно-аналитической системе для лиц, не являющихся российскими гражданами и юридическими лицами. В частности, в условиях сложной геополитической ситуации целесообразно ограничить доступ для лиц, связанных с недружественными государствами.

Впервые о необходимости создания базы генетической информации было заявлено Президентом РФ в 2020 г. в период пандемии коронавируса (COVID-19)<sup>11</sup>,

<sup>8</sup> Генеральный регламент о защите персональных данных от 27.04.2016 // URL: <https://gdpr.eu/tag/gdpr/> (дата обращения: 25.01.2023).

<sup>9</sup> Столбов А. П. О стандартизации методов псевдонимизации персональных данных в здравоохранении // Проблемы стандартизации в здравоохранении. 2017. № 9–10. С. 25–36.

<sup>10</sup> СЗ РФ. 2023. № 1 (ч. I). Ст. 90.

<sup>11</sup> Поручение Президента РФ от 04.06.2020 № Пр-920 «Перечень поручений по итогам совещания по вопросам развития генетических технологий» // URL: <https://base.garant.ru/74229773/> (дата обращения: 19.01.2023).

что частично объясняет цели данного поручения — обеспечение как научного развития, так и оперативного реагирования на потенциальные биологические угрозы. Риск несанкционированного доступа к информации, содержащейся в консолидированных базах данных, несет в себе опасности как для частных, так и для публичных интересов, вплоть до угроз национальной безопасности.

В результате цифровизации персональные данные в цифровом пространстве должны быть защищены от несанкционированного доступа, модификации, раскрытия путем передачи, а также от уничтожения или повреждения. Для обеспечения безопасности персональных данных необходимо разработать порядок обращения с персональными данными в условиях развития киберугроз; внедрить систему контроля за соблюдением конфиденциальности и защитой данных; определить масштабы рисков, которые могут возникнуть в случае несанкционированной обработки персональных данных и ответственность в случае причинения ущерба, связанного с личными данными, в рамках интернет-пространства.

По всем процессам, связанным с обработкой больших персональных данных, необходимо проводить в соответствии с требованиями законодательства объективную оценку вреда субъектам персональных данных, который потенциально может быть причинен<sup>12</sup>. Это даст возможность своевременной корректировки мер по обеспечению безопасности данных со стороны операторов персональных данных во взаимоотношениях с внешними подрядчиками (например, с облачными провайдерами).

В целом можно утверждать, что новые риски и киберугрозы появляются по мере того, как сбор и использование генетических данных становятся широко распространенным явлением. Возникновение таких рисков частично связано со стремительным падением стоимости секвенирования ДНК, а также достижениями в области синтетической биологии. За последние несколько лет стоимость секвенирования целого генома снизилась с 1 000 долларов США до 100 долларов США за один геном<sup>13</sup>, а всего 15 лет назад стоимость данной процедуры была на уровне около 1 миллиона долларов США<sup>14</sup>.

Вследствие этого генетические данные становятся все более доступными из ряда различных информационных источников. Представители частного сектора экономики осуществляют сбор генетических данных, начиная с поставщиков услуг в области ДНК-диагностики и составления родословных, которые также записываются и в цифровом виде, и заканчивая фармацевтическими компаниями, ведущими анализ данных о состоянии здоровья потребителей. Также данные генерируются в ходе исследований, финансируемых государством, и попадают в электронные базы.

<sup>12</sup> Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Подпункт 5 ч. 1 ст. 18.1 // СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.

<sup>13</sup> Regalado A. China's BGI says it can sequence a genome for just \$100 // MIT Technology review. 26.02.2020. URL: <https://www.technologyreview.com/2020/02/26/905658/china-bgi-100-dollar-genome/> (дата обращения: 23.01.2023).

<sup>14</sup> Wetterstrand K. A. DNA Sequencing Costs: Data // National Human Genome Research Institute. URL: <https://www.genome.gov/about-genomics/fact-sheets/dna-sequencing-costs-data> (дата обращения: 23.01.2023).



Эти исследовательские программы несут в себе огромный потенциал для развития науки и медицины, который даст возможность предсказывать предрасположенность к болезням и проводить лечение с учетом индивидуальных особенностей генетики. Для такого прогресса необходимы большие базы генетических данных, включающие разнообразные личные данные, начиная от данных о состоянии здоровья и заканчивая выбранным образом жизни. Именно поэтому они становятся объектом для возможных кибератак. Как правило, такие базы данных обезличиваются или деидентифицируются путем присвоения участникам цифровых идентификаторов вместо личных имен, однако в некоторых случаях данные могут быть повторно идентифицированы.

Угрозы, связанные с этими незащищенными базами данных, усугубляются с развитием искусственного интеллекта, особенно машинного обучения — области искусственного интеллекта, связанной с обработкой данных. Применение машинного обучения к генетическим данным способствует ускоренному развитию возможностей медицинской науки и врачебной практики по разработке методов геномной диагностики и терапии.

В то же время эти достижения предоставляют злоумышленникам опасные средства для использования генетических данных с целью причинения ущерба и масштабирования угроз. Например, с помощью методов машинного обучения можно определить рост с точностью до нескольких сантиметров<sup>15</sup> или реконструировать черты лица<sup>16</sup>. При наличии базы данных лиц с именами, к примеру базы данных фотографий водительских прав, генетические данные могут быть повторно идентифицированы с помощью машинного обучения<sup>17</sup>.

Применение искусственного интеллекта к генетической информации уже привело к значительным открытиям и революционным методам лечения, но некоторые из этих достижений также могут быть использованы для разработки биооружия. Научные открытия в области генеалогии позволяют достичь беспрецедентного понимания истории, но также могут привести к потере анонимности как в онлайн-, так и в офлайн-пространстве.

Особенный характер генетических данных делает их особенно интимными, значимыми и ценными для их обладателей. Это объясняется тем, что генетические данные являются постоянными и принадлежат человеку на протяжении всей его жизни, что неотъемлемо привязывает их к личности. Нарушения безопасности генетических данных из-за их неизменной природы могут иметь долгосрочные последствия, и их правовой режим должен регулироваться отдельно от иных

<sup>15</sup> Lello L., Avery S. G., Tellier L., Vazquez A. I., Los Campos G. de, Hsu S. D. H. Accurate Genomic Prediction of Human Height // *Genetics*. 2018. No. 210 (2). P. 477—497. URL: <https://doi.org/10.1534/genetics.119.302946> (дата обращения: 23.01.2023).

<sup>16</sup> Robust genome-wide ancestry inference for heterogeneous datasets: illustrated using the 1,000 genome project with 3D facial images / J. Li, T. G. Zarzar, J. D. White [et al.] // *Scientific Reports*. No. 10. 11850. 2020. URL: <https://doi.org/10.1038/s41598-020-68259-w> (дата обращения: 19.01.2023).

<sup>17</sup> Facial recognition from DNA using face-to-DNA classifiers / D. Sero, A. Zaidi, J. Li [et al.] // *Nature Communications*. No. 10, 2557. 2019. URL: <https://doi.org/10.1038/s41467-019-10617-y> (дата обращения: 19.01.2023).

видов данных, так как в случае нарушения конфиденциальности или непосредственного вмешательства в наследственность одного человека последствия могут затронуть его родственников.

Если генетические данные дальнего родственника раскрыты, то множество родственных людей оказываются под угрозой установления личности посредством сопоставления семейных особенностей генетики. Целый ряд генетических баз данных открытого и частично открытого типа уже доступны публично, а другие базы данных признаны уязвимыми перед несанкционированным доступом<sup>18</sup>. Используя эти данные, уже сейчас можно идентифицировать многих людей только по ДНК их родственников.

Характер и значимость генетических данных, обеспечение безопасности которых предоставит защиту для будущих поколений, имеет под собой конституционное обоснование, с учетом того, что в преамбуле Конституции РФ определена ответственность народа Российской Федерации перед своими потомками<sup>19</sup>.

Возможности машинного обучения по обработке сведений о культуре, эпигенетических и этнических особенностях могут привести к созданию моделей, позволяющих получать точные прогнозы даже в отношении заболеваний, не обладающих высокой степенью наследуемости<sup>20</sup>. Умение предсказывать предрасположенность к заболеваниям и применение методов превентивной медицины станут ключевыми элементами медицины будущего. Однако возможность прогнозирования даже незначительных по тяжести заболеваний в больших масштабах позволит использовать уязвимости в рамках целых социальных групп или популяций.

Таким образом, для ряда киберугроз, связанных с получением и обработкой генетических данных, крайне высок риск причинения ущерба как конкретному человеку, так и отдельным группам населения, в связи с чем особенно возрастает роль процесса усовершенствования правовой базы в рамках цифрового поля.

По мере развития биотехнологий могут возникнуть и другие потенциальные угрозы, которые в настоящее время не учитываются или не прогнозируются. Здесь применима известная цитата бывшего министра обороны США Дональда Рамсфелда: «Есть известные известные — вещи, о которых мы знаем, что знаем их. Есть также известные неизвестные — вещи, о которых мы знаем, что не знаем. Но еще есть неизвестные неизвестные — это вещи, о которых мы не знаем, что не знаем их».

Хотя для предотвращения или смягчения будущих угроз можно применить ряд мер, включая ограничение развертывания моделей искусственного интеллекта,

<sup>18</sup> Greshake B., Bayer P. E., Rausch H., Reda J. openSNP — A Crowdsourced Web Resource for Personal Genomics // PLoS ONE. 9(3). URL: <https://doi.org/10.1371/journal.pone.0089204> (дата обращения: 21.01.2023).

<sup>19</sup> Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // URL: <http://www.pravo.gov.ru> (дата обращения: 20.01.2023).

<sup>20</sup> Finding the missing heritability of complex diseases / T. Manolio, F. Collins, N. Cox [et al.] // Nature. 2009. 461. P. 747—753. URL: <https://doi.org/10.1038/nature08494> (дата обращения: 20.01.2023).



жесткое нормативно-правовое регулирование и контроль за биотехнологиями, неизбежные достижения в данной области следует учитывать при определении баланса между необходимостью обеспечения доступа к генетическим данным и защитой их безопасности. Обмен генетическими данными и развитие технологий не могут и не должны быть остановлены.

Создание парадигмы безопасности генетических данных требует объединения усилий широкого круга заинтересованных сторон, привлечения соответствующих ресурсов и всеобщего признания генетической информации как критически важной составляющей инфраструктуры, нуждающейся в защите, аналогичной другим фундаментальным активам.

### БИБЛИОГРАФИЯ

1. Болтанова Е. С., Имекова М. П. Генетическая информация в системе объектов гражданских прав // *Lex russica*. — 2019. — № 6. — С. 110—121.
2. Кубитович С. Н. ДНК как носитель информации неограниченного круга лиц // *Вестник экономической безопасности*. — 2017. — № 4.
3. Минбалеев А. В. Право и современные информационные технологии: основные проблемы // *Информационное пространство: обеспечение информационной безопасности и право* : сборник научных трудов / под ред. Т. А. Поляковой, В. Б. Наумова, А. В. Минбалеева. — М. : ИГП РАН, 2018. — С. 86—91.
4. Рассолов И. М., Чубукова С. Г. Правовое регулирование использования банков генетической информации // *Генетические технологии и право в период становления биоэкономики*. — 2020. — С. 329—340.
5. Рассолов И. М., Чубукова С. Г., Микурова И. В. Правовое регулирование использования генетической информации в Евросоюзе // *Аграрное и земельное право*. — 2019. — № 7 (175). — С. 120—123.
6. Чубукова С. Г. Правовые проблемы защиты генетической информации: субъектный подход // *Вестник Университета имени О.Е. Кутафина (МГЮА)*. — 2020. — № 5. — С. 96—103.

## Актуальные вопросы правового регулирования искусственного интеллекта в условиях необходимости обеспечения национального цифрового суверенитета в период санкционного давления

**Аннотация.** В статье анализируется потенциал использования технологий искусственного интеллекта для снижения или предотвращения различного рода рисков для отечественного бизнеса в условиях усиливающегося санкционного давления ряда зарубежных стран, которое достигло беспрецедентных масштабов после начала специальной военной операции на Украине.

В статье рассмотрены аспекты, связанные с применением зарубежными странами современных ИТ-решений для контроля соблюдения санкционного законодательства по отношению к Российской Федерации, а также способы информирования отечественного бизнес-сообщества о возможности учета принятых в отношении него ограничительных мер.

Проанализированы подходы к определению понятия цифрового суверенитета и сформулированы его критерии. На основе анализа нормативных и доктринальных источников показано, что технологии ИИ неразрывно связаны с обеспечением национального цифрового суверенитета, а уровень правового регулирования должен отвечать запросам настоящего времени.

**Ключевые слова:** искусственный интеллект, цифровой суверенитет, ИТ-решения, односторонние ограничительные меры, санкционный комплаенс.



**Антон Александрович  
ЖУРКОВ,**

заместитель начальника  
Управления  
по внеучебной и  
воспитательной работе  
Университета имени  
О.Е. Кутафина (МГЮА),  
соискатель кафедры  
информационного права  
и цифровых технологий  
Университета имени  
О.Е. Кутафина (МГЮА)  
**aazhurkov@msal.ru**  
125993, Россия, г. Москва,  
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2023.102.2.177-186

**ANTON A. ZHURKOV,**

Deputy Head of the Department for extracurricular and educational work  
of the Kutafin Moscow State Law University (MSAL), Applicant of the Department  
of information law and digital technologies  
of the Kutafin Moscow State Law University (MSAL)  
**aazhurkov@msal.ru**

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

### Topical issues of legal regulation of artificial intelligence in the context of the need to ensure national digital sovereignty during the period of sanctions pressure

**Abstract.** The article analyzes the potential of using artificial intelligence technologies (hereinafter referred to as AI) for the purpose of reducing or preventing various kinds of risks for domestic business in the face of increasing

© Журков А. А., 2023

*sanctions pressure from a number of foreign countries, which reached unprecedented proportions after the start of a special military operation in Ukraine. The article discusses aspects related to the use of modern IT solutions by foreign countries for the purposes of monitoring compliance with sanctions legislation in relation to the Russian Federation, as well as ways to inform the domestic business community about the possibility of taking into account restrictive measures taken against it.*

*The approaches to the definition of the concept of digital sovereignty are analyzed and its criteria are formulated. Based on the analysis of regulatory and doctrinal sources, it is shown that AI technologies are inextricably linked with ensuring national digital sovereignty, and the level of legal regulation should meet the demands of the present time.*

**Keywords:** *artificial intelligence, digital sovereignty, IT solutions, unilateral restrictive measures, sanctions compliance.*

Роль и значение отечественных разработок в сфере ИИ и принципиально иной уровень ее нормативного регулирования еще более возросли с начала специальной военной операции на Украине и ввода в отношении Российской Федерации значительного числа односторонних ограничительных мер со стороны США, Канады, Австралии, Евросоюза и ряда других государств. В условиях изменившихся политических и правовых реалий российские компании были вынуждены перестраивать свои бизнес-процессы, складывавшиеся с начала 1990-х гг. в условиях построения рыночной экономики в Российской Федерации.

Для информирования российского бизнес-сообщества о замораживании активов и запрете на предоставление средств или экономических ресурсов на сайте Торгово-промышленной палаты РФ были размещены часто задаваемые вопросы и ответы Еврокомиссии об обходе вводимых санкций и должной осмотрительности<sup>1</sup>.

Правительство РФ сформулировало и опубликовало перечень мер по повышению устойчивости экономики и поддержке граждан в условиях санкций. Соответствующий документ вместе с интерактивной инфографикой был опубликован на официальном сайте государственного органа еще в феврале 2022 г.<sup>2</sup> Более того, тематические страницы по отдельным отраслям национальной экономики регулярно обновляются и дополняются актуальной информацией и нормативными актами.

Для потенциального получателя обнародована информация о механизме получения государственной услуги, связанной с поддержкой бизнеса, в электронном виде, без необходимости личного обращения в органы исполнительной власти. Также получателю услуги на информационном портале «Ваш контроль» предоставляется возможность дать свою личную оценку, характеризующую качество и полноту опубликованной информации на сайте Правительства РФ, с

<sup>1</sup> Официальный сайт Европейской комиссии. URL: <https://sanctionsmap.eu/#/main> (дата обращения: 16.01.2023).

<sup>2</sup> URL: [http://government.ru/sanctions\\_measures/category/regulation/](http://government.ru/sanctions_measures/category/regulation/) (дата обращения: 16.01.2023).

возможностью обратной связи. В позитивном ключе важно отметить и роль, которую вносят иные цифровые ресурсы, например, сервисы Федеральной налоговой службы, портал «Госуслуги» и др.

Вышеуказанные и иные меры, связанные с информированием российского бизнес-сообщества и оказанием ему цифровой помощи, свидетельствуют не просто о заинтересованности Правительства РФ в доведении сведений до соответствующих субъектов, но и о предельной решимости ускорить рассмотрение огромного числа вопросов, появившихся у предприятий и граждан после начала специальной военной операции и введения санкционных мер в отношении Российской Федерации, о заинтересованности в практическом решении появившихся проблем.

Сейчас многие компании для проверки своих контрагентов и клиентов используют специальные базы информационных данных (Factiva, Qixin, LexisNexis, Refinitiv World Check и проч.), а также открытые зарубежные базы данных, которые ведут иностранные правительства для публикации сведений из официальных регистров зарегистрированных компаний в соответствии с национальным законодательством. К слову, с такой информацией можно ознакомиться и в российском сегменте Интернета, в частности на платформе ФНС России функционирует соответствующий сервис.

Применение подобных систем позволяет проверять актуальные сведения, а также профили предприятий, морских и воздушных судов, принадлежащих лицам, включенным в санкционный список, или контролируемых ими, выявить ценные бумаги, в отношении которых действуют санкции, провести оценку рисков и т.д. Меры реагирования по сведениям из баз данных заключаются как в выявлении организаций, непосредственно попавших под действие санкций, так и в проверке благонадежности любой вызывающей сомнения организации.

Причина такого комплексного подхода к соблюдению американского санкционного законодательства состоит в том, что любое лицо может попасть в подобные списки не только за прямое нарушение, но и за сотрудничество с субъектами, уже включенными в эти списки. Попытки действовать в обход односторонних ограничительных мер могут грозить штрафом в размере свыше 1 млн долл. США, а также лишением свободы на срок до 20 лет<sup>3</sup>.

После 24 февраля 2022 г. для представителей российского бизнес-сообщества образовались следующие риски:

- 1) вторичные санкции за взаимодействие с подсанкционным лицом, например, в виде заключения сделок или совершения операций с ним, а также «теневые санкции». Это так называемое «правило 50 %»<sup>4</sup>, согласно которому компания, где подсанкционное лицо индивидуально или в совокупной сумме с

<sup>3</sup> См.: Сазонов В. Как предотвратить попадание в санкционные списки. Важные факторы, которые следует учитывать при проведении санкционного комплаенса // URL: <https://www.advgazeta.ru/mneniya/kak-predotvratit-popadanie-v-sanktsionnye-spiski/?ysclid=l4cjh58806490253> (дата обращения: 10.06.2022).

<sup>4</sup> Официальный сайт газеты «Ведомости». URL: <https://www.vedomosti.ru/business/news/2022/03/28/915563-es-nachal-primenyat-pravilo-50-v-sanktsiyah-protiv-rossii> (дата обращения: 16.01.2023).



иными подсанкционными лицами прямо или косвенно владеет 50 % и более акций (долей), автоматически подпадает под санкционное законодательство. Похожее правило действует и в Европейском союзе — контроль может осуществляться на основании договора, в рамках которого пороговое значение по владению должно быть более 50 %;

- 2) усиленный санкционный комплаенс со стороны контрагентов, банков или внутри самой компании<sup>5</sup>;
- 3) ограничение возможностей на совершение банковских операций доступа к активам, в том числе валютным;
- 4) отказ зарубежных контрагентов от перспективного сотрудничества и возросшие риски банкротства.

Возможно образование пятого риска в виде уголовной ответственности за злоупотребление полномочиями в целях исполнения решения иностранного государства, союза иностранных государств или международной организации о введении мер ограничительного характера против Российской Федерации. Однако проект федерального закона<sup>6</sup>, которым предлагается введение такой ответственности, еще не принят, в настоящее время проходит рассмотрение в первом чтении в Государственной Думе.

Создавшееся беспрецедентное санкционное давление остро обозначило необходимость обеспечения национального цифрового суверенитета, и прежде всего в сфере ИИ. Сопоставляя позиции различных юристов, следует прийти к выводу о том, что единого понятия цифрового суверенитета в доктрине, как в отечественной, так и в зарубежной, не выработано. Существует проблема подхода к основным критериям при выработке единого понятия. Одни авторы ограничиваются исключительно правовым регулированием, а другие рассматривают систему мер по обеспечению функционирования государства в информационном пространстве через призму политики, производственно-технологических, экономических и прочих процессов.

При этом справедливо будет отметить, что многими специалистами часто не разделяются вопросы национального цифрового суверенитета и государственной информационной политики. Обобщая различные позиции, можно прийти к выводу, что под цифровым суверенитетом понимается определенно высокий уровень развития производственного, технологического, правового, экономического и информационного взаимодействия государства, физических и юридических лиц, который позволяет самостоятельно осуществлять цифровую трансформацию, организовывать национальную цифровую систему и управлять ею, исключать возможность воздействия на нее извне.

Обеспечение неприкосновенности национального цифрового суверенитета диктует необходимость формирования основных критериев, позволяющих оценить его объективное состояние. К ним, по нашему мнению, относятся:

<sup>5</sup> Ершова И. В., Енькова Е. Е. Санкционный комплаенс, или Внутрифирменное управление рисками от рестрикций // Актуальные проблемы российского права. 2022. № 8. С. 93—103.

<sup>6</sup> Проект федерального закона № 102053-8 // URL: <https://sozd.duma.gov.ru/bill/102053-8> (дата обращения: 16.01.2023).

- 1) доля цифровых услуг отечественного производства в общем объеме внедренных на территории страны услуг в рамках одной группы (процент внедренных ИТ-решений на соответствующий период времени);
- 2) величина импорта цифровых технологий;
- 3) степень автономности национальной системы в области хранения, обработки и передачи пользовательских данных.

Национальный цифровой суверенитет формируется под воздействием субъектов цифровизации и во взаимодействии различных групп, начиная от взаимоотношений физических и юридических лиц, в том числе и транснациональных корпораций, заканчивая межгосударственным сотрудничеством в рамках двусторонних отношений и отношений, возникающих в рамках международных межправительственных организаций.

Согласно отчету аналитической платформы Statista по итогам 2021 г. Российская Федерация занимала 8-е место в мире по объему инвестиций в исследования и развитие ИИ, хотя объем инвестиций был в 10 раз ниже, чем у лидеров — КНР и США. По некоторым же направлениям российские компании являются мировыми лидерами. Здесь надо прежде всего назвать VisionLabs с его компьютерным зрением или «Яндекс», обогнавший таких цифровых гигантов, как американские Google и Microsoft по качеству машинного перевода<sup>7</sup>. В 2022 г. Всемирный банк признал нашу страну одной из самых преуспевающих в цифровизации государственного управления и сфер общественной жизни<sup>8</sup>.

В Программе фундаментальных научных исследований в Российской Федерации на долгосрочный период (2021—2030 годы), утвержденной Правительством РФ, среди основных направлений названо изучение правового статуса ИИ<sup>9</sup>. В Национальной стратегии развития искусственного интеллекта на период до 2030 года утверждается, что создание универсального (сильного) интеллекта, способного, подобно человеку, решать различные задачи, мыслить, взаимодействовать и адаптироваться к изменяющимся условиям, является сложной научно-технической проблемой, решение которой находится на пересечении различных сфер научного знания, в том числе социально-гуманитарного.

Выработка правовых условий для внедрения технологических решений на основе искусственного интеллекта предполагает делегирование информационным системам возможности принятия отдельных решений без ущемления прав и законных интересов граждан<sup>10</sup>.

<sup>7</sup> Сайт аналитической платформы «Statista». URL: [https://www.statista.com/topics/3104/artificial-intelligence-ai-worldwide/#topicHeader\\_\\_wrapper](https://www.statista.com/topics/3104/artificial-intelligence-ai-worldwide/#topicHeader__wrapper) (дата обращения: 16.01.2023).

<sup>8</sup> URL: <https://www.worldbank.org/en/programs/govtech/gtmi> (дата обращения: 16.01.2023).

<sup>9</sup> Распоряжение Правительства РФ от 31.12.2020 № 3684-р «Об утверждении Программы фундаментальных научных исследований в Российской Федерации на долгосрочный период (2021—2030 годы)» // СЗ РФ. 2021. № 3. Ст. 609.

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



В сентябре 2022 г. Правительство РФ утвердило план мероприятий «Создание дополнительных условий для развития отрасли информационных технологий»<sup>11</sup>, в котором содержится перечень мероприятий по развитию отрасли информационных технологий, в том числе и технологий ИИ. План включает 62 мероприятия, 20 из которых носят общий характер и предусматривают меры по выравниванию условий ведения предпринимательской деятельности в Российской Федерации для международных интернет-корпораций и российских ИТ-компаний, по стимулированию внедрения отечественных ИТ-решений в деятельность предприятий, по поддержке экспорта и продвижению российских ИТ-решений на внешних рынках. Остальные 42 мероприятия направлены на стимулирование развития и внедрения российских разработок в отдельных сферах.

Документом предлагаются следующие мероприятия:

- 1) поправки в налоговое законодательство, предусматривающие учет расходов на приобретение и внедрение отечественного программного обеспечения, в том числе и технологий ИИ (мера предложена в целях дальнейшего расчета налога на прибыль организации);
- 2) предложения по внесению изменений в нормативные правовые акты в сфере здравоохранения в целях обеспечения регламентированного доступа российских разработчиков решений в сфере ИИ к деперсонализированным (обезличенным) государственным дата-сетам (наборам данных) и сведениям из электронных медицинских карт; внесение изменений в нормативные правовые акты в целях создания репозитория (хранилища данных) государственных дата-сетов (обработанного и структурированного массива данных) для использования российскими разработчиками ИИ-решений и урегулирования вопросов передачи обезличенных данных, а также порядка доступа разработчиков ИИ-решений к данным, содержащимся в репозитории;
- 3) внесение изменений в ведомственные программы цифровой трансформации, предусматривающих создание репозитория данных для российских разработчиков ИИ-решений, а также реализацию проектов по внедрению ИИ в сфере государственных услуг, здравоохранения, образования, безопасности и др.;
- 4) внесение изменений в нормативные правовые акты в целях введения обязательных требований о необходимости использования отечественных решений в сфере ИИ в ЖКХ, пожарной и другой безопасности.

По замыслу разработчиков документа, «дорожная карта» должна дать импульс развитию ИТ-индустрии и практическому внедрению технологий ИИ в повседневную деятельность организаций, предприятий и граждан, что в конечном итоге должно привести к качественному преобразованию отдельных сегментов государственного управления, отечественной экономики, промышленности и социальной сферы.

Важно принимать во внимание санкционное давление и необходимость обеспечения ясных перспектив развития правового регулирования применения технологий ИИ, направленных на повышение спроса на отечественные ИТ-решения,

<sup>11</sup> План мероприятий («дорожная карта») «Создание дополнительных условий для развития отрасли информационных технологий» (утв. Правительством РФ 09.09.2021) // URL: <http://government.ru/news/43255/> (дата обращения: 16.01.2023).

обеспечение ускоренной цифровой трансформации, создание комфортных условий ведения ИТ-бизнеса в Российской Федерации. Речь идет о стимулировании российских разработок в сфере ИИ, больших данных, интернета вещей и информационной безопасности. Ключевой является подготовка кадров для отдельных отраслей экономики, необходимых для внедрения современных цифровых решений<sup>12</sup>.

В условиях изменившихся геополитических реалий после 24.02.2022 остро встал вопрос о расширении мер государственной поддержки отечественных разработок в сфере ИИ, особенно тех, которые направлены на достижение целей национального развития на период до 2024 года<sup>13</sup>, в части, касающейся применения технологий ИИ, и на обеспечение защиты отечественных компаний от неправомерных односторонних ограничительных действий со стороны третьих стран (США, государств Евросоюза, Норвегии, Японии, Австралии и др.).

В ноябре 2022 г. Президент РФ Владимир Путин, выступая на дискуссионной площадке международной конференции по ИИ и машинному обучению Artificial Intelligence Journey — 2022 с докладом на тему «Технологии искусственного интеллекта для обеспечения экономического роста», обратил внимание участников мероприятия на важность внедрения технологий ИИ в национальные проекты и государственные программы. В частности, главой государства было заявлено следующее: «Технологическое развитие ускоряется, каждая отрасль, предприятие, организация должны быстрее перестраивать свои взгляды и подходы, отбрасывать мешающие двигаться вперед шаблоны. Считаю, что каждый национальный проект, государственная программа должны содержать конкретные меры, направленные на внедрение в отраслях технологий искусственного интеллекта»<sup>14</sup>.

Разнообразные технологии ИИ активно применяются в производстве товаров, работ, услуг, в новых цифровых технологиях и сети Интернет, посредством них эффективно решаются функциональные задачи (производственные, технические, организационные и проч.). В связи с вышеизложенным представляется интересной позиция В. К. Андреева о целесообразности включения в состав предприятия как имущественного комплекса (ст. 132 ГК РФ) цифровых технологий, искусственного интеллекта как вида имущества и как охраняемых результатов интеллектуальной деятельности<sup>15</sup>.

В целях обеспечения цифрового суверенитета в части его правового регулирования представляется интересным исследование Е. Б. Подузовой об отношениях

<sup>12</sup> План мероприятий («дорожная карта») «Создание дополнительных условий для развития отрасли информационных технологий».

<sup>13</sup> Распоряжение Правительства РФ от 01.10.2021 № 2765-п // URL: [https://www.economy.gov.ru/material/dokumenty/edinyy\\_plan\\_po\\_dostizheniyu\\_nacionalnyh\\_celej\\_razvitiya\\_rossiyskoy\\_federacii\\_na\\_period\\_do\\_2024\\_goda\\_i\\_na\\_planovyy\\_period\\_do\\_2030\\_goda.html](https://www.economy.gov.ru/material/dokumenty/edinyy_plan_po_dostizheniyu_nacionalnyh_celej_razvitiya_rossiyskoy_federacii_na_period_do_2024_goda_i_na_planovyy_period_do_2030_goda.html).

<sup>14</sup> URL: <http://www.kremlin.ru/events/president/transcripts/speeches/69927> (дата обращения: 16.01.2023).

<sup>15</sup> Андреев В. К. Приобретение и осуществление прав юридического лица с использованием искусственного интеллекта // Предпринимательское право. 2021. № 4. С. 11—17.



по оказанию услуг в сфере использования ИИ, в рамках которого рассмотрены проблемы, связанные с предоставлением исключительного права на ИИ при возмездном оказании услуг, а также с электронным обменом данными, обеспечением конфиденциальности информации. Рассмотрены условия обеспечения конфиденциальности, целесообразности порядка идентификации и аутентификации пользователя при использовании ИИ<sup>16</sup>.

Обращают на себя внимание дискуссии о правосубъектности ИИ<sup>17</sup>, в том числе и при создании результатов интеллектуальной деятельности<sup>18</sup>, а также правоприменительная практика зарубежных стран о признании такой правосубъектности<sup>19</sup>.

В соответствии с п. 3.17 ГОСТа Р 430.5-2009 ИИ определяется как моделируемая (искусственно воспроизводимая) интеллектуальная деятельность мышления человека. В этой связи А. В. Минбалева справедливо отмечает, что цифровые понятия, в том числе и искусственный интеллект, должны формироваться изначально на уровне технического регулирования, и право как механизм правового воздействия не должно ставить перед собой задачу урегулировать технические объекты<sup>20</sup>. Примерно по такому пути идут власти КНР, где создана Администрация киберпространства (Cyberspace Administration of China — САС), разработавшая целый пакет рекомендаций, которым необходимо следовать при использовании и разработке технологий ИИ<sup>21</sup>.

В то же время вызывает интерес позиция Б. А. Шахназарова о том, что физические лица при этом должны иметь возможность контролировать ИИ — систему высокого риска в контексте требования о человеческом надзоре. Как представляется, человеческий надзор должен быть нормативно установленным фильтром использования систем ИИ любого уровня риска. Здесь необходим разумный баланс между деятельностью ИИ и деятельностью человека при обязательном

<sup>16</sup> Подузова Е. Б. Договоры об оказании услуг в сфере использования «искусственного интеллекта» и технологий «искусственного интеллекта»: проблемы теории и практики // Актуальные проблемы российского права. 2022. № 8. С. 59—67.

<sup>17</sup> См., например: Егорова М. А. Особенности определения правосубъектности искусственного интеллекта в контексте преподавания дисциплин в сфере интеллектуальной собственности в условиях цифровизации // Право и цифровая экономика. 2021. № 4. С. 73—76.

<sup>18</sup> См., например: Эббот Р. Проект «Искусственный изобретатель» // Журнал ВОИС. 2019. № 6. URL: [https://www.wipo.int/wipo\\_magazine/ru/2019/06/article\\_0002.html](https://www.wipo.int/wipo_magazine/ru/2019/06/article_0002.html) (дата обращения: 16.01.2023).

<sup>19</sup> См.: Янушкевич К. Австралийский суд подтвердил право нейросети на получение патента // URL: <https://trends.rbc.ru/trends/industry/6109576b9a794779eed90de8> (дата обращения: 16.01.2023).

<sup>20</sup> Механизмы и модели регулирования цифровых технологий : монография / под ред. А. В. Минбалева. М., 2020. С. 13.

<sup>21</sup> ИИ под контролем: Как Китай будет регулировать технологии искусственного интеллекта // URL: <https://overclockers.ru/blog/amv212/show/81091/ii-pod-kontrolem-kak-kitaj-budet-regulirovat-tehnologii-iskusstvennogo-intellekta> (дата обращения: 16.01.2023).

восприятию целей ИИ по упрощению и оптимизации общественных процессов, а также при добросовестном и законном использовании систем ИИ человеком<sup>22</sup>.

В зарубежной доктрине, в частности в США, уже сейчас отмечается необходимость реализации концепции уголовной ответственности за действия искусственного интеллекта, учитывающей действия создателя, программиста, пользователя и иных имеющих отношение к ИИ лиц<sup>23</sup>.

Учитывая вышеизложенное, можно сформулировать следующие выводы:

- 1) активное внедрение технологий ИИ во все ключевые сферы государства и общества, а также обеспечение его надлежащего правового регулирования являются одними из основных средств достижения национального цифрового суверенитета;
- 2) национальная безопасность в условиях санкционного давления неразрывно связана с цифровым суверенитетом, что должно отражаться не только в импортозамещении оборудования, так называемого «железа», или программного обеспечения, но и в обеспечении качественного правового регулирования, соответствующего релевантным запросам национальной экономики и общества;
- 3) нормативное обеспечение цифрового суверенитета не может быть эффективным без достаточной технологической базы, поэтому отечественному экспертному сообществу необходимо провести работу по формированию обновленной документации, отвечающей запросам сегодняшнего дня, на уровне технического регулирования.

Непринятие во внимание объективных процессов может привести к усилению кризисных процессов и снижению влияния тех государств, которые в новой технологической гонке будут цепляться за стремительно устаревающие парадигмы, в том числе и правовые. Конкуренция идет не только внутри нашей страны, между субъектами управленческих отношений, но и между государствами и транснациональными компаниями (своего рода гонка за юрисдикцию).

Российской Федерации все больше придется приспосабливаться к правилам конкурентной борьбы в вопросах реализации прежних суверенных полномочий, и важной составляющей в этом вопросе будет степень защищенности нашего цифрового суверенитета.

## БИБЛИОГРАФИЯ

1. Андреев В. К. Приобретение и осуществление прав юридического лица с использованием искусственного интеллекта // Предпринимательское право. — 2021. — № 4. — С. 11—17.
2. Егорова М. А. Особенности определения правосубъектности искусственного интеллекта в контексте преподавания дисциплин в сфере интеллектуальной

<sup>22</sup> Шахназаров Б. А. Правовое регулирование отношений с использованием искусственного интеллекта // Актуальные проблемы российского права. 2022. № 9. С. 63—72.

<sup>23</sup> См., например: Hallevy G. When Robots Kill: Artificial Intelligence under Criminal Law. University Press of New England, 2013.



- собственности в условиях цифровизации // Право и цифровая экономика. — 2021. — № 4. — С. 73—76.
3. *Ершова И. В., Енькова Е. Е.* Санкционный комплаенс, или внутрифирменное управление рисками от рестрикций // Актуальные проблемы российского права. — 2022. — № 8. — С. 93—103.
  4. Механизмы и модели регулирования цифровых технологий : монография / под ред. А. В. Минбалева. — М., 2020.
  5. *Подузова Е. Б.* Договоры об оказании услуг в сфере использования «искусственного интеллекта» и технологий «искусственного интеллекта»: проблемы теории и практики // Актуальные проблемы российского права. — 2022. — № 8. — С. 59—67.
  6. *Шахназаров Б. А.* Правовое регулирование отношений с использованием искусственного интеллекта // Актуальные проблемы российского права. — 2022. — № 9. — С. 63—72.
  7. *Эббот Р.* Проект «Искусственный изобретатель» // Журнал ВОИС. — 2019. — № 6.

## Институт личной информации религиозного характера: определение и структура. Особенности оборота такой информации в киберпространстве

**Аннотация.** В статье представлен авторский подход к определению и структуре института личной информации религиозного характера и обороту такой информации в киберпространстве. В статье читателю предлагается определение указанного института, а также раскрывается состав информации и данных, которые в него входят. Приводятся конкретные примеры такой информации и рассматривается зарубежный и международный опыт ее определения и защиты. Утверждается, что данный институт регулируется нормами не только информационного права, но и иных отраслей права. Для обоснования предложенного подхода проводится анализ различных отраслей российской правовой системы и норм, которые составляют институт личной информации религиозного характера. В результате исследования делается вывод о комплексности института личной информации религиозного характера и о необходимости разработки специальных методов межотраслевой защиты, а также формируются предложения о стандартизации процессов анонимизации и деанонимизации такой информации в киберпространстве.

**Ключевые слова:** права человека, свобода совести, персональные данные, личная информация, информационное право, личная тайна, конфиденциальность информации.



**Артем Андреевич ТКАЧЕНКО,**  
ассистент кафедры  
информационного права  
и цифровых технологий  
Университета имени  
О.Е. Кутафина (МГЮА),  
советник юстиции 3 класса  
[aatkachenko@msal.ru](mailto:aatkachenko@msal.ru)  
125993, Россия, г. Москва,  
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2023.102.2.187-195

**ARTEM A. TKACHENKO,**

assistant of the Department of information law and digital technologies  
of the Kutafin Moscow State Law University (MSAL),  
3 class adviser of Justice  
[aatkachenko@msal.ru](mailto:aatkachenko@msal.ru)  
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

### The Institution of Personal Information of Religious Nature: Definition, Structure, the Specificities of the Circulation in Cyberspace

**Abstract.** The article presents the author's approach to the definition and structure of the institute of personal information of religious nature and the circulation of such information in cyberspace. The article offers the reader a definition of the mentioned institute as well as discloses the composition of

© Ткаченко А. А., 2023

*the information and data that it includes. The article provides specific examples of such information and discusses foreign and international experience in defining and protecting it. It is argued that this institution is governed not only by the rules of information law but also by the rules of various branches of law. In order to confirm the proposed approach, an analysis of the various branches of the Russian legal system and the norms that make up the institute of personal information of a religious nature. The study concludes that the institute of personal information of a religious nature is complex and the need to develop special methods of inter-sectoral protection, as well as forming proposals for the standardization of processes of anonymization and de-anonymization of such information in cyberspace.*

**Keywords:** *human rights, freedom of conscience, personal data, personal information, information law, privacy, confidentiality of information.*

В рамках цифровизации современной жизни и перехода большей части процессов в телекоммуникационные сети можно наблюдать все большее скопление личной информации в облачных хранилищах больших данных мультисервисов, например, в экосистемах «Госуслуги», «ВК», «Яндекс», «Сбер», «Гугл» и т.д. и социальных сетей. Пользователи названных площадок предоставляют в рамках своей деятельности и использования их сервисов большое количество личной информации различного характера, в том числе информации, которая напрямую связана с особыми категориями персональных данных. Вместе с тем сама личная информация, за исключением персональных данных, подлежит защите в общем порядке, установленном действующим законодательством РФ.

Следует отметить, что личная информация — это многосоставный элемент, информационная единица, в которую входят как персональные данные лица, так и иная информация, непосредственно связанная с этим лицом, или же такая информация, при доступе к которой можно точно идентифицировать лицо<sup>1</sup>.

Личная информация, в частности, может касаться реализации гражданином своих конституционных прав и свобод. Так, например, в рамках использования сервисов экосистемы «ВК» пользователи в своем профиле могут указать свое вероисповедание, а также вступать в сообщества, связанные с реализацией их конституционного права на свободу совести. А в рамках сервисов экосистемы «Яндекс» («Яндекс.Еда»), возможно формирование данных о моделях пищевого поведения пользователя, что также может указывать на определенную конфессиональную принадлежность.

В рамках сервисов экосистемы «Сбер» («Сбер Онлайн») формируется информация о благотворительных или иных переводах в религиозные или конфессиональные организации, на счета храмов и приходов, что также непосредственно указывает на конфессиональную принадлежность пользователя сервисов. Вместе с тем такая информация не относится к персональным данным.

<sup>1</sup> What is personal information? // Australian Government. Office of the Australian Information Commissioner. URL: <https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information> (дата обращения: 13.10.2022).

Весь указанный набор данных формирует личную информацию религиозного характера, так как непосредственно связан с реализацией гражданином своего права на свободу совести и вероисповедания.

В данной статье мы рассмотрим определение института личной информации религиозного характера, обозначим его структуру, а также дадим обзор механизмов защиты различных категорий данных, входящих в этот информационный институт. Рассматриваемый институт информации и данных представляет особый интерес в связи с его недостаточной, на наш взгляд, теоретической разработкой и особой важностью для многих граждан нашей страны.

Исходя из вышесказанного, можно сделать вывод о том, что личная информация религиозного характера — это совокупность сведений о реализации гражданином или иным физическим лицом своего права на свободу совести, зафиксированных в определенной форме, и (или) результат преобразования или анализа таких сведений. Данное понятие охватывает широкий спектр данных и информации, начиная от персональных и личных данных, заканчивая информацией, которая может быть собрана автоматизированными системами учета и анализа цифрового поведения (программы анализа потребительского и пищевого поведения, алгоритмы рекламы в сети, алгоритмы учета и записи поисковых запросов и т.д.).

На всеобъемлющий комплекс такой информации указал европейский регулятор по защите персональных данных — Европейский орган по защите данных (European Data Protection Board — EDPB). В Руководстве 8/2020 по сбору информации о пользователях социальных сетей он обозначил, что информация о геолокации и посещении определенных мест (церквей, мест собраний верующих, мест паломничества и др.), в том числе информация, полученная алгоритмами при анализе использования физическим лицом определенных видов сервисов (доставка, поисковые сервисы, новостные сервисы и др.)<sup>2</sup>, по своему источнику получения не является специальной категорией данных в соответствии со ст. 9 Регламента (ЕС) 2016/679 о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных<sup>3</sup>.

Вместе с тем EDPB отмечено, что в случае обработки такой информации совместно с персональными данными лица — источника названной информации результаты обработки подпадают под критерии специальной защиты, предусмотренной Регламентом. Таким образом, указанную информацию можно отнести к личной информации религиозного характера.

Вместе с тем следует отметить, что алгоритмический анализ различного рода данных в Сети чаще всего происходит в анонимизированном виде, т.е. с потерей

<sup>2</sup> Guidelines 8/2020 on the targeting of social media users // URL: [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en) (дата обращения: 13.10.2022).

<sup>3</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // EUR-Lex. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата обращения: 13.10.2022).



связи непосредственно с субъектом данных. Вместе с тем при несанкционированном доступе к серверам, на которых происходит анонимизация собранной информации, возможно деанонимизировать такие сведения.

Порядок обработки информации в анонимизированном виде, стандарты обработки, порядок деанонимизации такой информации, гарантии при ее обработке в настоящее время регулируются непосредственно операторами информации. Вместе с тем представляется необходимым вывести такое регулирование в правовое поле.

Организация по безопасности и сотрудничеству в Европе в докладе «Использование персональных данных в финансовых услугах и роль финансового образования. Ориентированный на потребителя анализ» указывает на то, что финансовая информация, связанная с религиозной активностью лица или с его взносами в бюджет религиозной организации, при определенных условиях может негативно сказываться как на кредитном рейтинге лица, так и на его финансовой безопасности<sup>4</sup>, что также дает нам право отнести информацию о финансовой активности к категории личной информации религиозного характера.

Международная организация труда в рекомендациях «Защита персональных данных работников» также указывает, что информация о предыдущей должности сотрудника в религиозной организации может являться чувствительной и просит работодателя, который обрабатывает данные, относиться к такой информации с особым вниманием и предпринимать все возможные меры по недопущению ее несанкционированного распространения<sup>5</sup>.

Таким образом, мы видим, что личная информация религиозного характера включает: персональные данные о лице, осуществляющем реализацию своего права на свободу слова; информацию о его участии в религиозных культурах или организациях; сведения о его трудовой деятельности; информацию о его цифровом поведении; информацию о финансовой активности.

Данный институт, как мы видим, включает широкий спектр данных и информации и, соответственно, не может ограничиваться лишь персональными данными о религиозных убеждениях.

Определение этого набора данных как института неслучайно. В теории государства и права правовой институт определяется как сравнительно небольшая, устойчивая группа правовых норм, регулирующих определенную разновидность общественных отношений<sup>6</sup>. Правовой институт также обладает рядом признаков: 1) юридическое единство правовых норм, 2) полнота регулирования определенной совокупности общественных отношений, 3) обособление правовых норм, образующих правовой институт, в главах, разделах, частях нормативных правовых актов<sup>7</sup>.

<sup>4</sup> OECD Personal Data Use in Financial Services and the Role of Financial Education // URL: <https://www.oecd.org/finance/Personal-Data-Use-in-Financial-Services-and-the-Role-of-Financial-Education.pdf> (дата обращения: 13.10.2022).

<sup>5</sup> ILO Protection of workers' personal data // URL: [https://www.ilo.org/wcmsp5/groups/public/-/ed\\_protect/---protrav/---safework/documents/normativeinstrument/wcms\\_107797.pdf](https://www.ilo.org/wcmsp5/groups/public/-/ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf) (дата обращения: 13.10.2022).

<sup>6</sup> Матузов Н. И., Малько А. В. Теория государства и права. 2-е изд. М. : Юристъ, 2005.

<sup>7</sup> Казьмин И. Ф., Сырых В. М. Понятие системы права. Правовой институт, отрасль права // Общая теория права / под ред. С. А. Пиголкина. М. : Изд-во МГТУ имени Н. Э. Баумана, 1996.

В нашем случае определенной разновидностью общественных отношений, в рамках которых распространяются и возникают обозначенные данные и информация, являются общественные отношения, возникающие в связи с реализацией и защитой лицом своего конституционного права на свободу совести. Вместе с тем правовое обеспечение реализации и защиты данных и информации, входящих в названный институт, является комплексным (разноотраслевым).

В рамках указанного института в национальной правовой системе России на первом этапе практических исследований можно выделить: нормы-принципы; нормы-дефиниции; нормы, устанавливающие правовое положение операторов соответствующей информации; нормы, устанавливающие правовое положение субъектов такой информации в рамках ее предоставления и распространения; нормы, закрепляющие пределы использования такой информации; нормы, закрепляющие режимы охраны (конфиденциальности) такой информации; нормы-требования; охранительно-запретительные нормы.

Основополагающим актом в сфере обеспечения и защиты личной информации религиозного характера является Конституция РФ, нормы которой закрепляют наличие у гражданина права на реализацию своих прав на свободу совести, а также обязанность государства обеспечить возможности такой реализации и защиту права от нарушений<sup>8</sup>. Эти нормы представляют собой нормы-принципы института.

Развиваются указанные нормы-принципы в таких нормативных правовых актах, как Федеральные законы от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон № 149-ФЗ), от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — Закон № 152-ФЗ), от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и о религиозных объединениях» (далее — Закон № 125-ФЗ), Гражданский кодекс РФ и др.<sup>9</sup>

Закон № 125-ФЗ конкретизирует нормативные гарантии и инструменты защиты для реализации гражданами своего конституционного права на свободу

<sup>8</sup> Конституция Российской Федерации. Статьи 14, 17, 18, 21—24, 28, 29, 30, 36, 37, 43 // СПС «КонсультантПлюс».

<sup>9</sup> См.: Кодекс РФ об административных правонарушениях. Ст. 13.11, 13.12, 13.14; Уголовный кодекс РФ. Ст. 137, 138, 148, 244, 282; Уголовно-процессуальный кодекс РФ. Ст. 56; Уголовно-исполнительный кодекс РФ. Ст. 14, 185; Гражданско-процессуальный кодекс РФ. Ст. 182, 185; Федеральный закон от 2 августа 1995 г. № 122-ФЗ «О социальном обслуживании граждан пожилого возраста и инвалидов». Ст. 12; Федеральный закон от 10 января 1996 г. № 5-ФЗ «О внешней разведке». Ст. 19; Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Ст. 47. Ст. 50; Закон РФ от 11 марта 1992 г. № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации». Ст. 7; Федеральный закон от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации». Ст. 15; Федеральный закон от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации». Ст. 42; Федеральный закон от 2 марта 2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации». Ст. 14, 29; Федеральный закон от 17 января 1992 г. № 2202-1 «О прокуратуре Российской Федерации». Ст. 40.4; Федеральный закон от 3 марта 1995 г. № 40-ФЗ «О Федеральной службе безопасности». Ст. 6.



совести как индивидуально, так и совместно. Пунктом 5 ст. 3 Закона № 125-ФЗ устанавливается запрет на принудительное или несанкционированное разглашение информации о религиозной принадлежности лица или его отношении к религии, а также о его участии или членстве в религиозном объединении лиц (охранительно-запретительные нормы).

Пункт 2 ст. 4 Закона № 125-ФЗ устанавливает право религиозной организации определять конфиденциальный режим обращения ряда данных внутри организации (нормы, устанавливающие правовое положение операторов соответствующей информации). Статья 7 Закона № 125-ФЗ закрепляет особый режим защиты данных и информации, полученных в рамках религиозного обряда исповеди и иных обрядов, в которых каким-либо образом разглашаются личные данные или информация о лицах (нормы, закрепляющие режимы охраны (конфиденциальности) такой информации).

Весь указанный набор установлений в части защиты данных и информации в рамках Закона № 125-ФЗ можно обозначить как режим религиозной тайны<sup>10</sup>. Вместе с тем данный режим не является исчерпывающим для института личных данных религиозного характера.

В рамках Закона № 149-ФЗ информация определяется как сведения, независимо от формы их представления (нормы-дефиниции). Информация может быть предоставлена информационной системе или использована в рамках информационной технологии при санкционировании доступа к информации ее обладателем (нормы, устанавливающей правовое положение субъектов такой информации в рамках ее предоставления и распространения).

Частями 5 и 6 ст. 9 Закона № 149-ФЗ установлено, что информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей (это относится и к священнослужителям или иным сотрудникам религиозной организации) или организациями (в том числе религиозными) при осуществлении ими деятельности, подлежит защите в случаях, если на этих лиц федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации, и такая информация не может быть передана третьим лицам (охранительно-запретительные нормы).

Пунктом 7 ст. 3 Закона № 149-ФЗ устанавливается принцип правового регулирования в сфере информации, информационных технологий и защиты информации, который запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Также пунктом 8 ст. 9 Закона № 149-ФЗ установлен запрет требовать от гражданина предоставления информации о его частной жизни, в том числе информации, составляющей религиозную тайну (нормы, закрепляющие режимы охраны (конфиденциальности) такой информации).

Частью 5 ст. 12.2 Закона № 149-ФЗ устанавливается запрет на использование информации, полученной в результате систематического сбора, записи, систематизации и анализа данных, относящихся к объему и предпочтениям аудитории информационных ресурсов (анонимизированные данные), иначе

<sup>10</sup> Андреев К. М. Понятие и особенности религиозной тайны в рамках реализации конституционной свободы вероисповедания. М. : Юриспруденция, 2015.

чем в целях проведения исследований объема аудитории (охранительно-запретительная норма).

Органом, осуществляющим контроль за оборотом персональных данных и информации, является Роскомнадзор. Вместе с тем Роскомнадзор, в соответствии со своим положением, имеет право применять меры профилактического и пресекающего характера, а также давать разъяснения по вопросам, отнесенным к компетенции службы<sup>11</sup>.

С учетом практики Европейского органа по защите данных можно утверждать, что для эффективной защиты данных, в том числе личной информации религиозного характера, необходимо наделить Роскомнадзор компетенцией по выпуску рекомендаций в сфере ведения службы.

Закон № 152-ФЗ устанавливает правовые основы защиты персональных данных в Российской Федерации, в том числе персональных данных о религиозных убеждениях, а также полученных в рамках религиозной деятельности.

В соответствии со статьей 2 Закона № 152-ФЗ, его целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, в рамках которой может быть также рассмотрена семейная и личная религиозная тайна (охранительно-запретительные нормы).

Статья 10 Закона № 152-ФЗ устанавливает категории специальных персональных данных, обработка которых запрещена. К таким персональным данным относятся данные о религиозных или философских убеждениях (охранительно-запретительные нормы). Их обработка возможна в ряде случаев, в том числе при наличии согласия субъекта персональных данных на такую обработку, и с применением ограничений и условий, установленных в ст. 10.1 (устанавливающей правовое положение субъектов такой информации в рамках ее предоставления и распространения)<sup>12</sup>.

Вместе с тем главой 3 Закона № 152-ФЗ устанавливается обширный круг прав субъекта персональных данных, а также прямые (непосредственные), надзорные (в рамках уполномоченного органа) и судебные методы защиты<sup>13</sup>.

Гражданский кодекс РФ также содержит некоторые нормы о защите личной информации религиозного характера.

Пункт 5 ст. 52 ГК РФ устанавливает право юридического лица самостоятельно принимать нормы относительно своего внутреннего функционирования, в том числе это касается религиозных организаций и установления правил обработки данных внутри них. Такие правила, как нами было отмечено, должны соответствовать

<sup>11</sup> Положение о Роскомнадзоре // URL: <https://rkn.gov.ru/about/> (дата обращения: 13.10.2022).

<sup>12</sup> Защита прав субъектов персональных данных // Управление Роскомнадзора по Томской области. URL: <https://70.rkn.gov.ru/social/p12060/p12067/> (дата обращения: 13.10.2022).

<sup>13</sup> К прямым методам защиты относится непосредственный запрос субъекта персональных данных о прекращении неправомерной обработки его персональных данных; к надзорным — обращение в Роскомнадзор с жалобой на операторов персональных данных или лиц, которые осуществляют неправомерную обработку персональных данных. Судебные методы защиты реализуются в рамках гражданского, уголовного или административного судопроизводства.



законодательству РФ по защите персональных данных (нормы, устанавливающие правовое положение операторов соответствующей информации).

Статья 152.2 ГК РФ устанавливает, что без согласия гражданина не допускаются сбор, хранение, распространение и использование любой информации о его частной жизни, в частности сведений о его происхождении, о месте его пребывания или жительства, о личной и семейной жизни. В вопросы личной жизни также может входить информация о реализации гражданином своего права на свободу совести (охранительно-запретительные нормы).

На основании проведенного анализа можно сделать вывод о том, что правовой статус личной информации религиозного характера закрепляется в различных отраслях права. Многовекторность и сложность набора данных и информации, содержащихся в личной информации религиозного характера, не позволяют вести регулирование этого института лишь в рамки защиты персональных данных.

Также можно отметить, что в большинстве норм, представленных в национальной правовой системе в рамках института личной информации религиозного характера, урегулированы вопросы защиты персональных данных, режимы охраны (конфиденциальности) информации, предоставления согласия на обработку информации субъектом. Вместе с тем в нормативно-правовой базе отсутствует регулирование вопросов, связанных с обращением информации, не являющейся персональными данными, но напрямую связанной с реализацией права на свободу совести в киберпространстве.

Как уже ранее было отмечено, при проведении анализа нами не были обнаружены стандарты проведения процедур анонимизации и деанонимизации данных и информации, собранных в рамках различных исследований различными цифровыми операторами. Не вся такая информация используется для статистики, участвует в исследовании цифрового поведения лиц, может служить основанием для анализа «цифрового следа» и т.д.

Представляется необходимым рассмотреть вопрос урегулирования указанных процессов в рамках нормативных актов ответственного органа государственной власти в виде стандартов или правил поведения, получения, передачи и обработки такой информации, взяв за основу релевантный международный опыт.

Таким образом нами были сделаны выводы о том, что личная информация религиозного характера — это комплексная структурная единица, состоящая из различного рода данных и информации. С развитием цифровизации ее составляющие расширились и, соответственно, правовые нормы должны подстраиваться под возникающие вызовы в связи с распространением личной информации религиозного характера в киберпространстве.

Институт личной информации религиозного характера представляется нам комплексным (разноотраслевым). Его составные части урегулированы в различных отраслях права, но вместе с тем имеют единый предмет своего регулирования — отношения, возникающие в рамках получения, обработки, создания и защиты личной информации религиозного характера.

Вместе с тем представляется также необходимой разработка правового регулирования в сфере оборота информации религиозного характера в киберпространстве.

## БИБЛИОГРАФИЯ

1. *Андреев К. М.* Понятие и особенности религиозной тайны в рамках реализации конституционной свободы вероисповедания. — М. : Юриспруденция, 2015. — 232 с.
2. *Казьмин И. Ф., Сырых В. М.* Понятие системы права. Правовой институт, отрасль права // Общая теория права / под ред. А. С. Пиголкина. — М. : Изд-во МГТУ имени Н. Э. Баумана, 1996.
3. *Матузов Н. И., Малько А. В.* Теория государства и права. — 2-е изд.. — М. : Юристъ, 2005. — 541 с.

# ПРАВО В ИСТОРИЧЕСКОМ ПРЕЛОМЛЕНИИ

## Кибернетика в СССР<sup>1</sup>

**Юрий Григорьевич ШПАКОВСКИЙ,**  
главный редактор  
журнала «Вестник  
Университета имени  
О.Е. Кутафина (МГЮА)»,  
доктор юридических наук,  
профессор

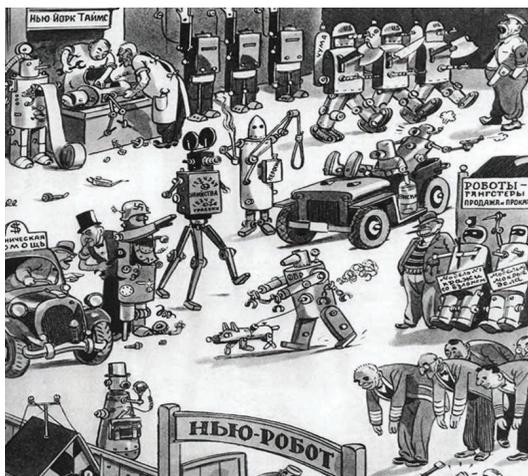
**П**ервые десятилетия после окончания Второй мировой войны современники называли «новой волной рационализации» и сравнивали их с эпохой Ренессанса. Холодная война, гонка вооружений требовали прорывных открытий в науке. Новая система научных знаний получила название «кибернетика».

Сущность кибернетики трактовалась по-разному. Одни называли ее наукой, изучающей математические методы и процессы управления, другие — наукой о передаче, переработке, хранении и использовании информации. Были и те, кто видел суть ее в изучении способов создания, раскрытия, строения и тождественного преобразования алгоритмов, описывающих процессы управления в реальности.

Советское руководство прикладывало большие усилия для развития этой отрасли в СССР. На протяжении 1950—1952 гг. Советом министров был принят целый ряд постановлений, таких, например, как «О проектировании и строительстве автоматической быстродействующей цифровой вычислительной машины» (от 11.01.1950 № 133), «О мероприятиях, обеспечивающих выполнение работ Академией наук СССР по созданию быстродействующих электронных вычислительных машин» (от 01.08.1951 № 2759), «О мероприятиях по обеспечению проектирования и строительства быстродействующих математических вычислительных машин» (от 19.05.1952 № 2373) и др.<sup>2</sup>

Вопросами развития новой отрасли интересовался и лично И. В. Сталин. Например, когда вице-президент Академии наук Украинской ССР М. А. Лаврентьев написал Сталину о необходимости ускорения исследований в области вычислительной техники и перспективах использования ЭВМ, то он был вскоре назначен директором созданного летом 1948 г. в Москве Института точной механики и вычислительной техники (ИТМиВТ) АН СССР. Интерес вождя был вполне понятен: главная сфера применения тогдашних компьютеров — военная.

В 1951 г. в журнале «Вестник машиностроения» была опубликована обширная статья инженера Н. А. Игнатова, в которой наряду с подробным освещением новых советских счетных машин говорилось и о создании машин электронных. Однако



Карикатура на кибернетику 1950-х гг.

<sup>1</sup> Материалы подготовлены с использованием интернет-ресурсов.

<sup>2</sup> Все эти решения Совета министров СССР выходили в свет с грифом «Не для печати» и в свободном доступе отсутствуют.

популяризация темы в массовых журналах имела и негативные последствия для развития кибернетики.

В начале 1950-х гг. в советской прессе вышел ряд критических статей, направленных против кибернетики, что дало повод говорить о существовании гонений на эту науку. В то же время, как можно убедиться, критики кибернетики четко отделяли технический аспект от идеологического.

В основном эти статьи критиковали философские тезисы кибернетики о тождественности человеческого разума и вычислительной машины, но в то же время в «антикибернетических» статьях не отрицалась необходимость развития вычислительной техники, внедрения автоматизации в экономику СССР.

В настоящем выпуске журнала мы предлагаем читателям одну из статей того времени с критикой кибернетики под названием «Кому служит кибернетика». Статья была опубликована в 1953 году в научном журнале «Вопросы философии», № 5 под рубрикой «Критика буржуазной идеологии». Статья была подписана псевдонимом «Материалист».



## Кому служит кибернетика<sup>3</sup>

Среди современных буржуазных социологических теорий, направленных на защиту капитализма, не последнее место занимают «теории», фетишизирующие технику, пытающиеся изобразить ее основным двигателем общественного развития. Некоторые буржуазные ученые склонны все общественные противоречия, существующие в капиталистическом обществе, все беды и несчастья отнести за счет техники. В «мистической силе» техники они видят причины войн, безработицы, кризисов. Эти «социологи» призывают к разрушению техники и возвращению к идиллическим временам первобытной жизни, когда не было ни машин, ни социальных конфликтов. Другие «социологи» из того же лагеря фетишизируют технику как силу положительную, способную якобы устранить все противоречия капиталистического строя.

Все эти измышления ученых лакеев империализма ничего общего не имеют с наукой и свидетельствуют лишь о вырождении современной буржуазной науки.

Развитие техники зависит от характера экономического строя и определяется потребностями общественного производства. Социалистические общественные отношения открывают безграничный простор для развития производительных сил, для максимального совершенствования техники производства.

Только при социалистическом общественном строе оказалась осуществимой та грандиозная техническая революция во всех областях народного хозяйства, благодаря которой Советский Союз за короткий срок во многом превзошел передовые капиталистические страны.

Колоссальные успехи, достигнутые в индустриализации нашей страны, неуклонное прогрессивное развитие техники производства, небывалый в истории рост творческой активности и инициативы миллионов трудящихся, проявляющийся в изобретательстве и рационализаторских предложениях, исчисляемых миллионами, свидетельствуют о том, что социализм как высший общественный строй создал все условия, благоприятствующие расцвету техники. Все это целиком обусловлено действием основного экономического закона социализма, направленного на обеспечение максимального удовлетворения постоянно растущих материальных и культурных потребностей всего общества путем непрерывного роста и совершенствования социалистического производства на базе высшей техники.

Совершенствование социалистического производства целиком отвечает назревшим потребностям социалистического общества. Прогресс науки и техники находится в полном соответствии с производственными отношениями в социалистическом обществе.

<sup>3</sup> Журнал «Вопросы философии», 1953. № 5.

В капиталистических странах, где развитие науки и техники подчиняется действию основного экономического закона современного капитализма, техника развивается в тех областях производства, которые приносят наивысшую прибыль. В доимпериалистический период капитализм способствовал развитию техники почти во всех областях. Правда, и тогда в силу коренных противоречий, присущих капиталистическому строю, тормозились те технические изобретения и научные открытия, которые не сулили капиталистам немедленной прибыли. Эта реакционная тенденция капитализма с особенной силой проявляется на современном этапе его развития, обуславливая уродливое, одностороннее направление развития техники. В капиталистических странах не жалеют затрат на совершенствование техники только в тех отраслях производства, которые обслуживают интересы войны — самого выгодного бизнеса капиталистов.

Развитие техники в военной промышленности капиталистических стран некоторые буржуазные социологи пытаются объяснить мистическими силами самой техники, якобы диктующей сферы своего приложения, а не империалистической политикой.

Так, изобретение атомной бомбы было объявлено учеными лакеями империализма началом «атомного века», требующего и новой, «атомной социологии». Согласно этой «социологии», миром правит «мировой диктатор» — атомная бомба, и люди бессильны противиться этому. Она определяет направление развития общества, стимулирует развитие одних областей производства — военных — и требует сокращения других. Таким образом, с капиталистов снимается ответственность за войны, безработицу, дороговизну средств существования, жилищный кризис и т.д.

Примером того, как односторонне, в военных целях, используются новейшие достижения техники, может служить положение в США новой отрасли производства — индустрии вычислительных машин и других сложных автоматических приборов, имеющих специальное назначение.

Опираясь на новейшие открытия в области радиотехники и телетехники, американские конструкторы создали сложные вычислительные машины, решающие задачи автоматически, при помощи системы передаточных механизмов и сигнализаций, использующих законы обратной связи. Эти машины способны изменить направление математических операций в зависимости от промежуточных результатов.

Конструирование вычислительных машин имеет свою длительную историю. Начиная от первого арифмометра, изобретенного Лейбницем, идет целая серия разнообразных вычислительных приборов, каждый из которых производил все более сложные математические операции. За последние десятилетия производство вычислительных машин подверглось новой реконструкции. Она выразилась в достижении полной автоматизации вычислительных операций. Электронные машины представляют собой огромные агрегаты, в которых, благодаря применению радио- и телетехники, вычислительные операции совершаются с исключительной быстротой. Арифметические действия выполняются ими в тысячные доли секунды. Более сложные, интегральные и дифференциальные вычисления, требующие от высококвалифицированных математиков затраты недельного труда, производятся в минуты и секунды.



Применение подобных вычислительных машин имеет огромное значение для самых различных областей хозяйственного строительства. Проектирование промышленных предприятий, жилых высотных зданий, железнодорожных и пешеходных мостов и множества других сооружений нуждается в сложных математических расчетах, требующих затраты высококвалифицированного труда в течение многих месяцев. Вычислительные машины облегчают и сокращают этот труд до минимума. С таким же успехом эти машины используются и во всех сложных экономических и статистических вычислениях.

Огромным преимуществом этих машин является полная безошибочность их действий и получаемых результатов, тогда как в сложные расчеты, производимые математиками, неизбежно вкрадываются ошибки.

Благодаря вычислительным машинам, современная математика может решать в короткие сроки задачи, считавшиеся раньше из-за большого числа необходимых вычислений неразрешимыми. Это привело к созданию нового раздела прикладной математики, так называемой машинной математики.

В последнее время создано немало и других сложных, саморегулирующихся машин, используемых в различных отраслях производства.

Как вычислительные машины, так и другие автоматические приборы, построенные с применением электроники, получили распространение во многих странах. Они успешно используются и в Советском Союзе, в котором осуществляется огромное строительство.

В США вычислительные машины и другие приборы, снабженные сервомеханизмами, получили одностороннее применение. Вычислительные машины, производящие сложнейшие математические вычисления в предельно короткие сроки, применяются для управления снарядами дальнего действия или летательными аппаратами. Возможность военного использования этого изобретения обеспечила ему в США широкую практику.

В статье «Гигантские мозги, или Думающие машины» Эдмунд Беркли сообщает, что лаборатория вычислительных машин Гарвардского университета обслуживает военно-морской флот; лаборатория Пенсильванского университета работает по заданиям армии; сконструированная ею машина находится в баллистической лаборатории Министерства обороны в Эбердине (штат Мериленд); машины, изобретенные лабораторией телефонной компании Белла, куплены комитетом авиации и баллистической лабораторией Министерства обороны.

Можно не сомневаться в том, что в действительности масштабы использования вычислительных машин в военной промышленности США значительно шире того, что дает скупая, но достаточно красноречивая информация, которая дана в статье Беркли.

Вокруг этого нового изобретения, получившего такое широкое применение в военной промышленности США, американские ученые подняли невообразимую шумиху. Профессор математики Массачусетского университета Норберт Винер увидел в нем очередной «этап» в развитии человечества, новую «промышленную революцию», чреватую огромными социальными последствиями.

По мнению Винера, деятельность вычислительных машин даст ключ к познанию самых разнообразных природных и общественных явлений. Эта в корне

порочная идея послужила Винеру основанием для создания новой «науки» — кибернетики.

За короткий срок своего существования кибернетика приобрела немало сторонников среди буржуазных деятелей науки, работающих в разных областях знаний. Это симптоматично для ученых, которые вынуждены цепляться за обветшалые лохмотья идеалистической философии и даже за такие «новинки» научной фантастики, как кибернетика.

Газета «Нью-Йорк уорлд телеграмм» разрекламировала домыслы Винера как научный подвиг:

*«Доктор Винер сделал для познания человеческого мозга то, что Эйнштейн сделал для познания Вселенной».*

Пропаганда кибернетики получила в капиталистических странах большой размах. Десятки книг, сотни журнальных и газетных статей распространяют ложные представления о «новой науке». Начиная с 1944 г., в Нью-Йорке ежегодно происходят конференции кибернетиков, в которых активно участвуют научные работники самых различных специальностей. Конференции кибернетиков состоялись также во Франции и Англии. Даже в Индию американские экспортеры завезли этот гнилой идеологический товар.

Апологеты кибернетики считают, что область ее применения безгранична. Они утверждают, что кибернетика имеет большое значение не только для решения вопросов, относящихся к телемеханике, саморегулирующимся приспособлениям, реактивным механизмам и сервомеханизмам, но даже к таким областям знания, как биология, физиология, психология и психопатология. Энтузиасты кибернетики допускают, что социология и политэкономия также должны использовать ее теорию и методы.

Что же представляет собой эта новая наука — кибернетика? По-древнегречески слово *«кибернетос»* означает кормчий, а *«кибернетикос»* — способный быть кормчим, то есть способный управлять. Определяя содержание кибернетики, Норберт Винер без излишней скромности заявил:

*«Мы решили назвать кибернетикой всю теоретическую область контроля и коммуникаций, как в машине, так и в живом организме».*

Итак, прежде всего кибернетика ставит перед собой задачу доказать отсутствие принципиальной разницы между машиной и живым организмом. Задача, мягко выражаясь, неблагодарная в XX веке. Но тем не менее, проводя аналогию между работой сложных вычислительных агрегатов, содержащих до 23 тысяч радиоламп, автоматически переключающихся, кибернетики утверждают, что разница между работой такой «умной» машины и человеческим мозгом только количественная. Профессор Лондонского университета Джон Янг с восторгом оповестил мир о том, что *«мозг — это гигантская вычислительная машина, содержащая 15 миллиардов клеток вместо 23 тысяч радиоламп, имеющих в самой крупной из донныне сконструированных вычислительных машин».* И это отнюдь не метафора, а утверждение, претендующее на научность!

Более осмотрительный профессор Гарвардского университета Луис Раденауэр высказался на этот счет осторожнее: *«Самая сложная современная вычислительная машина соответствует уровню нервной системы... плоского червя».*



Существенно в этих высказываниях не то, что в них отмечается разница между количеством «реагирующих клеток», а в том, что в них игнорируется качественная разница между живым организмом и машиной.

Основоположников кибернетики приводит в восхищение способность вычислительных машин к саморегулированию, хотя весь этот процесс, совершающийся в вычислительных машинах, происходит по законам той связи, с помощью той автоматической сигнализации и тех механических приспособлений, которые все до мельчайшего винтика сконструированы человеком и способны действовать лишь по его установкам.

Отбросив это коренное качественное различие между механизмом и организмом как якобы несущественное, теоретики новой науки определяют счетные машины как саморегулирующиеся механизмы, как «мыслящие машины», как «гигантские мозги» и утверждают, что деятельность вычислительных машин дает ключ к познанию как биологических, так и социальных явлений, чем и надлежит заняться кибернетике.

Нетрудно установить, что эти претензии кибернетиков отбрасывают науку на двести лет назад, к взглядам французского материалиста XVIII века Ламеттри. В своем произведении «Человек-машина» Ламеттри проводил аналогию между человеком и машиной. Организм животных — человека, — по Ламеттри, подчиняется таким же материальным закономерностям, как и механизм машин, и приводится в движение воздействием внешних условий, которые через посредство органов чувств и мозга действуют на конечности животного и человека и приводят в действие весь организм. Машина также приводится в действие внешней силой, передающейся с помощью системы механизмов.

Аналогия, проведенная Ламеттри, между человеком и машиной, несмотря на ее механистический характер, имела прогрессивную тенденцию. Она была направлена против представлений об особых божественных силах, якобы управляющих организмом, и доказывала обусловленность его жизнедеятельности действием материальных сил. В противоположность французскому мыслителю XVIII столетия современные кибернетики исходят из стремления принизить человека, показать, что человека вполне можно и нужно заменить машиной, но не любого человека, а только лишнего, такого, который считается «беспокойным элементом». Таким людям кибернетики отказывают в способности суждения, в сознании и сводят всю деятельность их мозга к механической связи и сигнализации. Конечно, до таких социологических измышлений дошли не все кибернетики, но так или иначе все они служат одной цели — разделить людей на **«мыслящую администрацию»**, деятельность которой не сводится к механизму сигнализации, а признается творческой, и **«рабочих со средними способностями»**, которые приравниваются к механизмам. В этом отношении кибернетика оказывается лишь разновидностью распространенной в странах империализма технократической теории, возникшей еще в конце XIX века, вместе с империализмом.

Современные технократы — кибернетики — навели густой наукообразный туман вокруг своей архиреакционной теории. Они проводят *«сравнительное изучение функционирования вычислительных машин и человеческой мысли»*, нервной системы и передаточных механизмов и приходят к выводу, что *«сверхскоростная*

*вычислительная машина является почти идеальной моделью для понимания проблем, возникающих при изучении нервной системы».*

Профессор анатомии Глазговского университета Джордж Уиберн в статье, опубликованной в 1952 году, пишет:

*«Кибернетики подходят к проблеме нервной деятельности с чисто функциональной точки зрения и рассматривают деятельность мозга в целом как электронные устройства современной системы коммуникаций и сервомеханизмов, стараясь использовать их в терминах теории информации и статистики».*

Подобные механистические представления о мозге высказываются в то время, когда наука в лице русских ученых И. М. Сеченова и И. П. Павлова создала учение о физиологии высшей нервной деятельности животных и человека, освещающее деятельность мозга с последовательно материалистических позиций, дающее действительное решение вопроса об отношении мышления к бытию, сознания к материи.

Самое прогрессивное учение современного естествознания встречает бешеное сопротивление со стороны реакционеров от науки. Так как они не в состоянии найти научные аргументы против учения И. П. Павлова, то им остается стать на путь фальсификации и извращения этого учения. Ничтоже сумняшеся, они наделяют вычислительную машину свойствами центральной нервной системы. *«Ничто не препятствует вычислительной машине демонстрировать условные рефлексы»*, — утверждает Винер, имея при этом в виду изобретенную Греем Уолтером саморегулирующуюся машину, которая может быть приведена в движение свистком. Эта машина приближается к цели, если последняя излучает слабый свет, и отталкивается от нее, если цель дает сильное излучение, она способна обходить препятствия. И тем не менее это всего лишь механизм, управляемый звуковыми, световыми и механическими сигналами и ничего общего не имеющий с рефлексами человека.

По учению И. П. Павлова, мозг регулирует все функции организма, всю его жизнедеятельность. Мозг — орган познавательной и созидательной деятельности человека, материальный субстрат его психики. По определению И. П. Павлова, *«нервная система на нашей планете есть невыразимо сложнейший и тончайший инструмент сношений, связи многочисленных частей организма между собой и организма как сложнейшей системы с бесконечным числом внешних влияний»* (Павлов И. П. Соч. Т. 3. С. 559).

Кора больших полушарий головного мозга представляет собой систему анализаторов, то есть тех сложных приборов, которые воспринимают все явления действительности, анализируют и синтезируют их. Вся функциональная деятельность коры соотнесена с ее анатомической структурой. Сама же деятельность мозга обусловлена воздействием на него через воспринимающие приборы анализаторов — глаз, ухо, кожа и др. — многочисленных раздражителей внешнего мира и внутренней среды организма. Вся эта деятельность строго детерминирована воздействиями на мозг извне и является рефлексом, то есть ответом на эти воздействия.

Бессмертной заслугой И. П. Павлова является созданное им стройное учение о рефлекторной деятельности мозга, установление существенных различий



между врожденными, безусловными, рефлексам, образовавшимися в процессе длительной эволюции вида, и приобретенными в индивидуальной жизни животного, условными, рефлексам, образующимися в тех случаях, когда действие внешнего раздражителя совпадает по времени с безусловным рефлексом или непосредственно предшествует ему.

Каждое раздражение, воспринятое периферическими нервными приборами и центральным концом анализатора, вызывает в нем возбуждение, которое распространяется на соседние участки коры, а затем вновь концентрируется в исходном участке. Разные раздражители в зависимости от их биологического значения для организма могут вызвать в коре различные процессы — возбуждение или торможение с одинаковой тенденцией любого из этих процессов к распространению по всей коре и последующему сосредоточению в исходном участке. Взаимодействие процессов возбуждения и торможения, их чередование и взаимная индукция являются объективными законами высшей нервной деятельности.

Одним из важнейших открытий И. П. Павлова является установление того факта, что у человека к деятельности обычных многочисленных раздражителей внешней среды, воздействующих непосредственно на органы зрения, слуха и другие анализаторы первой сигнальной системы, присоединяется вторая сигнальная система действительности — речь, которая вносит новый принцип в высшую нервную деятельность человека. Слово для человека является раздражителем особого рода, многообъемлющим по своему значению, не идущим в сравнение ни с какими другими раздражителями первой сигнальной системы, общей для человека и животных. Благодаря речи, дающей человеку возможность отвлечения и вместе с тем обобщения сигналов предшествующей системы, мысль человека облекается в наиболее гибкую и выразительную форму. Этим в высшую нервную деятельность человека вносится принцип, *«обуславливающий безграничную ориентировку в окружающем мире и создающий высшее приспособление человека — науку, как в виде общечеловеческого эмпиризма, так и в ее специализированной форме»* (Павлов И. П. Соч. Т. 3. С. 476).

Учение И. П. Павлова о высшей нервной деятельности является естественнонаучной основой материалистической психологии. Оно ставит человеческую психику на твердую почву объективных законов природы, тогда как идеалистическая психология окутывает ее мистическим покровом. Опираясь на законы высшей нервной деятельности, открытые великим физиологом, материалистическая психология дает подлинно научное объяснение психической деятельности человека, показывает, как работа мозга обуславливает целенаправленную деятельность человека, сумевшего приспособиться к природе, создать ту искусственную среду, ту материальную и духовную культуру, которая неизмеримо высоко подняла его над остальным животным миром. Человек, благодаря работе мозга, достигшего сложнейшего строения, смог проникнуть в тайны природы, сформулировать ее законы, создать промышленность на основе высокой техники.

Это относится, в частности, и к вычислительным машинам, которые также созданы человеческим мозгом — этим наисовершеннейшим творением природы.

Нам понадобилось некоторое отступление в область физиологии высшей нервной деятельности для того, чтобы показать всю несостоятельность аналогий, проводимых кибернетиками между вычислительной машиной и мозгом.

Ученым лакеям капитализма трудно отрицать величайшее достижение павловской физиологии, но так как она является серьезным препятствием в создании ими научной фантазмагии, они спешат объявить учение И. П. Павлова... превзойденным. В статье «Гипотеза кибернетики», помещенной в № 5 «Британского журнала философии науки» за 1951 год, Джон Уисдом пишет: *«Кибернетика — это наука об обратной связи у животных... Неврология может теперь сделать новый шаг вперед по сравнению с капитальной работой Павлова».*

В чем же заключается этот шаг вперед? *«Все, что нам известно, — пишет тот же автор, — это то, что мозг меньше похож на систему рычагов и шестерен, чем на радиолокационную установку или термостат...».* При помощи таких софистических фокусов Уисдом попросту уваливает от подтверждения своего невежественного заявления.

В заключение статьи автор задумывается над тем, не перехватил ли он в оценке кибернетики, и с прискорбием заявляет: *«Правда, кибернетика упускает из виду духовный аспект действия... Она не разрешает проблемы соотношения духа и тела, поскольку она отбрасывает один из соотносящихся элементов и страдает односторонностью своих предшественников (бихевиористов и др.)».*

Итак, кибернетика *«упускает из виду»* всего-навсего сознание. Уисдом туманно называет его *«одним из соотносящихся элементов».* Американские бихевиористы за полстолетие до кибернетиков создали уже такую абсурдную концепцию. Выбросив сознание из психологии, они рассматривают животных и человека как машины, реагирующие на внешние раздражители.

В то время как И. П. Павлов применил открытый им метод объективного изучения высшей нервной деятельности для естественно-научного обоснования происхождения и деятельности сознания как функции мозга; кибернетики вслед за бихевиористами отбросили сознание — *«один из соотносящихся элементов»*, потому что его при всем желании нельзя приписать машине.

Известный французский ученый физик Луи де Бройль трезво заключает: *«Поскольку невозможно приписать этим машинам сознание, аналогичное нашему, деятельность вычислительных машин, как бы они ни были совершенны, нельзя отождествлять с деятельностью нашего мышления. Нельзя ожидать, что кибернетика даст нам ключ ко всей совокупности биологических явлений».*

И другие буржуазные ученые, даже соблазненные перспективами кибернетики, высказывают сомнение насчет всеобъемлющего значения этой псевдонауки. В начале прошлого года сессия индийского научного института в Бенгалоре специально обсуждала вопрос о кибернетике. К чести индийских ученых, следует отметить, что на этой сессии раздавались и трезвые голоса ученых (Говендасвами, Чанди), подвергших критике лженаучные претензии кибернетиков.

Непримиримую позицию по отношению к лженаучной кибернетике занимают ученые-марксисты. В апрельском номере теоретического органа французских марксистов «Ла пансе» за текущий год (№ 47) напечатана статья Андре Лянтэна, разоблачающая кибернетические мистификации. Автор статьи намечает основные линии научной критики кибернетических измышлений.

Правильно отмечая положительное техническое и научное значение развития нового типа машин, основанных на электронике, Лянтэн разъясняет, что *«вне области технологии кибернетика является лишь затеянной в огромных*



*масштабах мистификацией»,* основанной на легковесных, ненаучных аналогиях. По мнению Лянтэна, кибернетика тщетно пытается перенести формы движения, свойственные одним видам материи, на качественно отличные формы материи, где действуют иные, высшие закономерности.

С этой точки зрения Лянтэн раскрывает несостоятельность антинаучных механистических построений кибернетиков, пытающихся «превзойти» научную физиологию, разработанную И. П. Павловым. Кибернетика, по словам Лянтэна, — это *«орудие холодной войны против Павлова»*. Журнал передовой научной мысли «Ла пансе» предостерегает против кибернетических мистификаций и призывает французских ученых разных специальностей принять участие во всесторонней критике этой лженауки, пропагандируемой американским империализмом, старающейся проникнуть в самые различные отрасли знания.

Кибернетики стремятся приписать универсальное значение принципу действия вычислительных машин, они распространяют его не только на живые организмы, но и на все общество.

*«Один из уроков этой книги, — пишет Винер, — состоит в том, что всякий организм сохраняется в своей деятельности как единое целое благодаря тому, что он обладает средствами приобретения, использования, сохранения и передачи информации. В обществе... такими средствами служат: печать, радио, телефон, телеграф, почта, театр, кино, школы и церковь»* (Н. Винер «Кибернетика или контроль и коммуникации в животном и в машине» — Wiener Norbert «Cybernetics or Control and communication in the animal and the machine». 1949).

Суждения Винера об общественных явлениях необычайно примитивны. Он пропагандирует неверие в возможность познания их и в достоверность тех данных, которыми располагают общественные науки:

*«В общественных науках мы не можем быть уверены, что значительная часть наблюдаемых нами явлений не есть наше собственное измышление... Эти науки никогда не могут обеспечить нас надежной, проверенной информацией... Не следует возлагать преувеличенные ожидания на возможности этих наук»*.

Нет необходимости оспаривать это утверждение в отношении общественных наук в капиталистических странах, где действительно субъективные измышления деятелей этих наук служат критерием истины. Не будем возражать также против того, что общественные науки в странах капитализма не могут обеспечить надежной, проверенной информацией. Бесполезно ждать этого от наук, основная задача которых состоит в том, чтобы скрывать правду, затушевывать вопиющие противоречия капитализма, отравлять ядом лжи и обмана трудящиеся массы.

Но кибернетики объективно выступают против всякой общественной науки. Винер отрицает объективный характер законов общественного развития, не зависящих от воли и сознания людей. «Основоположник» кибернетики выражает неверие в общественные науки и уповает на деятельность вычислительных машин новейших конструкций, которым якобы суждено внести существенные коррективы в общественную жизнь.

Винер уверяет, что обществу предстоит пережить новую революцию, на которую он возлагает большие надежды.

*«Нынешний промышленный переворот, — вещает он, — ведет к обесцениванию человеческого мозга, по крайней мере, в его простейших и более рутинных функциях... Квалифицированный ученый и квалифицированный администратор могут пережить эту промышленную революцию. Но коль скоро она совершится, рядовому человеку со средними способностями или со способностями ниже среднего нечего будет продавать, за что стоило бы что-либо платить».*

Такова мрачная перспектива, которую кибернетика открывает перед трудящимися, зачисляющимися в разряд людей «средних способностей». Останутся вычислительные машины совершенной технической конструкции, «гигантские мозги», которые будут управлять всеми остальными машинами благодаря круговым процессам типа обратной связи. Необходимость в рабочих отпадет, ибо регулированием деятельности самих вычислительных машин займутся квалифицированные администраторы и ученые, та самая «технически квалифицированная интеллигенция», которой технократы предсказывали господство в будущем обществе.

Кибернетики не задумываются над тем, куда же денется вся масса рабочих «со средними способностями или со способностями ниже среднего». Если им не за что будет платить, то кто же будет покупать то, что произведут промышленность и сельское хозяйство, управляемые механическими мозгами?

Винеру, очевидно, невдомек, что, рисуя подобную перспективу, он подрубает тот сук на дереве жизни, на котором еще продолжает держаться капитализм, ибо нельзя уничтожить рабочий класс, не уничтожив капитализма.

Но не только рабочие будут, по мнению кибернетиков, вытеснены вычислительными машинами. Эта участь угрожает даже... дипломатам. Снискавший печальную известность на дипломатическом поприще, бывший глава американской делегации на переговорах в Кэсоне и Паньмыньчжоне, контр-адмирал Джой в речи, произнесенной в Гарвардском университете, заявил:

*«Пожалуй, не будет фантазией предсказать, что будущее развитие производства механических мозгов может привести к созданию такого механизма, который будет содействовать анализу проблем международных отношений».*

В представлении контр-адмирала Джоя, в будущих международных конференциях и дипломатических переговорах со стороны США будут принимать участие за круглым столом вместо живых представителей машины. Джой возлагает больше надежд на механические мозги, чем на мозги ныне действующих американских дипломатов. Хотя это только фантазия, притом весьма нелестная для коллег Джоя на дипломатическом фронте, она все же свидетельствует о неверии американских политиков и идеологов в продуктивную деятельность человеческого мозга. В противном случае они не договорились бы до такой беспрецедентной глупости.

Но эта глупость вполне закономерна. Она является логическим выводом из «теоретического» предвидения «основоположника» кибернетики, увидевшего суть грядущей промышленной революции в замене рабочих роботами, снабженными механическими мозгами.

К счастью для человечества, эта опасность ему не угрожает. Кибернетика — одна из тех лженаук, которые порождены современным империализмом и обречены на гибель еще до гибели империализма.



Теория кибернетики, пытающаяся распространить принципы действия вычислительных машин новейшей конструкции на самые различные природные и общественные явления без учета их качественного своеобразия, является механицизмом, превращающимся в идеализм. Это пустоцвет на древе познания, возникший в результате одностороннего и чрезмерного раздувания одной из черт познания.

Не следует закрывать глаза на те глубоко реакционные, человеконенавистнические выводы, которые делают кибернетики, пытаясь решать общественные проблемы.

Перепуганные рабочим движением империалисты мечтают о таком положении, когда никто не будет угрожать их господству. Роботы, только роботы их устраивают; все остальное человечество пусть гибнет, лишь бы остались они и машины, их обслуживающие. Наукообразные бредни кибернетиков отражают этот страх перед трудящимися массами.

Автор уже цитированной нами статьи Эдмунд Беркли пишет: *«Сомнительно, чтобы машины-роботы сами по себе были опасны для людей. Но, когда враждебные обществу люди получают возможность контроля над машинами-роботами, опасность для общества будет велика...»*. Опасными для общества людьми Беркли считает отнюдь не своих империалистических хозяев, а коммунистов и идущих вместе с ними трудящихся, которые могут так же овладеть техникой управления саморегулирующимися машинами, как они овладели ею в Советском Союзе.

Между тем вычислительные машины, или «гигантские мозги», тесно связаны по меньшей мере с двумя родами оружия — с атомными взрывами и управляемыми снарядами. В этом, по мнению Беркли, таится опасность, и поэтому *«было бы благоразумно, если бы в США вся деятельность в этой области находилась под контролем Министерства обороны»*.

Вот какому богу служит кибернетика! Все свои бесспорные практические достижения в конструировании вычислительных машин вместе с глубоко реакционными теориями она несет на алтарь войны. В этом отношении кибернетики проявляют большую активность.

Империалисты бессильны разрешить те противоречия, которые раздирают капиталистический мир. Они не в состоянии предотвратить неумолимо надвигающийся на них экономический кризис. Они не могут избавиться от страха, который внушает им победоносное развитие Советского Союза и стран народной демократии. Безрезультатными оказываются их попытки сломить нарастающее национально-освободительное движение в колониальных и зависимых странах. В дикий ужас повергает их рост революционного сознания и сопротивления рабочего класса и могучее массовое движение прогрессивного человечества в борьбе за мир.

Они ищут спасения не только в бешеной гонке вооружений, но также в идеологическом оружии. В отчаянии они прибегают к лженаукам, которые дают им хотя бы тень надежды на продление существования.

Процесс производства, осуществляемый без рабочих, одними только машинами, управляемыми гигантским мозгом вычислительной машины! Ни забастовок, ни

стачек, ни тем более революционных восстаний! Машины вместо мозга, машины без людей! Какая заманчивая перспектива для капитализма!

Великий основоположник марксизма гениально предвидел возможность подобной деградации мышления ученых слуг господствующих классов, порождаемой антагонизмом между производительными силами и производственными отношениями капиталистического общества.

*«Даже чистый свет науки не может... сиять иначе, как только на темном фоне невежества. Результат всех наших открытий и всего нашего прогресса, очевидно, тот, что материальные силы наделяются духовной жизнью, а человеческая жизнь оупляется до степени материальной силы» (Маркс К. Соч. Т. 11. Ч. 1. С. 5—6).*

Панический страх идеологов империализма перед активной творческой деятельностью человеческого мышления, перед человеком, сознающим свою роль и место в обществе, заставляет их измышлять человеконенавистнические лже-теории, подобные кибернетике.

В такой безнадежный тупик загнаны дипломированные холопы империализма, обязанные в угоду своим хозяевам поставлять новейшие технические изобретения на службу массовому истреблению людей и разрушению величайших достижений материальной и духовной культуры человечества.

*Материалист*

## Памятники права

### **Постановление ЦК КПСС и Совета министров СССР от 8 октября 1970 г. № 849-291 «О мерах по совершенствованию управления в народном хозяйстве на основе широкого использования средств вычислительной техники»**

Центральный комитет КПСС и Совет министров СССР отмечают, что на современном этапе развития экономики Советского Союза одним из важнейших факторов повышения эффективности общественного производства является совершенствование управления в народном хозяйстве на основе широкого использования средств вычислительной техники и автоматизированных систем управления.

Однако работы по внедрению электронной вычислительной техники и автоматизированных систем для управления в народном хозяйстве развернуты еще слабо. Постановление ЦК КПСС и Совета министров СССР от 6 марта 1966 года № 187 «Об улучшении организации работы по созданию и внедрению в народное хозяйство средств вычислительной техники и автоматизированных систем управления» и постановление Совета министров СССР от 30 декабря 1967 года № 1180-420 «О дальнейшем развитии разработки и производства средств вычислительной техники» выполняются неудовлетворительно.

Министерства и ведомства не уделяют должного внимания вопросам совершенствования системы планирования и методов управления отраслями на основе применения экономико-математических методов и средств вычислительной техники.

Министерство радиопромышленности и Министерство приборостроения, средств автоматизации и систем управления со значительным отставанием от установленных сроков выполняют задания по разработке новых средств электронной вычислительной техники и развития производственных мощностей для их изготовления. Капитальные вложения для этих целей в объемах, предусмотренных постановлением Совета министров СССР от 30 декабря 1967 года № 1180-420, не выделяются.

В целях ускорения работ по совершенствованию управления в народном хозяйстве и применению для этих целей современных научных методов и технических средств Центральный комитет КПСС и Совет министров Союза ССР постановляют:

1. Считать важнейшей задачей министерств и ведомств совершенствование системы планирования и методов управления отраслями народного хозяйства на основе широкого внедрения современных средств электронной вычислительной техники и автоматизированных систем управления.

Обязать Госплан СССР, министерства и ведомства предусмотреть в плане развития народного хозяйства СССР на 1971—1975 годы создание в министерствах и ведомствах автоматизированных систем управления, сбора и обработки информации и ввод в действие не менее 1 600 автоматизированных систем управления предприятиями и организациями в промышленности, строительстве, сельском хозяйстве, связи, торговле и на транспорте.

2. Обязать министерства и ведомства разработать и утвердить в 1971 году планы работ до 1975 года по совершенствованию методов и структуры управления, развития автоматизированных систем управления, упорядочению нормативного хозяйства, повышению квалификации руководящих кадров в области управления производством и подготовке специалистов для внедрения и эксплуатации автоматизированных систем управления.

Установить, что министры и руководители ведомств несут персональную ответственность перед ЦК КПСС и Советом министров СССР за уровень и темпы работы в указанной области.

3. Признать необходимым создать Общегосударственную автоматизированную систему сбора и обработки информации для учета, планирования и управления в народном хозяйстве на базе Государственной сети вычислительных центров и Единой автоматизированной сети связи страны.

4. Возложить на Государственный комитет Совета министров СССР по науке и технике:

— разработку предложений по совершенствованию методов, структуры и процессов управления в народном хозяйстве с максимальным использованием вычислительной техники;

— координацию работ по созданию Общегосударственной автоматизированной системы сбора и обработки информации для учета, планирования и управления в народном хозяйстве и Государственной сети вычислительных центров;

— руководство работой по повышению квалификации руководящих работников народного хозяйства в области современных методов управления, организации производства и планирования с применением экономико-математических методов и вычислительной техники.

Для руководства этими работами считать необходимым иметь в Государственном комитете Совета министров СССР по науке и технике дополнительно должность первого заместителя Председателя.

Разрешить Государственному комитету Совета министров СССР по науке и технике:



— организовать на базе Отдела вычислительной техники и систем управления Главное управление вычислительной техники и систем управления;

— создать при Комитете научно-исследовательский институт по вопросам управления в народном хозяйстве.

5. Для разработки основных направлений по совершенствованию управления в народном хозяйстве на основе широкого использования средств вычислительной техники и автоматизированных систем управления, координации работ в этой области, а также для подготовки и внесения в ЦК КПСС и Совет министров СССР соответствующих предложений по этим вопросам признать необходимым создать Междуведомственный совет по вопросам совершенствования управления в народном хозяйстве в составе:

Председатель Государственного комитета Совета министров СССР по науке и технике (председатель Совета), министр приборостроения, средств автоматизации и систем управления, министр радиопромышленности, министр связи СССР, министр финансов СССР, председатель Государственного комитета Совета министров СССР по вопросам труда и заработной платы, председатель Государственного комитета цен Совета министров СССР, начальник Центрального статистического управления при Совете министров СССР, президент Академии наук СССР, первый заместитель председателя Госплана СССР, первый заместитель председателя Госстроя СССР, первый заместитель председателя Государственного комитета Совета министров СССР по науке и технике.

Установить, что решения Междуведомственного совета по вопросам совершенствования управления в народном хозяйстве на основе широкого использования средств вычислительной техники являются обязательными для всех министерств и ведомств СССР и союзных республик.

6. Поручить Государственному комитету Совета министров СССР по науке и технике в шестимесячный срок разработать с участием заинтересованных министерств и ведомств и утвердить техническое задание на создание Общегосударственной автоматизированной системы сбора и обработки информации для учета, планирования и управления в народном хозяйстве и Государственной сети вычислительных центров и совместно с Госпланом СССР, Министерством радиопромышленности, Министерством связи СССР, ЦСУ СССР и Академией наук СССР представить в 1971 году в Совет министров СССР предложения о порядке и сроках их создания.

7. Обязать Министерство приборостроения, средств автоматизации и систем управления:

— принять меры по ускорению разработки и подготовки производства средств вычислительной техники, предусмотренных постановлением Совета министров СССР от 30 декабря 1967 года № 1180-420, и о принятых мерах в январе 1971 года доложить Совету министров СССР;

- обеспечить в 1971—1972 годах разработку типовых методологических и технических решений по построению автоматизированных систем управления отраслями и предприятиями, а также разработку совместно с Академией наук СССР межотраслевых методических и инструктивных материалов по организации, проектированию, математическому обеспечению и вводу в действие автоматизированных систем управления;
- разработать и осуществить мероприятия по развитию существующих и созданию в необходимых случаях новых научно-исследовательских, проектных и конструкторских организаций по автоматизированным системам управления.

8. В целях ускорения и повышения уровня работ по созданию и внедрению в народное хозяйство автоматизированных систем управления принять предложение Министерства приборостроения, средств автоматизации и систем управления о возложении на объединение «Союзпромавтоматика» вопросов проектирования, комплектной поставки, монтажа, наладки и сдачи в эксплуатацию автоматизированных систем управления с необходимым математическим обеспечением, производства специальной аппаратуры и устройств для указанных систем, а также стендовой отладки в необходимых случаях автоматизированных систем управления технологическими процессами производства.

Разрешить Министерству приборостроения, средств автоматизации и систем управления организовать в г. Москве в составе указанного объединения специализированный трест по комплектной поставке заказчикам средств вычислительной и организационной техники, приборов и средств автоматизации, входящих в автоматизированные системы управления.

Госплану СССР, Госнабу СССР и ЦСУ СССР выделять с 1971 года Министерству приборостроения, средств автоматизации и систем управления по его заявкам фонды на вычислительные машины, приборы, средства автоматизации и другое оборудование целевым назначением для обеспечения комплектации и поставки заказчикам автоматизированных систем управления.

9. Обязать Министерство радиопромышленности и Министерство электронной промышленности принять меры по ускорению разработки и подготовки производства комплекса электронных вычислительных машин «Ряд», предусмотренных постановлением Совета министров СССР от 30 декабря 1967 года № 1180-420, и о принятых мерах доложить Совету министров СССР в январе 1971 года.

Министерству радиопромышленности и Академии наук СССР в двухмесячный срок разработать и утвердить планы совместных работ по созданию систем математического обеспечения комплекса электронных вычислительных машин «Ряд» и по развитию математического обеспечения серийно выпускаемых электронных вычислительных машин.



10. Обязать Министерство черной металлургии СССР, Министерство цветной металлургии СССР, Министерство химической промышленности, Министерство целлюлозно-бумажной промышленности и Министерство авиационной промышленности принять меры по ускорению разработки и освоения в серийном производстве комплектующих изделий и материалов для изготовления средств вычислительной техники, предусмотренных постановлением Совета министров СССР от 30 декабря 1967 года № 1180-420, и о принятых мерах доложить Совету министров СССР в январе 1971 года.

11. Обязать ЦСУ СССР совместно с Госпланом СССР и Комитетом стандартов, мер и измерительных приборов при Совете министров СССР принять меры по ускорению работ, предусмотренных постановлением ЦК КПСС и Совета министров СССР от 6 марта 1966 года № 187, в том числе по совершенствованию системы формирования, обработки и хранения нормативной информации, по сокращению и унификации форм документации, приспособлению их к обработке на вычислительных машинах.

ЦСУ СССР и Госплану СССР разработать совместно с министерствами и ведомствами и в 1970 году утвердить комплексный план работ по совершенствованию системы нормативной информации и унификации первичной документации, имея в виду проведение указанных работ в отраслях и ведомствах в 1971—1972 годах.

12. Обязать Госплан СССР:

- предусмотреть выделение в 1971—1975 годах капитальных вложений Министерству радиопромышленности, Министерству электронной промышленности и Министерству приборостроения средств автоматизации и систем управления целевым назначением для строительства и реконструкции предприятий и организаций по производству, разработке и внедрению в народное хозяйство вычислительной техники, предусмотренных постановлением Совета министров СССР от 30 декабря 1967 года № 1180-420, имея в виду обеспечить ввод их в действие в сроки, установленные указанным постановлением. Установить, что указанные капитальные вложения предусматриваются в годовых планах развития народного хозяйства СССР отдельной строкой;
- предусмотреть выделение в 1971—1975 годах Министерству связи СССР капитальных вложений целевым назначением на развитие сети связи и создание центров коммутации сообщений, как составной части Единой автоматизированной сети связи, необходимых для Общегосударственной автоматизированной системы сбора и обработки информации для учета, планирования и управления в народном хозяйстве на базе Государственной сети вычислительных центров и отраслевых и ведомственных автоматизированных систем управления.

13. Отметить, что Министерство строительства СССР, Министерство промышленного строительства СССР, Министерство

строительства предприятий тяжелой индустрии СССР, Министерство монтажных и специальных строительных работ СССР и Главмосстрой Мосгорисполкома недостаточными темпами ведут строительство и реконструкцию предприятий и организаций Министерства радиопромышленности, Министерства электронной промышленности, Министерства приборостроения, средств автоматизации и систем управления, предусмотренных постановлением Совета министров СССР от 30 декабря 1967 года № 1180-420.

Госплану СССР совместно с указанными министерствами в 1970 году рассмотреть план строительства и реконструкции этих объектов на 1971—1975 годы и предусматривать в годовых планах развития народного хозяйства СССР необходимые объемы подрядных работ и сроки ввода в действие строящихся предприятий и организация.

Возложить на руководителей указанных министерств и Главмосстроя Мосгорисполкома персональную ответственность за своевременное завершение строительства и реконструкцию предприятий и организаций, предусмотренных постановлением Совета министров СССР от 30 декабря 1967 года № 1180-420.

14. Обязать Министерство радиопромышленности, Министерство электронной промышленности, Министерство приборостроения, средств автоматизации и систем управления и Академию наук СССР во II квартале 1971 года разработать и утвердить комплексный план поисковых и научно-исследовательских работ, обеспечивающих своевременную подготовку научно-технического задела для создания в будущем пятилетия электронных вычислительных машин четвертого поколения, дальнейшее совершенствование автоматизации программирования и развитие информационно-вычислительных систем коллективного пользования.

15. Министерству радиопромышленности, Министерству электронной промышленности, Министерству приборостроения, средств автоматизации и систем управления и Министерству связи СССР с участием Госплана СССР, Государственного комитета Совета министров СССР по науке и технике и Министерства внешней торговли разработать и во II квартале 1971 года внести в Совет министров СССР предложения по закупке за рубежом лицензий, оборудования и аппаратуры, необходимых для ускорения создания и производства средств вычислительной техники и аппаратуры коммутации сообщений.

16. Распространить на работы по созданию средств вычислительной техники и автоматизированных систем управления для народного хозяйства, выполняемые Министерством радиопромышленности и Министерством приборостроения, средств автоматизации и систем управления, порядок премирования, установленный постановлением Совета министров СССР от 8 января 1960 года № 28-10.

Предоставить право Министерству радиопромышленности и Министерству приборостроения, средств автоматизации и систем управления устанавливать и выплачивать единовременные премии 6—13-й



степени, предусмотренные частью первой Положения, утвержденного постановлением Совета министров СССР от 8 января 1960 года № 28-10, за создание наиболее важных и сложных средств вычислительной техники и систем управления.

17. В целях расширения масштабов и ускорения работ по созданию и внедрению в народное хозяйство автоматизированных систем управления разрешить Министерству приборостроения, средств автоматизации и систем управления и Министерству радиопромышленности устанавливать объем выполняемых по договорам с заказчиками научно-исследовательских и проектных работ по автоматизированным системам управления, с соответствующим фондом заработной платы, сверх объемов этого вида работ, планируемых для указанных министерств.

Размер фонда заработной платы в процентах от объемов сверхплановых договорных работ по автоматизированным системам управления устанавливается по согласованию с Госпланом СССР.

18. Поручить Госплану СССР рассмотреть возможности организации в 1971 году производства отдельных прецизионных электро-механических вычислительных устройств и узлов для электронных вычислительных машин третьего поколения на заводах оборонных отраслей промышленности.

19. Министерству высшего и среднего специального образования СССР обеспечить в 1971—1975 годах в необходимых масштабах подготовку в высших и средних специальных учебных заведениях и выпуск по специальностям и в сроки по согласованию с Госпланом СССР специалистов по созданию и применению в народном хозяйстве вычислительной техники и автоматизированных систем управления, в том числе не менее 125 тыс. специалистов с высшим образованием, из них не менее 50 тыс. специалистов по математическому обеспечению электронно-вычислительных машин и автоматизированных систем управления.

20. Поручить Академии наук СССР и Министерству высшего и среднего специального образования СССР организовать в 1971 году при ведущих институтах соответствующего профиля и вычислительных центрах Академии наук СССР и при ряде университетов специальные курсы по подготовке высококвалифицированных программистов-математиков и экономистов-математиков для разработки математического обеспечения электронных вычислительных машин и автоматизированных систем управления.

21. Признать целесообразным созвать в 1971 году Всесоюзное совещание по применению вычислительной техники и автоматизированных систем управления на предприятиях и в отраслях промышленности для широкого обсуждения вопросов дальнейшего совершенствования управления в народном хозяйстве на этой основе.

Подготовку и проведение указанного совещания поручить Государственному комитету Совета министров СССР по науке и технике.

22. Поручить Государственному комитету Совета министров СССР по науке и технике ежегодно к 1 марта докладывать ЦК КПСС и Совету министров СССР о ходе работ по совершенствованию управления в народном хозяйстве на основе широкого использования средств вычислительной техники и автоматизированных систем управления.

\* \* \*

Центральный комитет КПСС и Совет министров СССР обращают внимание партийных, государственных и хозяйственных органов на то, что совершенствование управления в народном хозяйстве на современном этапе является не только технической, но и важнейшей политической задачей, успешное решение которой обеспечит ускорение создания материально-технической базы коммунизма.

ЦК компартий союзных республик, крайкомам и обкомам КПСС взять под особый контроль выполнение мероприятий, предусмотренных настоящим постановлением.

Секретарь  
Центрального комитета КПСС  
*Л. Брежнев*

Председатель  
Совета министров Союза ССР  
*А. Косыгин*

**Юрий Григорьевич ШПАКОВСКИЙ,**  
главный редактор  
журнала «Вестник  
Университета имени  
О.Е. Кутафина (МГЮА)»,  
доктор юридических наук,  
профессор

**П**ожалуй, ни в одной другой стране взаимоотношения государства и религии не были столь диаметрально противоположными, как в России, причем в относительно короткий временной промежуток.

В 1917 г. атеизм был провозглашен одной из главных составляющих советской идеологии, а православие стало считаться пережитком прошлого, рудиментом, мешающим двигаться к «коммунистическому раю», построенному прямо на земле.

Антирелигиозные задачи перед партией большевиков ставились задолго до взятия власти.

Так, одним из пунктов программы Российской социал-демократической рабочей партии, принятой на II съезде партии (17 (30) июля — 10 (23) августа 1903 г.) было «отделение церкви от государства и школы от церкви». Антирелигиозные идеи присутствовали в работах Карла Маркса. В статье «К критике гегелевской философии права. Введение», опубликованной в 1844 г., он писал: «Религия — это вздох угнетенной твари, сердце бессердечного мира, подобно тому как она — дух бездушных порядков. Религия есть опиум народа». Многократно цитировалось высказывание Фридриха Энгельса о том, что «религия есть акт самоопустошения человека».



Плакат 1920-х гг.

В первые годы существования Советского государства религиозная политика несколько раз меняла свое направление. Первоначально проявилось устойчивое желание покончить с Русской православной церковью как главенствующей на момент революции религиозной организацией в стране. Религиозная политика была последовательно направлена на искоренение религии как несовместимой с марксистской идеологией.

Интересно, что И. Сталин не понаслышке был знаком с религией и верой — он окончил семинарию. Однако революционные идеалы оказались ему дороже.

Важным моментом начала антирелигиозной кампании является принятие Декрета Совета народных комиссаров (23 января 1918 г.) «Об отделении церкви от государства и школы от церкви». Что было главное в этом декрете?

Во-первых, из всех официальных актов всякое указание на религиозную принадлежность и непринадлежность граждан устранилось.

Во-вторых, действия государственных и иных публично-правовых общественных установлений не должны были сопровождаться никакими религиозными обрядами или церемониями.

В-третьих, свободное исполнение религиозных обрядов обеспечивалось постольку, поскольку они не нарушали общественного порядка и не сопровождались посягательствами на права граждан Советской Республики.

В-четвертых, никто не мог, ссылаясь на свои религиозные воззрения, уклоняться от исполнения своих гражданских обязанностей.

В-пятых, школа отделялась от церкви. Преподавание религиозных вероучений во всех государственных и общественных, а также частных учебных заведениях, где преподавались общеобразовательные предметы, не допускалось.

В-шестых, все церковные и религиозные общества стали подчиняться общим положениям о частных обществах и союзах и не могли пользоваться никакими преимуществами и субсидиями ни от государства, ни от его местных автономных и самоуправляющихся установлений. Никакие церковные и религиозные общества не имели права владеть собственностью. Прав юридического лица они не имели. Все имущество существующих в России церковных и религиозных обществ объявлялось народным достоянием. Здания и предметы, предназначенные специально для богослужебных целей, отдавались по особым постановлениям местной или центральной государственной власти в бесплатное пользование соответствующих религиозных обществ.

Для проведения в жизнь антирелигиозной компания в русле реализации Декрета «Об отделении церкви от государства и школы от церкви» был создан ликвидационный отдел Народного комиссариата юстиции (НКЮ) РСФСР во главе с Петром Красиковым.

Новая власть вела активную борьбу с религиозными учреждениями, прежде всего с принадлежащими Русской православной церкви, которая рассматривалась как крупнейший рассадник соперничающей идеологии и оплот царизма. Жителям молодого социалистического государства активно прививали новую «красную религию», и конкуренты власти были ни к чему.

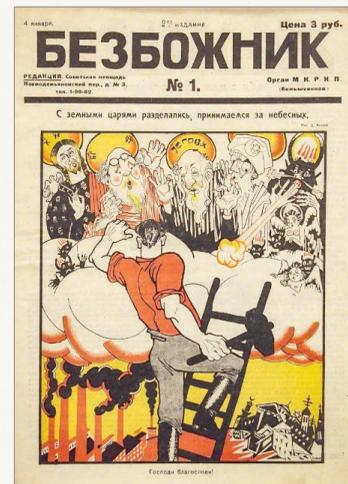
Для борьбы с религией в СССР с 1922 г. стали издавать журнал «Безбожник», в большом количестве выпускались антирелигиозные плакаты. Были закрыты все духовные учебные заведения, прекращено издание религиозной литературы.

Официально атеизм в СССР провозглашен не был, но правящая партия поддерживала данную идеологию и всячески поощряла. По всей стране звучали лозунги «Религия — опиум для народа».

За окрашивание яиц перед Пасхой или участие в пасхальном крестном ходе выгоняли с работы или исключали из колхоза. Вскоре даже дети прекрасно знали: о том, что дома пекли куличи, никому говорить нельзя. Некоторые перед Пасхой даже боялись держать дома яйца.



Плакат 1930-х гг.



Выпуск журнала «Безбожник»



Имена посещавших пасхальную службу писали для всеобщего обозрения



Конфискация церковного имущества



Плакат 1930-х гг.

В пасхальную неделю и иные большие религиозные праздники проводились массовые мероприятия с обязательным присутствием: ленинские субботники, спортивные соревнования, эстафеты. Были и массовые шествия с антирелигиозными символами, которые потом предавали огню.

16 февраля 1919 г. коллегия Наркомата юстиции приняла постановление об организации вскрытия мощей святых на территории России, был определен «порядок их инспекции и конфискации государственными органами». Вскрытие мощей (снятие с них покровов и облачений) должны были осуществлять священнослужители в присутствии представителей местных органов советской власти, ВЧК и медицинских экспертов.

Кампания по вскрытию мощей носила пропагандистский характер и началась осенью 1918 г. со вскрытия в Олонецкой губернии мощей св. Александра Свирского (жившего в XV—XVI вв.). Пик кампании пришелся на 1919—1920 гг., хотя отдельные эпизоды имели место и в 1930-е гг.

Практика «безбожной пятилетки» началась в 1928 г. В основе этого плана лежала относительно простая идея. Традиционное национальное сознание нужно было искоренить, чтобы строить общество, основанное на универсальных принципах социализма. Эти принципы были впоследствии использованы другими коммунистическими странами.

В 1925 г. в стране появился Союз безбожников. Его программа выглядела следующим образом: «Союз безбожников есть добровольная пролетарская общественная организация, ставящая своей задачей объединение широких масс трудящихся СССР для активной систематической и последовательной борьбы с религией во всех ее видах и формах как тормозом социалистического строительства и культурной революции». Воинствующими же безбожники стали только в 1929 г. Долгие годы Союз воинствующих безбожников возглавлял Емельян Ярославский (урожденный Миней Израилевич Губельман)<sup>2</sup>.

В состав Союза воинствующих безбожников входили члены партии, члены комсомольского молодежного

<sup>2</sup> Революционер, советский партийный и государственный деятель, идеолог и руководитель антирелигиозной политики в СССР. Председатель Союза воинствующих безбожников и Антирелигиозной комиссии при ЦК РКП — ЦК ВКП(б), академик АН СССР, лауреат Сталинской премии первой степени, член Центрального комитета ВКП(б).

движения, лица без определенной политической принадлежности, рабочие и ветераны боевых действий.

Руководствуясь принципами коммунистической пропаганды и указаниями партии в отношении религии, Союз стремился искоренить религию во всех ее проявлениях и сформировать у рабочих антирелигиозное научное мышление. Он пропагандировал атеизм и научные достижения, вел так называемую «индивидуальную работу» (метод направления наставников-атеистов на встречи с отдельными верующими с целью заставить их отречься от своей веры). Лозунг Союза был «Борьба с религией — это борьба за социализм», он должен был связать атеистические взгляды с коммунистическим стремлением «построить социализм».

Все комсомольцы были обязаны вступать в Союз, всем членам партии предписывалось поддерживать его работу. В 1932 г. Союз получил от Сталина указание принять антирелигиозный пятилетний план с целью ликвидации Церкви и ее влияния в СССР. Отношения между Советским государством и РПЦ достигли той критической точки, за пределами которой само понятие «отношения» лишилось содержания — Русская православная церковь в СССР как социальный институт стояла на пороге полного уничтожения.

Однако после 1939 г. отношение государства к РПЦ стало меняться, а деятельность Союза постепенно сворачиваться. Формально организация существовала, но фактически ее деятельность уже не была заметна. Важно, что с присоединением западных земель к СССР там уже не проводилась антирелигиозная пропаганда.

После начала Великой Отечественной войны Союз воинствующих безбожников, не будучи официально распущенным, свою деятельность прекратил<sup>3</sup>. В июле 1941 г. вышел последний номер журнала «Безбожник». Более того, Ярославский в первые месяцы войны написал статью «Почему религиозные люди против Гитлера», тональность которой кардинально отличалась от всех его антирелигиозных статей, написанных ранее.

Историки до сих пор спорят о том, что стало причиной столь кардинальной смены отношения советской власти к Русской православной церкви. Вне всякого сомнения, Церковь после начала Великой Отечественной войны проявила себя как сила, способная консолидировать общество и подвигнуть его на жертвенность в деле борьбы с фашизмом, — но одного этого было бы недостаточно.

В первые же месяцы войны выявились неправильность и пагубность сформировавшейся государственной политики в отношении религии и церкви. Иллюзии об успешном и повсеместном «преодолении» религии и о победе «безбожного» движения рассеялись, уступив место правде жизни — в стране насчитывались миллионы верующих, которые были несправедливо ограничены в правах. Существенным потенциалом влияния на эту категорию граждан могли быть действовавшие в стране религиозные организации и духовенство различных конфессий.

В начале 1943 г. И. Сталин пришел к окончательному решению о необходимости приступить к нормализации государственно-церковных отношений. На это



Емельян Ярославский

<sup>3</sup> В 1947 г. Союз был официально распущен, а его деятельность передана Всесоюзному обществу по распространению политических и научных знаний (общество «Знание»).

повлияли как внутренние, так и внешнеполитические факторы. Одной из причин была активная патриотическая деятельность подавляющего большинства духовенства и мирян. За полтора года войны, несмотря на отсутствие необходимого аппарата управления, печатного органа и юридического статуса, церковь показала свою силу в борьбе против фашизма, сумела во многом расширить и упрочить влияние в стране. Определенное значение имело обращение в ходе войны к русским национальным традициям. В процессе завершения перехода от интернационального к национально-патриотическому курсу церкви отводилась роль катализатора и цементирующего компонента.

5 января 1943 г. митрополит Сергей (патриарший местоблюститель) предпринял важный шаг на пути к фактической легализации Русской православной церкви, сославшись на сбор средств для обороны страны, который активно велся РПЦ с первых дней войны. Он послал И. Сталину телеграмму, прося его разрешения на открытие патриархией банковского счета, куда вносились бы деньги, пожертвованные в храмах на нужды войны. Председатель СНК дал свое письменное согласие и от лица Красной армии поблагодарил РПЦ за ее труды. Получив разрешение открыть банковский счет, патриархия приобрела урезанный статус юридического лица.

В июне 1943 г. постановление Государственного комитета обороны «Об утверждении мероприятий по улучшению зарубежной работы разведывательных органов СССР» впервые отнесло религиозные организации за рубежом к категории интересов советской внешней разведки. Необходимо это было сделать в преддверии освобождения советской территории и развития внешнеполитических связей с союзниками и другими странами.

Считается, что аргументом в пользу изменения отношений государства и церкви могло стать и внешнеполитическое давление: накануне Тегеранской конференции И. Сталину требовалось сделать все, чтобы заручиться поддержкой союзников и иметь возможность выдвинуть им свои требования, а на Западе почти напрямую увязывали помощь СССР с решением вопроса о свободе совести в Советском Союзе.

Возможно, сыграло роль и то обстоятельство, что во время оккупации на захваченной территории было открыто множество православных приходов, которые теперь, когда началось освобождение этих земель, невозможно было просто

взять и снова закрыть, но при этом необходимо было легализовать их и удержать под контролем.

В ночь с 4 на 5 сентября 1943 г. три митрополита Русской православной церкви были вызваны в Кремль к Иосифу Сталину. Встреча началась с того, что Сталин одобрил патриотическую деятельность митрополитов и поинтересовался, какие нужды испытывает Церковь. Затем затронули целый ряд практических вопросов.

Первым из них было восстановление нормально функционирующего высшего церковного управления и избрание патриарха. Исторический титул московских патриархов, вплоть до патриарха Тихона включительно, звучал как «патриарх Московский и всея России»



Архиерейский собор РПЦ 8 сентября 1943 г.

(некогда к этому прибавлялось еще и «всех Северных стран»). Словосочетание «всёя России», видимо, не очень нравилось Сталину, и иерархи предложили изменить титул на «патриарх Московский и всея Руси».

Сталин потребовал, чтобы вопрос о дате выборов патриарха решили «большевистскими темпами», т.е. созвали собор буквально за три дня. И действительно, задача была решена — с привлечением спецсредств и военной авиации. В ночь на 5 сентября состоялась встреча, а уже 8 сентября открылся Собор. На нем было всего 19 архиереев — все, кто мог быть привлечен на Собор в тот момент. Из мест заключения непосредственно перед Собором был освобожден лишь один из девятнадцати епископов. Итогом Собора стало избрание патриархом митрополита Сергия (Страгородского). Так же быстро Собор решил и вопрос избрания Синода при патриархе.

Важно подчеркнуть, что с началом Великой Отечественной войны религиозное пробуждение коснулось всей Советской армии — от рядовых до генералов. Одним из православных руководителей нашей Армии был маршал Борис Михайлович Шапошников. очевидцы свидетельствовали, что маршал Шапошников носил финифтевый образ Николая Чудотворца.

Конечно, помощь РПЦ имела огромное значение для поднятия боевого духа Армии. Не случайно многие удивительные события, чудеса и явления связывали с божественным проявлением.

Некоторые из этих чудес передавались устно, обрастая все новыми подробностями и в конечном счете превращаясь в благочестивые легенды.

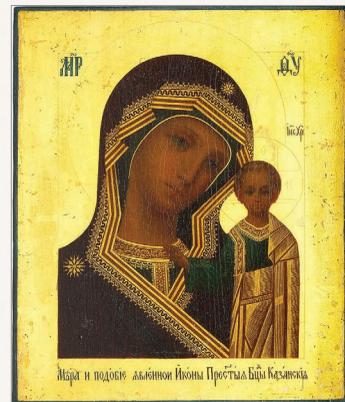
Пожалуй, самой известной является история о воздушном крестном ходе над Москвой, который остановил наступление немецкой армии.

Говорят, что по приказу Сталина над городом поднялся самолет, на борту которого находилась Казанская икона Богородицы. Хотя иногда упоминаются и другие образы Богородицы. Одни говорят про чудотворный список с Тихвинской иконы Божией Матери, хранившийся в храме села Алексеевское, другие — про аналогичную икону, но уже из самого Тихвина или из Ленинграда. Есть и еще один вариант, по которому Тихвинская икона участвовала в воздушном крестном ходе, а Казанский образ был пронесен по оборонительным позициям.

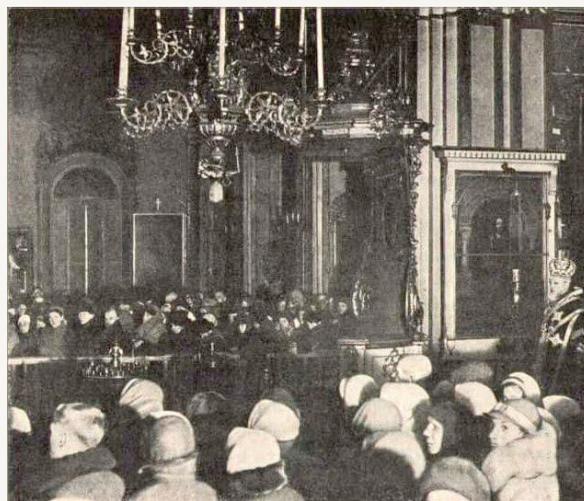
Однако ни свидетельств летчика, который совершал или мог бы совершить такой полет, ни воспоминаний священников, проводивших подобный молебен, не сохранилось. Духовенство официально не подтверждает версию о прошедшем крестном ходе, но и не опровергает ее категорически.

Но нужно заметить, что по чудесному совпадению на следующий день после предполагаемого воздушного крестного хода резко похолодало и пошел сильный снег, отчего упала видимость, и это дало возможность Красной армии перегруппироваться и начать контрнаступление.

Вторая часто рассказываемая история связана с блокадой Ленинграда.



Казанская икона Божьей Матери



Служба в Никольском соборе блокадного Ленинграда

Митрополиту Антиохийскому Илие (Караму) в Ливане было явление Богородицы, в котором она объявила: «По всей России должны быть открыты храмы, монастыри и духовные академии. Священников нужно возвратить с фронтов, выпустить из тюрем. Сейчас готовятся сдать Ленинград — делать этого нельзя. Пусть вынесут чудотворную Казанскую икону Божией Матери и обнесут ее крестным ходом вокруг города. Потом она должна оказаться в Сталинграде, который тоже нельзя отдавать врагу. Если все это не будет исполнено, Россия погибнет». После этого, как гласит легенда, по каналам Красного Креста Илия связался с Советским правительством и передал слова Пречистой. В это время вокруг Ленинграда уже сомкнулось кольцо блокады. Рассказывают, что Сталин вызвал к себе митрополита Ленинградского Алексия и поручил исполнить то, что передал Илия.

Из Владимирского собора вынесли Казанскую икону Божией Матери и обошли с нею крестным ходом вокруг Ленинграда. Документальных подтверждений этого до сих пор не найдено.

Однако фактом является то, что действительно в десяти храмах города начались регулярные богослужения, в церквях проходили таинства причастия, хотя для этого требовались красное вино и мука. Малоизвестным фактом является то, что власти блокадного Ленинграда согласились выдавать священникам минимальное количество вина и муки для совершения таинства причастия. В октябре 1943 г. впервые за все годы советской власти 12 ленинградским священникам, в том числе и митрополиту Алексию, были вручены правительственные награды.

Победа под Сталинградом, где враг потерял убитыми, ранеными и пленными до полутора миллионов человек, стала коренным переломом во Второй мировой войне. Примечательно, что среди руин Сталинграда уцелело здание церкви в честь Казанской иконы Божией Матери.

Есть также неподтвержденный факт о приезде к блаженной Матроне в октябре 1941 г. И. В. Сталина. Блаженная сказала ему: «Красный петух победит. Победа будет за тобой. Из начальства один ты не выедешь из Москвы». Возможно, что это просто красивая легенда. Причины, почему Сталин не покинул Москву вслед за правительством в октябре 1941 г., историки называют несколько. Вероятнее всего, И. Сталин понял, что вопрос о его пребывании в Москве — это вопрос о жизни и смерти самого возглавляемого им государства.

После войны и в начале 1950-х гг. антицерковный гнет ослаб, но затем опять наступило «охлаждение отношений». Это может быть связано с тем, что после победы в войне начался мощный экономический рост Советской страны. Уровень жизни населения из года в год повышался, была уверенность, что завтрашний день будет еще лучше, т.е. людям опять можно было говорить о перспективах построения «рая» на земле.

При этом с приходом к власти Н. Хрущева вновь стала набирать обороты антицерковная кампания. В 1954 г. было принято постановление ЦК КПСС «О крупных недостатках в научно-атеистической пропаганде и мерах ее улучшения».

На фоне технических достижений СССР в области науки и космонавтики в 1960-х гг. религия стала отождествляться с дремучестью. Самым популярным аргументом того периода было: «наши космонавты поднялись в космос максимально высоко, а Бога так и не увидели!»

Опять началось закрытие храмов. Чтобы крестить ребенка, родителям приходилось ехать в отдаленную деревню, подальше от города. Ношение религиозных символов в школе и на работе стало недопустимым.

После прихода в 1964 г. к власти Л. Брежнева и до самой перестройки борьба с религией носила в целом формальный характер. Так, чтобы удержать молодежь от похода в церковь в пасхальную ночь, ближе к полуночи в кинотеатрах страны обязательно демонстрировали интересные западные фильмы, а по телевидению пускали передачи типа «Мелодии и ритмы зарубежной эстрады».

Пропаганда же велась в основном в школе, где рассказывали о вреде религии, и уже не столь активно и настойчиво. Все шло как бы по инерции.

Поворотным событием стало торжественное празднование в стране в 1988 г. тысячелетия крещения Руси, отметить которое «как крупнейшее событие в европейской и мировой истории и культуре» призвала в ноябре 1987 г. XXIV сессия Генеральной ассамблеи ЮНЕСКО.

Генеральный секретарь ЦК КПСС М. С. Горбачев встретился в Кремле с патриархом Пименом и Священным Синодом. При этом Генсек сказал: «Мы ясно видим всю глубину наших мировоззренческих различий, но вместе с тем реалистически учитываем существующую ситуацию. Верующие — это советские люди, трудящиеся, патриоты, и они имеют полное право достойно выражать свои убеждения».

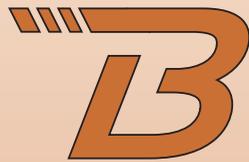
В 1990 г. был принят Закон РСФСР «О свободе вероисповеданий».



Антирелигиозные плакаты 1960-х гг.



М. С. Горбачев и патриарх Пимен



ISSN 2311-5998



9 772311 599771 >