

**ИНСТИТУТ НАУЧНОЙ ИНФОРМАЦИИ ПО ОБЩЕСТВЕННЫМ НАУКАМ
РОССИЙСКОЙ АКАДЕМИИ НАУК
(ИНИОН РАН)**

**СОЦИАЛЬНЫЕ
И
ГУМАНИТАРНЫЕ НАУКИ**

**ОТЕЧЕСТВЕННАЯ И ЗАРУБЕЖНАЯ
ЛИТЕРАТУРА**

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЖУРНАЛ

СЕРИЯ 4

**ГОСУДАРСТВО
И
ПРАВО
2026 – 1**

Издается с 1974 года
Выходит 4 раза в год
Индекс серии 2.4

Учредитель
Институт научной информации по общественным наукам
Российской академии наук

Редакционная коллегия серии «Государство и право»:

Умнова-Конюхова И.А. – гл. ред., д-р юрид. наук, профессор (ИНИОН РАН);
Алферова Е.В. – зам. гл. ред., канд. юрид. наук (ИНИОН РАН); *Алешкова И.А.* –
канд. юрид. наук, доцент (ИНИОН РАН); *Андриченко Л.В.* – д-р юрид. наук,
профессор (ИЗиСП при Правительстве РФ); *Бурдина Е.В.* – д-р юрид. наук, до-
цент (Рос. гос. ун-т правосудия (РГУП)); *Вакула М.А.* – канд. юрид. наук, про-
фессор (Юрид. ин-т РУДН); *Васильева Т.А.* – д-р юрид. наук (ИГП РАН); *Гло-
тов С.А.* – д-р юрид. наук, профессор (ИНИОН РАН); *Грудцына Л.Ю.* – д-р
юрид. наук, профессор (Ин-т управления образованием Российской акад. образо-
вания); *Егорова М.А.* – д-р юрид. наук, профессор (Моск. гос. ун-т им. О.Е. Кута-
фина (МГЮА)); *Ефременко Д.В.* – д-р полит. наук (НИУ ВШЭ; ИНИОН РАН);
Исаков В.Б. – д-р юрид. наук, профессор (НИУ ВШЭ); *Карицхия А.А.* – д-р юрид.
наук, профессор (Рос. гос. ун-т нефти и газа (НИУ) им. И.М. Губкина); *Кодане-
ва С.И.* – канд. юрид. наук, доцент (ИНИОН РАН); *Кравец И.А.* – д-р юрид. наук,
профессор (Ин-т философии и права, юрид. ф-т Новосиб. гос. ун-та); *Краси-
ков Д.В.* – канд. юрид. наук, доцент (Сарат. гос. юрид. акад.); *Крысанова Н.В.* –
канд. юрид. наук (ИНИОН РАН); *Лапаева В.В.* – д-р юрид. наук (ИГП РАН);
Лужина А.Н. – канд. юрид. наук, доцент (РГУП); *Манова Н.С.* – д-р юрид. наук,
профессор (Сарат. гос. юрид. акад.); *Пудовочкин Ю.Е.* – д-р юрид. наук, профес-
сор (Моск. гос. юрид. ун-т им. О.Е. Кутафина (МГЮА)); *Сафина С.Б.* – д-р
юрид. наук, доцент (Башкирская акад. гос. службы); *Синцов Г.В.* – д-р юрид.
наук, профессор (Пензенский гос. ун-т); *Толстых В.Л.* – д-р юрид. наук, профес-
сор (Моск. гос. юрид. ун-т им. О.Е. Кутафина (МГЮА)); *Ястребова А.Ю.* – д-р
юрид. наук, доцент (Дипломат. акад. МИД России).

Включен в ЕГПНИ и Российский индекс
научного цитирования (РИНЦ)

DOI: 10.31249/iajpravo/2026.01.00

ISSN 2219-861X

Регистрационное свидетельство ПИ № ФС 77-80872 от 21.04.2021

© ИНИОН РАН, 2026

СОДЕРЖАНИЕ

ТЕМА НОМЕРА ПРАВО БЕЗОПАСНОСТИ: НАУЧНЫЕ ПОДХОДЫ И ЗАКОНОДАТЕЛЬНОЕ РЕГУЛИРОВАНИЕ

<i>Умнова-Конюхова И.А.</i> Право безопасности: актуальные аспекты природы, правовые основы и особенности российской модели (Статья)	7
<i>Третьякова Е.С.</i> Право биобезопасности: теоретико-правовое обоснование и место в системе российского права (Статья)	25
<i>Алешкова И.А.</i> Принципы биобанкинга в системе биоправа: научные подходы и перспективы развития (Обзорная статья)	40
<i>Алферова Е.В.</i> Безопасность человека в условиях вирусных пандемий: международно-правовые аспекты (Обзор)	58
<i>Карицкая А.А.</i> Энергобезопасность как фактор национальной безопасности (Статья)	76
<i>Коданева С.И.</i> Правовое регулирование и институциональные основы информационной безопасности в России и в зарубежных странах (Статья)	90
<i>Скурко Е.В.</i> Безопасность, кибербезопасность применения искусственного интеллекта: правовые аспекты (Обзор)	109
<i>Алферов О.Л., Алферова Е.В.</i> Интеграция надежных механизмов правовой защиты в систему управления искусственным интеллектом (Обзор)	125
<i>Маджумаев М.М.</i> Уголовно-правовое обеспечение безопасности государственного суверенитета в трансграничных метавселенных (Статья)	142
<i>Крысанова Н.В.</i> Киберстрахование в условиях расширения киберугроз (Обзор)	158
<i>Захаров Т.В.</i> К вопросу о системе международной безопасности на основе Устава ООН (Обзор)	172

<i>Глотов С.А.</i> «Цифровой Китай»: Обзор законодательных актов КНР, регулирующих вопросы кибербезопасности и защиты персональных данных	182
<i>Гроголь А.Г.</i> Правовое регулирование использования технологий искусственного интеллекта в медицине: вопросы обеспечения функционирования надежного искусственного интеллекта и безопасности медицинских данных в Европейском союзе (Обзор)	199
<i>Скурко Е.В.</i> Рецензия на книгу: Законодательство о бедствиях: подходы к управлению и имплементация / ред. Янь Цуй и Раджиб Шоу	213

CONTENTS

ISSUE THEME SECURITY LAW: SCIENTIFIC APPROACHES AND LEGISLATIVE REGULATION

<i>Umnova-Koniukhova I.A.</i> Security law: current aspects of nature, legal foundations and features of the Russian model (Article)	7
<i>Tretyakova E.S.</i> Biosecurity law: theoretical and legal justification and place in the system of Russian law (Article)	25
<i>Aleshkova I.A.</i> Principles of biobanking in the biolaw system: scientific approaches and development prospects (Review article)	40
<i>Alferova E.V.</i> Human security in the context of viral pandemics: international legal aspects (Review)	58
<i>Kartskhiya A.A.</i> Energy security as a factor of national security (Article)	76
<i>Kodaneva S.I.</i> Legal regulation and institutional framework of information security in Russia and abroad (Article)	90
<i>Skurko E.V.</i> Security, cybersecurity of artificial intelligence applications: legal aspects (Review)	109
<i>Alferov O.L., Alferova E.V.</i> Integration of reliable legal protection mechanisms into the artificial intelligence management system (Review)	125
<i>Madzhumayev M.M.</i> Criminal legal maintenance of state sovereignty in cross-border metaverse (Article)	142
<i>Krysanova N.V.</i> Cyberinsurance in the context of expanding cyber threats (Review)	158
<i>Zakharov T.V.</i> On the issue of the international security system based on the UN charter (Review)	172
<i>Glotov S.A.</i> «Digital China»: Review of legislative acts of the people's republic of china regulating cybersecurity and personal data protection	182

Grogol A.G. Legal regulation of the use of AI technologies in medicine: issues of ensuring the functional of reliable AI and security of medical data based on EU countries (Review)199

Skurko E.V. Book review: Disaster Law: implications to governance and implementation / ed. Yan Cui, Rajib Shaw213

ТЕМА НОМЕРА ПРАВО БЕЗОПАСНОСТИ: НАУЧНЫЕ ПОДХОДЫ И ЗАКОНОДАТЕЛЬНОЕ РЕГУЛИРОВАНИЕ

УДК 349; 34.09

DOI: 10.31249/iajpravo/2026.01.01

УМНОВА-КОНЮХОВА И.А.¹ ПРАВО БЕЗОПАСНОСТИ: АКТУАЛЬНЫЕ АСПЕКТЫ ПРИРОДЫ, ПРАВОВЫЕ ОСНОВЫ И ОСОБЕННОСТИ РОССИЙСКОЙ МОДЕЛИ

Аннотация. В статье поднимаются актуальные аспекты формирования и развития права безопасности, обосновывается его природа как мегаотрасли права, раскрываются основные признаки. Рассматриваются научные взгляды на безопасность как на юридически защищаемую ценность, эволюция правопонимания и практика регулирования как правовой категории; раскрываются вопросы межотраслевой и институциональной дифференциации безопасности; исследуются доктрина и правовое регулирование права на безопасность; дается оценка международно-правовых основ и конституционных основ права безопасности. Отдельное внимание уделяется оценке российской национальной модели права безопасности и перспективам ее совершенствования.

Ключевые слова: право безопасности; мегаотрасль права; виды безопасности; национальная безопасность; право на безопасность личности; международно-правовые основы безопасности; конституционные основы безопасности; законодательство Российской Федерации о безопасности.

UMNOVA-KONIUKHOVA I.A. Security law: current aspects of nature, legal foundations, and features of the Russian model

¹ Умнова-Конюхова Ирина Анатольевна, главный научный сотрудник отдела правоповедения ИНИОН РАН, доктор юридических наук, профессор.

Abstract. The article raises topical aspects of the formation and development of security law, substantiates its nature as a mega-branch of law, and reveals its main features. The scientific views on security as a legally protected value, the evolution of legal understanding and regulatory practice as a legal category are considered; the issues of intersectoral and institutional differentiation of security are revealed; the doctrine and legal regulation of the right to security are investigated; the assessment of international legal foundations and constitutional foundations of security law is given. Special attention is paid to the assessment of the Russian national model of security law and the prospects for its improvement.

Keywords: security law; mega-branch of law; types of security; national security; the right to personal security; international legal foundations of security; constitutional foundations of security; security legislation of the Russian Federation.

Для цитирования: Умнова-Конюхова И.А. (Статья) Право безопасности: актуальные аспекты природы, правовые основы и особенности российской модели // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2026. – № 1. – С. 7–24. – DOI: 10.31249/iajpravo/2026.01.01

Введение

В конце XX – начале XXI столетия в системе современного права стремительное развитие получило право безопасности. Это происходило на фоне роста факторов и рисков, влияющих на стабильное существование мирового сообщества, государств и отдельно взятого человека, в условиях глобализации вызовов человечеству со стороны международного терроризма и ядерных угроз, гонки вооружений и гибридизации войн, усиления экологической деградации, возникновения пандемий нового типа и т.д. Научно-технологическое развитие в XXI столетии и вхождение человечества в эпоху «НБИКС-революции»¹ породило новые угрозы (киберпреступность, кибертерроризм, цифровое вторжение в личную жизнь, биологические и генетические риски и пр.), что стало импульсом для расширения сфер и задач правового регулирования, обеспечивающих безопасность жизнедеятельности и определяя-

¹ НБИКС – гипотетическое ядро 6-го технологического уклада (включающее нано-, био-, инфо-, когнитивные и социогуманитарные технологии), синергия которых якобы обеспечит всеобщее глобальное процветание и счастье.

щих механизмы противодействия разным видам опасностей в глобальном, национальном, социогрупповом и индивидуальном измерениях.

Анализ структурно-функциональных свойств права безопасности позволяет утверждать, что этот феномен проявляет себя как новая комплексная мегаотрасль права, разветвляющаяся в национальном и международном праве в виде различных отраслей (например право международной безопасности в международном праве) и институтов права (экономическая, экологическая, ядерная, антитеррористическая, энергетическая, транспортная, продуктовая, промышленная, медицинская безопасность, биобезопасность и т.п.).

Развитие права безопасности внесло изменения в аксиологические и стратегические приоритеты правового регулирования, породило вопросы соотношения свободы и безопасности при установлении пределов ограничения прав и свобод, поставило задачи формирования координационных механизмов устранения правовых коллизий и конфликтов в публичных и частных интересах в целях защиты человека и человечества от существующих и возникающих угроз и вызовов.

Экзистенциальные аспекты свободы и безопасности вышли, как известно, на новый уровень задач правового регулирования в начале XXI столетия после террористических актов 11 сентября 2001 г. в Нью-Йорке и Вашингтоне, повлекших многочисленные жертвы. Эти события поставили не только перед США, но и другими государствами и мировым сообществом в целом новую задачу принятия международных правовых актов, законов и подзаконных актов государств, мобилизующих на эффективное противодействие глобальным вызовам и угрозам. «Патриотический Акт» США 2001 г. (USA Patriot Act) и аналогичные законы в других государствах, включая Российскую Федерацию¹, продемонстрировали смену приоритетов в сторону публичных интересов: не только личная, но и государственная и общественная безопасность определены основой для ограничения прав и свобод человека. Возникшие затем институты безопасности в самых различных отраслях права показали сквозное влияние права безопасности на всю систему права и ее устойчивое место в новой парадигме правового

¹ Феоктистов А.В., Зернов И.В. Эволюция развития законодательства о национальной безопасности в Российской Федерации // Электронный научный журнал «Наука. Общество. Государство». – 2023. – Т. 11. – № 1. – С. 68–76.

развития. В настоящее время и на международном, и на национальном уровнях право безопасности развивается межотраслевым путем, объединяя нормы большинства отраслей публичного и частного права.

В новейших исследованиях в контексте доктрин гибридных войн и вооруженных конфликтов содержание права международной безопасности постепенно расширяется, подразумевая защиту от таких опасностей, как киберпреступность, кибертерроризм, биоугрозы, экономические и информационные войны. При этом развивается теория управления рисками и конфликтами, все большее внимание привлекает потенциал использования методов арбитража, примирения, медиации, заключения сделок и переговоров, совершенствования стратегий предотвращения эскалации конфликтов, миростроительства и поддержания мира, правосудия переходного периода и т.д.¹

Современные исследования по праву безопасности охватывают общие, публичные и частные вопросы. В них разграничиваются понятия публичной и частной безопасности и рассматриваются самые разнообразные правовые инструменты защиты на примере опыта различных стран и взаимодействия между ними².

Сам по себе термин «право безопасности» практически не используется в действующем праве, предметом регулирования выступают различные виды безопасности, которые формулируются как право национальной безопасности, право экономической безопасности, право информационной безопасности и т.п. Данные правовые образования регулируются нормами различных отраслей права либо одной из них.

Так, институт экологической безопасности формируется в системе одной отрасли – экологического права, в то время как право экономической безопасности регулируется одновременно нормами конституционного, административного, финансового, гражданского и других отраслей права.

Интеграция и одновременно дифференциация принципов и норм права безопасности как мегаотрасли права обеспечивается интенсивным развитием международного права и национальных

¹ Threats to Peace and International Security: Asia versus West Current Challenges in a New Geopolitical Situation / ed. Juan Cayón Peña. – Springer, 2023. – P. 3–5.

² Handbook on Public and Private Security / ed. Erwin A. Blackstone, Simon Hakim, Brian Meehan. – Springer, 2023. – 412 p.

правовых систем в направлении создания правовых механизмов защиты и противодействия. С учетом складывающихся правовых реалий научное и практическое значение имеет конструирование идентифицирующих признаков права безопасности как правового образования надотраслевого типа. На данном этапе представляется целесообразным выделить следующие основные признаки права безопасности как мегаотрасли права:

- формализация безопасности как правовой категории и объекта правового регулирования, ее межотраслевая и институциональная дифференциация;
- регулирование права на безопасность как межотраслевого правового института;
- формирование международно-правовых основ, конституционных и законодательных основ права безопасности;
- проявление общего и идентичного в национальных моделях права безопасности.

Безопасность как правовая категория: эволюция правопонимания и ее виды

В отечественной юридической литературе «безопасность» как самостоятельная категория и объект правового регулирования стала активно исследоваться в 1990-х и первом десятилетии 2000-х годов. Российские ученые, не меняя сущности словарно-справочных определений, вносят в определение безопасности лишь дополнительные функциональные признаки. При этом некоторые правоведы различают безопасность в узком и широком смыслах.

Безопасность в широком значении определяется как обеспечение гражданам необходимых условий для цивилизованной жизни, развития и самовыражения¹. В узком смысле безопасность рассматривается в контексте наличия или отсутствия определенных угроз и рисков².

¹ Чернявский Г.С. К вопросу исследования проблем безопасности России // Военная мысль. – 1994. – № 29. – С. 29.

² Серебрянников В., Хлопьев А. Социальная безопасность России / под общ. ред. В.Н. Иванова, Р.Г. Яновского. – 1996. – С. 16. Казаков П.Д. Безопасность синэнергетики (опыт философского осмысления) // Безопасность. – 1994. – № 4. – С. 62–63. Комин И.С. Безопасность и риск в сфере внешнеэкономической деятельности (социально-философский анализ): автореферат дисс. ... канд. фило-соф. наук. – Тверь, 2005. – С. 12.

До начала XX в. понятие «безопасность» исследовалось преимущественно в контексте государственного суверенитета: самостоятельности внешней политики и невмешательства во внутренние дела. В XX в. проявляется научный и практический интерес к определению безопасных условий жизни отдельно взятого индивида (личности). В конце XX – начале XXI в. на фоне глобализирующихся угроз и вызовов человеческой цивилизации ставятся фундаментальные задачи комплексного определения безопасных условий жизни индивида (личности), общества, государства и нации (народа). Безопасность воспринимается как весьма широкая по смыслу категория, охватывающая разные сферы и различных субъектов права.

В Российской Федерации это выразилось в принятии Закона РФ от 05.03.1992 № 2446-1 «О безопасности» (утратил силу), в котором было дано определение безопасности как состояния защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Жизненно важные интересы детерминировались как совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Концепция национальной безопасности Российской Федерации, утвержденная Указом Президента РФ от 17.12.1997 № 1300, (утратила силу) содержала понятие национальной безопасности как безопасности ее многонационального народа – носителя суверенитета и единственного источника власти в Российской Федерации, однако затем в п. 6 Стратегии национальной безопасности Российской Федерации до 2020 г., утвержденной Указом Президента РФ от 12.05.2009 № 537, «национальная безопасность» (утратила силу) определялась уже шире, по аналогии с Законом РФ о безопасности, как «состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства». Таким образом, и безопасность, и ее разновидность – национальная безопасность – рассматривались как широкие по смыслу публично-правовые категории.

В конце XX – начале XXI в. в отечественной правовой науке вышли исследования по правовой (юридической) безопасности¹, конституционной безопасности², гражданской безопасности³ и другим видам безопасности. В этот период стало доминировать мнение о том, что безопасность должна охватывать все сферы жизнедеятельности – «политико-правовую, социальную, экономическую, духовную, причем на местном, национальном, региональном и глобальном уровнях»⁴.

Таким образом, от узкого понимания безопасности правовая наука и практика постепенно перешли к разностороннему и дифференцированному толкованию данной категории. С точки зрения субъекта защиты стали использоваться понятия «безопасность» личности, нации, народа, государства, общества, должностного лица, населения, трудового коллектива, детей, инвалидов, пациентов и т.п. По сферам регулирования и отраслям управления в правовой доктрине и практике выделяются экологическая, энергетическая, ядерная, радиационная, химическая, медицинская, пожарная и другие виды безопасности, такие как оборонная, военная, антитеррористическая, экономическая, финансовая, продовольственная, промышленная.

В условиях современного научно-технологического развития выдвигаются такие новые виды безопасности, как биологическая, генетическая, нейронная, духовная, психофизиологическая, электронная, цифровая и иные.

¹ См., напр.: Дрейшев В.В. Правовая безопасность и проблемы ее обеспечения // Правоведение. – 1998. – № 2. – С. 11–17; Фомин А.А. Юридическая безопасность – особая разновидность социальной безопасности: понятие и общая характеристика // Государство и право. – 2006. – № 2. – С. 72–80; Галузин А.Ф. Правовая безопасность как самостоятельный вид безопасности // Право и политика. – 2007. – № 12. – С. 117–125; Осипов В.А. Механизм обеспечения правовой безопасности правовой системы общества в современных условиях (теоретико-правовые аспекты) // Юридический мир. – 2009. – № 1. – С. 22–26.

² Гончаров И.В. Законодательное обеспечение конституционной безопасности Российской Федерации // Конституционное и муниципальное право. – 2003. – № 4. – С. 31–34.

³ Казанцев Н.М. Российское право гражданской безопасности в свете стандартов европейского права // Европейское право и национальное законодательство: сб. науч. тр. / РАН, ИНИОН. – Москва, 2007. – С. 190–191.

⁴ Эбзеев Б.С., Айбазов Р.У., Краснорядцев С.Л. Глобализация и государственное единство России. – Москва, 2006. – С. 8.

В образовательных программах и научных исследованиях внедряется новое направление – безопасность жизнедеятельности. В этом понятии синтезируются критерии благоприятных условий жизни, труда, отдыха и развития человека. В Российской Федерации интерес к безопасности жизнедеятельности возрос в связи с закреплением поправками в Конституцию РФ 2020 г. нового предмета совместного ведения Российской Федерации и субъектов РФ – «создание условий для ведения здорового образа жизни, формирование культуры ответственного отношения граждан к своему здоровью» (п. «ж» ч. 1 ст. 72). Соответствующим образом возникает запрос на формулирование таких нарративов, как «право безопасности жизнедеятельности» и «право на безопасность жизнедеятельности», что в свою очередь обуславливает необходимость выявления перспектив их формирования и развития как новых правовых образований, определения их природы и места в отраслях права. В российской литературе издаются учебники и учебные пособия, где отдельным блоком рассматриваются «правовые основы безопасности жизнедеятельности»¹.

Необходимо отметить, что в современных исследованиях используются различные подходы к пониманию видов безопасности. Встречается и такая точка зрения, что «общественная безопасность» – это родовое понятие по отношению к безопасности индивидов, семьи, организаций, государства и международной безопасности. Сама безопасность при этом называется явлением социальной опасности². Такая интерпретация скорее всего основывается на философско-социальном подходе, в то время как в праве основанием дифференциации выступают прежде всего субъект и объект правового регулирования.

Несмотря на разнообразие взглядов, общий подход заключается в понимании безопасности как состояния защищенности от опасностей, называемых рисками, вызовами и угрозами. При этом каждый из видов безопасности имеет общее и особенное в признаках и правовых механизмах обеспечения.

Дефиниция каждого вида безопасности должна опираться, как представляется, на аксиологическую ценность объекта защи-

¹ См., напр.: Безопасность жизнедеятельности: учеб. пособие / под ред. чл.-корр. РАН, проф. И.М. Чижа, д-ра мед наук, проф. С.Н. Русанова. – 2-е изд. перераб. и доп., электрон. – Москва, 2022. – 305 с.

² Фетисов В.Д., Эриашвили Н.Д. Правовой аспект безопасности Российской Федерации // Закон и право. – 2025. – № 6. – С. 134.

ты. К примеру, «государственная безопасность» – «это защищенность государственного строя от рисков и опасностей, общественная безопасность связана с отсутствием угроз и вызовов для общественного правопорядка», а «национальная безопасность» – это «способность государства и его народа (нации) самостоятельно или совместно с другими странами и народами препятствовать реализации внутренних и внешних угроз и вызовов государственному и общественному строю»¹.

Неоднозначное понимание вызывает термин «безопасность личности». Встречается трактовка «безопасности личности» как понятия, равнозначного или поглощаемого категорией «общественная безопасность»². Между тем это разные понятия. Безопасность личности касается законных прав и интересов конкретного индивида, в то время как объектом общественной безопасности является общественный правопорядок. Представляется, что научные взгляды и регулирование «безопасности личности» связаны с пониманием права на безопасность как субъективного права.

Право на безопасность реализуется в двух формах – индивидуальная (право человека или личности) и коллективная (право народов, населения, нации). Индивидуальная форма представлена сегодня чаще как право на безопасность личности, а не как универсальное право человека на безопасность. Между тем для современных концепций и доктрин, международных и национальных правовых актов более релевантен термин «человек» как носитель прав и свобод. Как верно отмечается в юридической литературе, «личность» – это абстрактная философская категория, социально-психологическое понятие, которое при этом в различные периоды человеческой цивилизации может трактоваться по-разному³. Тем не менее современные конституции и действующее законодательство государств по-прежнему содержат положения, определяющие право личности на безопасность (право на безопасность личности), соизмеряя это благо с такими ценностями, как жизнь и свобода. В этом контексте право человека на безопасность относится к группе личных прав и свобод.

¹ Подробнее об этом см.: Умнова И.А. Право мира. – Москва, 2010. – С. 380–398.

² Кондрашов Б.П. Общественная безопасность и административно-правовые средства ее обеспечения. – Москва, 1998. – С. 8.

³ Фетисов В.Д., Эриашвили Н.Д. Правовой аспект безопасности Российской Федерации // Закон и право. – 2025. – № 6. – С. 137.

Доктрина и регулирование права на безопасность: от истоков к современности

Доктринальные истоки права на безопасность берут свое начало в теории естественных и неотчуждаемых прав и свобод, разработанной Т. Гоббсом, Дж. Локком и их последователями в XVII–XVIII вв. Согласно этой теории, безопасность, наряду с правом на жизнь и свободу, рассматривается как естественное право человека.

В XVIII–XIX вв. развитие полицейского права в Европе и России привело к новой парадигме безопасности – защите в совокупности интересов государства, общества и индивида. Во второй половине XX столетия, наряду с пониманием права на безопасность как правовой возможности индивида, формируются коллективные права человека, в том числе право народов на безопасность¹.

Ключевой аспект, обсуждаемый в правовой науке относительно содержания права на безопасность, – это баланс между свободой и ее ограничениями. В этом отношении интересен прецедент из судебной практики США о признании приоритета общественной безопасности над свободой личности. В решении по делу *Buck vs Bell* (1981 г.) Верховный Суд США признал конституционным стерилизацию душевнобольных в штате Небраска, основываясь на приоритете общественных интересов над личными правами, в данном случае – сохранения генофонда нации.

Большинство современных конституционалистов настаивают на паритете свободы, жизни и безопасности как условия и цели вводимых ограничений в контексте реализации прав человека, подчеркивая морально-этическую сущность оценки соотношения между этими ценностями². В России это мнение также широко представлено в исследованиях, посвященных рассматриваемому

¹ Барбин В.В., Борисов А.В., Рыжова Ю.В. Обеспечение прав и свобод человека и гражданина в деятельности органов государственной власти: учебник. – Москва, 2020. – С. 45.

² Yu Sh., Carroll F. A Balance of Power: Exploring the Opportunities and Challenges of AI for a Nation // Applications for Artificial Intelligence and Digital Forensics in National Security / ed. Reza Montasari. – Switzerland: Springer, 2023. – P. 22–23.

праву¹. Между тем рост рисков и угроз человеческому существованию и развитию заставляет иначе расставлять приоритеты правовой защиты как в международном праве, так и в конституциях и законодательстве государств. Постепенно жизнь и безопасность занимают приоритетное положение над свободой в правовых доктринах и действующем праве, особенно в случае чрезвычайных и экстренных ситуаций, при необходимости защиты публичных интересов (государственный суверенитет, оборона, общественный порядок, общественная нравственность, благосостояние нации (народа) и т.п.).

Международно-правовые и конституционные основы права безопасности

Право безопасности на международно-правовом уровне формируется сегодня на основе большого и разноуровневого по своей природе числа актов:

– универсальных общего характера (Устав ООН, Заключительный акт СБСЕ 1975 г., Декларация тысячелетия ООН 2000 г., Пакт во имя будущего 2024 г.), которые определяют принципы безопасности;

– универсальных и региональных, касающихся прав человека (Всеобщая декларация прав человека 1948 г., Международные пакты ООН о правах человека 1966 г., Африканская Хартия прав человека и прав народов, принятой ОАЕ в 1981 г., Азиатско-Тихоокеанская Декларация человеческих прав индивидов и народов 1988 г., Конвенция СНГ о правах и основных свободах человека 1995 г. и др.);

– отраслевых и институциональных (Конвенция Международного агентства по атомной энергии (МАГАТЭ) о помощи в случае ядерной аварии или радиационной аварийной ситуации 1986 г., Конвенция МАГАТЭ о ядерной безопасности 1994 г., Объединенная конвенция МАГАТЭ о безопасности обращения с отработавшим топливом и о безопасности обращения с радиоактивными отходами 1997 г., Международный кодекс поведения в отношении поставок оружия, составленный в 2000 г. лауреатами Нобелевской премии мира (проект) и др.);

¹ Корабельникова Ю.Л. О конституционно-правовой природе и содержании права на безопасность // Труды Академии управления МВД России. – 2021. – № 3 (59). – С. 60–63.

– региональных, касающихся механизмов внешней политики, обороны и коллективной безопасности (Договор о коллективной безопасности 1992 г. государств – участников СНГ).

С 1999 г. в ООН функционирует Целевой фонд по безопасности человека, деятельность которого направлена на сотрудничество с государствами-участниками в реализации глобальных задач выживания и развития в условиях мирной жизни, поиска дополнительных ресурсов, направляемых на обеспечение благополучия и достоинства человека.

Важное значение имело признание на международно-правовом уровне права на безопасность. Данное право подразумевается в ряде положений, связанных с ограничением прав и свобод. Так, согласно ст. 29 Всеобщей декларации прав человека ООН, при осуществлении своих прав и свобод каждый человек должен подвергаться только таким ограничениям, какие установлены законом исключительно с целью обеспечения должного признания и уважения прав и свобод других и удовлетворения справедливых требований морали, общественного порядка и общего благосостояния в демократическом обществе.

Впервые право на безопасность человека и народов было закреплено в региональных международных правовых актах о защите прав и свобод («право на мир и безопасность как внутри страны, так и на международном уровне» в Африканской Хартии прав человека и прав народов 1981 г.; «право на мир и безопасность в своем коллективе, государстве, на Земле в целом» в Азиатско-Тихоокеанской Декларации человеческих прав индивидов и народов 1988 г.).

В конституциях современных государств право на безопасность формулируется как самостоятельно (ст. 16 Конституции Эфиопии), так в связке с другими правами и свободами: право на свободу и личную безопасность в конституциях Испании (ст. 17), Португалии (ст. 27), Перу (ст. 2); право на жизнь, здоровье и безопасность в Конституции Боливии (ст. 7).

Отдельные аспекты безопасности привязываются к конкретным видам и сферам жизнедеятельности. Так, согласно ст. 31 Конституции Азербайджана каждый обладает правом на безопасное проживание. В соответствии с ч. 3 ст. 37 Конституции РФ каждый имеет право на труд в условиях, отвечающих требованиям безопасности и гигиены. Аналогичные положения содержатся в конституциях республик Беларусь (ст. 41), Казахстана (ст. 24), Кыргызстана (ст. 42) и других. Исходя из содержания ст. 20

Конституции Либерии, никто не может быть лишен безопасности личности иначе как по решению суда.

Если конституционная формулировка «право на свободу и личную безопасность» отражает естественно-правовой смысл дихотомии «свобода и безопасность», то «право на безопасность» подразумевает более широкое понимание и дуализм индивидуального и коллективного с точки зрения носителей права и защищаемых законных интересов. Сочетание трех ценностей в модальности одного субъективного права – жизнь, здоровье и безопасность – также имеет естественно-правовые истоки и подчеркивает, что все три ценности являются фундаментальными по своей природе и предназначению.

Еще одним направлением конституционного регулирования является определение институтов публичной власти, системы и полномочий органов государственной власти, деятельность которых направлена на обеспечение безопасности (от органов общей компетенции до специализированных государственных органов). Конституции многих государств непосредственно в тексте основного закона указывают на специализированный государственный орган, отвечающий за безопасность в стране. К таким органам отнесены, к примеру, Совет Безопасности в РФ и Республике Беларусь, Совет национальной безопасности в Грузии и Турции, Высший Совет национальной безопасности в Иране, Комиссия по вопросам службы безопасности в Белизе и др.

Роль конституций государств состоит в том, чтобы определить основы безопасности, однако полноценное формирование национальных моделей права безопасности подразумевает системную взаимосвязь нормативных правовых актов всех уровней. На примере Российской Федерации можно продемонстрировать современные модели правового регулирования права безопасности, отражающие как общие подходы, так и национальную идентичность.

Российская национальная модель права безопасности

В российской Конституции (ред. 2020 г.) термин «безопасность» используется в различных комбинациях: «безопасность» (ст. 37; п. «м» ст. 71, 79.1), «безопасность государства» (ст. 13, 55; п. «м» ст. 71; ст. 82; п. «ж» ст. 83; п. «к» ч. 1 ст. 102), «государственная безопасность» (п. «д» ч. 1 ст. 114), «безопасность граждан» (ст. 56), «безопасность людей» (ст. 74; ч. 1, ст. 98), «безопасность

личности» (п. «м» ст. 71; п. «ж» ст. 83), «безопасность общества» (п. «м» ст. 71; п. «ж» ст. 83), «общественная безопасность» (п. «б» ч. 1 ст. 72), «экологическая безопасность» (п. «д» ч. 1 ст. 72).

Конституция РФ в различных главах содержит нормы, декларирующие как безопасность в целом, так и ее виды. По частоте упоминания на первом месте стоит безопасность государства (государственная безопасность). Трижды упоминается безопасность общества (общественная безопасность) как конституционно защищаемая ценность. Среди отраслевых видов безопасности отдельно упоминается экологическая безопасность.

В развитие конституционных положений в настоящее время в Российской Федерации действует разветвленное законодательство, регулирующее как общие вопросы безопасности, так и отдельные ее виды.

Ключевую роль в правовом регулировании безопасности играет Федеральный закон от 28.12.2010 № 390-ФЗ (ред. от 10.07.2023 № 286-ФЗ) «О безопасности». По сравнению с ранее действовавшим Законом РФ о безопасности новый Федеральный закон не содержит определения безопасности, однако исходя из Конституции РФ закрепляет его виды: безопасность государства, общественная безопасность, экологическая безопасность, безопасность личности, иные виды безопасности, предусмотренные законодательством Российской Федерации (ст. 1).

В более развернутом виде перечень видов безопасности представлен в подп. 1 п. 5 Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 02.07.2021 № 400. В действующей Стратегии «национальная безопасность» определяется как состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны. В отличие от определения, которое было дано в ранее действовавшей Стратегии национальной безопасности 2009 г., речь идет о защите не трех традиционных субъектов: личности, общества и государства, а национальных интересов Российской Федерации, при этом дополнительным объектом защиты выступает социально-экономическое развитие страны. Можно предположить, что законодатель стремится выйти из ограниченного перечня защищаемых субъектов, и

акцент сделать на защиту того, что является благом российской нации в целом. Следуя этому предположению, становится понятным, почему в новой Стратегии основными направлениями обеспечения национальной безопасности (разд. IV) определены: сбережение народа России и развитие человеческого потенциала (социальная или гражданская безопасность), оборона страны (военная безопасность), государственная и общественная безопасность, информационная безопасность, экономическая безопасность, научно-технологическое развитие, экологическая безопасность и рациональное природопользование, защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти.

Содержание и субъекты права на безопасность, а также виды безопасности как объекты правовой защиты конкретизируются в Российской Федерации различными федеральными законами: например, Законом РФ от 07.02.1992 № 2300–1 (ред. от 07.07.2025) «О защите прав потребителей», а также следующими федеральными законами: от 09.01.1996 № 3-ФЗ (ред. от 18.03.2023 № 67-ФЗ) «О радиационной безопасности населения»; от 06.03.2006 № 35-ФЗ (ред. от 28.02.2025 № 16-ФЗ) «О противодействии терроризму»; от 21.07.2011 № 256-ФЗ (ред. от 07.07.2025) «О безопасности объектов топливно-энергетического комплекса»; от 26.07.2017 № 187-ФЗ (ред. от 07.04.2025) «О безопасности критической информационной инфраструктуры Российской Федерации» и др. Право на безопасность обеспечивается соответствующей системой публичной власти, т.е. органами специальной и общей компетенции. Так, на органы полиции возложены обязанности по обеспечению безопасности граждан, устранению угроз их безопасности и общественной безопасности (Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 31.07.2025) «О полиции»).

Федеральный закон от 21.12.2021 № 414-ФЗ (ред. от 31.07.2025 № 327-ФЗ) «Об общих принципах организации публичной власти в субъектах Российской Федерации» определяет в ст. 44 полномочия органов государственной власти субъектов РФ в сферах обеспечения безопасности, связанной с чрезвычайными ситуациями (п. 5, 89); ситуациями, которые могут привести к нарушению функционирования систем жизнеобеспечения населения и ликвидации их последствий (п. 6); транспортной (п. 22,24) и пожарной безопасности (п. 65, 114); гражданской и территориальной обороны (п. 87,88); безопасности гидротехнических сооружений на территории субъекта РФ (п. 139, 147); информационной безо-

пасности (п. 163,166); климатической безопасности (п. 168); радиационной безопасности от источников и веществ, находящихся в собственности субъектов РФ (п. 170).

Безопасность на местном уровне обеспечивается Федеральным законом от 20.03.2025 № 33-ФЗ «Об общих принципах организации местного самоуправления в единой системе публичной власти». За органами местного самоуправления в ч. 2 и 3 ст. 32 закрепляются различные полномочия по обеспечению жизнедеятельности населения, в частности осуществления первичных мер пожарной безопасности (п. 21); деятельности аварийно-спасательных служб и (или) аварийно-спасательных формирований (п. 15); осуществления мероприятий по обеспечению безопасности людей на водных объектах (п. 16).

Практически вся система публичной власти федерального, регионального и местного уровней, представляющих все виды и ветви власти (законодательную, исполнительную, судебную), обеспечивает с помощью различных полномочий безопасность государства, общества и человека. В системе федеральных органов государственной власти определяющее значение имеет деятельность Президента РФ и Совета Безопасности РФ, а также правоохранительных и правозащитных органов¹.

Исходя из вопросов совместного ведения, субъекты РФ в своих конституциях (уставах) и законодательстве конкретизируют федеральное законодательство и выделяют в качестве собственных полномочий вопросы охраны общественного порядка и обеспечения безопасности граждан (например, ст. 13 Устава города Москва от 28.06.1995 (в ред. от 25.12.2024)). Во многих субъектах РФ и на уровне местного самоуправления приняты концепции безопасности, определяющие конкретные механизмы обеспечения безопасности на территории проживания. Например, в Концепции комплексной безопасности города Москвы, утвержденной распоряжением правительства Москвы 16.04.2010 № 707-РП (утратила силу), отмечалось, что обеспечение безопасности Москвы не только как столицы и субъекта РФ, но и как крупнейшего города страны с многомил-

¹ См., напр.: Федеральный конституционный закон от 26.03.1997 № 1-ФКЗ (ред. от 29.05.2023) «Об Уполномоченном по правам человека в Российской Федерации», а также федеральные законы: от 17.01.1992 № 2202-1 (ред. 03.03.2025) «О прокуратуре Российской Федерации»; от 30.11.2011 № 342-ФЗ (ред. 08.12.2024) «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации».

лионным населением является необходимым условием обеспечения жизни и деятельности жителей.

В настоящее время в городах-миллионниках в условиях широкого внедрения цифровых технологий разрабатываются концепции «безопасного города», при этом между регионами активно осуществляется обмен опытом в этом направлении (Москва, Санкт-Петербург, Казань, Ярославль и др.)¹. Предназначение Концепции «безопасного города» состоит в интеграции цифровых технологий для мониторинга и повышения безопасности городской среды, которые позволяют быстро реагировать на угрозы и риски, правонарушения, аварии и иные инциденты, предотвращать чрезвычайные и криминальные ситуации, совершенствовать работу экстренных служб. Повсеместно внедряются видеоаналитика, датчики и платформы управления для контроля безопасности общественных мест, управления социальной, транспортной и иной городской инфраструктурой. Благодаря этим мерам обеспечивается автоматическое обнаружение проблем с мгновенной передачей координат события и активацией служб реагирования.

Оценивая действующую систему российского законодательства, современные правоведы предлагают различные пути ее совершенствования. Интересным видится предложение о принятии Кодекса безопасности Российской Федерации². Его задача – это не только систематизация действующего законодательства и повышение статуса специализированного закона, но и устранение коллизий и неопределенностей в использовании основных понятий, проведение логически последовательной структуризации институтов права безопасности.

Заключение

Формирование и эволюция права безопасности дают основание утверждать о приобретении данным правовым образованием в XXI столетии качеств мегаотрасли права. Это проявляется в ком-

¹ Концепция «безопасного города»: какие технологии приблизят регионы к защищенной городской среде. – URL: <https://www.techinsider.ru/technologies/1715771-koncepciya-bezopasnogo-goroda-kakie-tehnologii-priblizyat-regiony-k-zashchishchennoi-gorodskoi-srede/?ysclid=miliudmhj58774239> (дата обращения: 20.11.2025).

² Фетисов В.Д., Эриашвили Н.Д. Правовой аспект безопасности Российской Федерации // Закон и право. – 2025. – № 6. – С. 138–140.

плексной, всеохватывающей юридикации безопасности как объекта правового регулирования, в межотраслевой и институциональной дифференциации видов безопасности, в регулировании права на безопасность как межотраслевого правового института, в формировании международно-правовых, конституционных и законодательных основ права безопасности.

Аксиологическая ценность безопасности как объекта правовой защиты рассматривается в современной юридической науке и практике как приоритетная цель правового регулирования и правоприменения. Безопасность как высшая ценность тесно связана с интересами нации (народа), государства, общества, человека, для которых принципиальное значение имеет самосохранение и развитие.

В перспективе видится целесообразным принятие универсального международного договора о всеобъемлющем обеспечении безопасности (Глобальный пакт безопасности) для систематизации базисных требований к безопасности с учетом современных угроз, вызовов и рисков. Это станет импульсом для принятия или обновления на их основе специализированных законов или кодексов безопасности в государствах – участниках данного договора.

ТРЕТЬЯКОВА Е.С.¹ ПРАВО БИОБЕЗОПАСНОСТИ: ТЕОРЕТИКО-ПРАВОВОЕ ОБОСНОВАНИЕ И МЕСТО В СИСТЕМЕ РОССИЙСКОГО ПРАВА (Статья)²

Аннотация. Статья посвящена теоретико-правовому анализу формирующегося права биобезопасности как нового правового образования. Обосновывается актуальность выделения права биобезопасности в связи с ростом биологических рисков, развитием биотехнологий и появлением принципиально новых угроз. В центре исследования находится определение и дифференциация предмета права биобезопасности. Важным аспектом работы является системный анализ взаимосвязи права биобезопасности с другими отраслями права: конституционным, экологическим, административным, уголовным и гражданским правом. Особое внимание уделяется соотношению права биобезопасности с другим формирующимся правовым образованием – биоправом. Сформулирована необходимость развития права биобезопасности по двум основным векторам: расширения сферы регулирования и углубления межотраслевой интеграции.

Ключевые слова: право биобезопасности; биологическая безопасность; предмет права биобезопасности; соотношение права биобезопасности с отраслями российского права.

TRETYAKOVA E.S. Biosecurity law: theoretical and legal justification and place in the system of Russian law (Article)

¹ © Третьякова Екатерина Сергеевна, профессор кафедры теории права и юридической практики Пермского филиала Национального исследовательского университета «Высшая школа экономики», доктор юридических наук, доцент.

² Статья выполнена в рамках проекта «Зеркальные лаборатории» совместно с НИУ ВШЭ-Пермь, ТюмГУ на тему: «Актуальные аспекты прав человека в контексте биоэтики».

Abstract. This article provides a theoretical and legal analysis of the emerging biosecurity law as a new legal framework. The relevance of distinguishing biosecurity law is justified by the increase in biological risks, the development of biotechnology, and the emergence of fundamentally new threats. The core of the research focuses on defining and differentiating the subject matter of biosecurity law.

An important aspect of the work is a systematic analysis of the relationship between biosecurity law and other branches of law: constitutional, environmental, administrative, criminal, and civil law. Special attention is paid to the correlation between biosecurity law and another emerging legal framework – biolaw.

The article formulates the necessity for the development of biosecurity law along two main vectors: expanding the scope of regulation and deepening cross-sectoral integration.

Keywords: biosecurity law; biological safety; subject of biosecurity law; interbranch relations, biolaw, legal regulation.

Для цитирования: Третьякова Е.С. Право биобезопасности: теоретико-правовое обоснование и место в системе российского права (Статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4: Государство и право. – 2026. – № 1. – С. 25–39. – DOI: 10.31249/iajpravo/2026.01.02

Введение

В настоящее время в связи с активным развитием биотехнологий, увеличением соответствующих рисков формируется новая с точки зрения правового регулирования сфера – биобезопасность. Вопросы безопасности являются крайне важными для любого государства, ведь биобезопасность является неотъемлемой частью как глобальной, так и национальной безопасности страны. За последние пять лет значительно увеличилось количество кибератак на лаборатории, работающие с биологическими материалами высокого риска, на 72% возросло число утечек данных таких лабораторий в Великобритании и Южной Африке¹. Во многих государствах продолжают реализовывать проекты по внедрению биологических технологий; так, в 2024 г. Правительством РФ было утверждено

¹ Biosecurity Guide Warns of Risks from AI, Cyber-attacks and Amateur Experiments. – URL: <https://healthpolicy-watch.news/biosecurity-guide-warns-of-risks-from-ai-cyber-attacks-and-amateur-experiments/> (дата обращения 21.10.2025).

распоряжение о создании Научно-технологического центра биоэкономики и биотехнологий¹.

При этом количество и виды рисков в сфере биобезопасности постоянно увеличивается. В 2024 г. Всемирной организацией здравоохранения (ВОЗ) было опубликовано обновленное руководство по лабораторной биобезопасности, в котором искусственный интеллект представлен как дополнительный новый источник возникновения биологического риска².

Правовое обеспечение биобезопасности на современном этапе становится первостепенной задачей многих государств. Количество нормативных правовых актов, обеспечивающих биобезопасность, постепенно увеличивается, а уже существующие правовые акты дополняются новыми нормами, в связи с чем можно констатировать факт формирования нового правового образования – права биобезопасности как совокупности норм, направленных на регулирование, обеспечение и защиту вопросов биобезопасности. В связи с этим требуются проработка соответствующих вопросов на доктринальном уровне, в том числе необходимо их теоретико-правовое обоснование с точки зрения самого формирующегося правового комплекса, вопросов терминологии, проведение анализа соответствующей сферы, а также сосредоточение внимания на включение права биобезопасности в существующую систему права.

Право биобезопасности как формирующееся правовое образование

Что такое право биобезопасности? Как часть объективного права – это формирующееся правовое образование, целью которого является упорядочение отношений в сфере биобезопасности, которые и следует признать предметом данного правового образования. Таким образом, в первую очередь следует разобраться с тем, что такое биобезопасность и какие сферы в нее включены.

¹ В России появится Научно-технологический центр биоэкономики и биотехнологий. – URL: <https://vademec.ru/news/2024/08/19/v-rossii-poyavitsya-nauchno-tekhnologicheskiiy-tsentr-bioekonomiki-i-biotekhnologiy/> (дата обращения 21.10.2025).

² ВОЗ публикует новую редакцию руководства по лабораторной биобезопасности. – URL: <https://www.who.int/ru/news/item/04-07-2024-who-updates-laboratory-biosecurity-guidance> (дата обращения 21.10.25).

Несмотря на то что термин «биобезопасность» в последнее время достаточно часто используется юристами, говорить о сформированности его унифицированного понимания преждевременно.

Легальное определение биобезопасности основывается в первую очередь на биологической, медицинской и экологической составляющих. Так, Федеральный закон от 30.12.2020 № 492-ФЗ (ред. от 23.07.2025) «О биологической безопасности в Российской Федерации», установивший основы государственного регулирования в сфере обеспечения биологической безопасности, предусматривает следующее определение категории «биобезопасность»: «состояние защищенности населения и окружающей среды от воздействия опасных биологических факторов, при котором обеспечивается допустимый уровень биологического риска». При этом определяются опасные биологические факторы, к числу которых относятся события, условия, свойства, эпидемический, эпизоотический, эпифитотический процессы или их комбинация, являющиеся причиной возможного воздействия патогенных биологических агентов (патогенов), паразитических организмов и содержащих их объектов, которые способны нанести вред здоровью человека, животных или растениям, продукции животного и (или) растительного происхождения и (или) окружающей среде.

Доктринальные подходы к определению понятия «биобезопасность», в свою очередь, можно дифференцировать на два основных – узкий и широкий. В узком смысле «биобезопасность» понимается как система мер, направленных на предотвращение попадания опасных микроорганизмов в окружающую среду, например в ходе работы с биологическими образцами в лабораториях; в широком смысле – «биологическая безопасность» охватывает управление всеми аспектами взаимодействия человека и биологической среды, включая борьбу с инфекциями, меры контроля за распространением заболеваний, защиту от вторжения в биологическую целостность организма и др. Сторонником узкого подхода является, в том числе, Д.Н. Шевырев, который формулирует понятие биобезопасности следующим образом: «состояние защищенности населения от угроз биологического характера, возникших естественным путем в отсутствие факторов антропогенного воздействия либо связанных с таким воздействием, а также ввиду ненадлежащего обращения с биологическими веществами, используемыми в мирных целях, либо в случае действий или бездействия,

произведенных в нарушение принципов обращения с биологическими веществами»¹.

Представители широкого подхода предлагают включать в биобезопасность и другие сферы, в том числе связанные с развитием новых технологий. Например, Н.Г. Жаворонкова и В.Б. Агафонов указывают, что «биологическая безопасность призвана обеспечить не только общественную безопасность, но и защиту генетической информации (генофонда), защиту биологических систем, сохранение живыми организмами (человеком, животными, растениями) своей биологической сущности, биологических качеств, предотвращение потери биологической ценности и др.»². Нельзя не согласиться с И.А. Умновой-Конюховой, которая обращает внимание на то, что «биобезопасность – это не только защита от возбудителей инфекций, т.е. от патогенных микробов, вирусов и проч., это в первую очередь защита от вторжения в биологическую идентичность и биоуникальность человека, обеспечение неприкосновенности его биохарактеристик, биологической целостности человека»³.

Представляется, что в современных условиях целесообразно исходить из широкого понимания биобезопасности, при этом учитывая тот факт, что количество рисков в обозначенной сфере постоянно увеличивается. В свою очередь, именно биобезопасность необходимо рассматривать как предмет формирующегося правового образования.

При этом предмет права биобезопасности не является монолитным и может быть дифференцирован в зависимости от сферы обеспечения биобезопасности, на несколько относительно самостоятельных блоков, в зависимости от конкретной сферы обеспечения биологической безопасности:

¹ Шевырев Д.Н. Биологическая безопасность: социально-правовые и терминологические характеристики // Юрист. – 2020. – № 4. – URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=128924#I2QG2VpN3ITwnF9> (дата обращения: 12.11.2025).

² Жаворонкова Н.Г., Агафонов В.Б. Теоретико-методологические проблемы правового обеспечения экологической, биосферной и генетической безопасности Российской Федерации // Lex russica. – 2029. – № 9 (154). – С. 96–109.

³ Умнова-Конюхова И.А. Право биобезопасности, биоправо и биоюриспруденция: соотношение понятий и их содержания // Конституционное и муниципальное право. – 2023. – № 12 – URL: <https://lawinfo.ru/articles/5098/pravo-biobezopasnosti-biopravo-i-bioyurispredenciya-sootnosenie-ponyatii-i-ix-soderzaniya> (дата обращения: 12.11.2025).

1) охрана здоровья человека (санитарно-эпидемиологическая биобезопасность), т.е. общественные отношения, направленные на предупреждение возникновения и распространения инфекционных и массовых неинфекционных заболеваний людей, обусловленных воздействием биологических патогенов. К ключевым объектам могут быть отнесены патогены человека (вирусы, бактерии, прионы), биологические токсины, образцы биоматериалов человека, содержащие патогены. Основные угрозы: пандемии и эпидемии (грипп, COVID-19, холера), внутрибольничные инфекции, последствия аварий в лабораториях working с патогенами 1–2 групп опасности, биотерроризм;

2) охрана здоровья животных (ветеринарная биобезопасность), отношения по предупреждению заноса и распространения возбудителей заразных болезней животных, включая сельскохозяйственных, диких и домашних питомцев. Ключевые объекты: возбудители болезней животных (ящур, африканская чума свиней, грипп птиц и др.), животные-переносчики, животноводческая продукция. К основным угрозам относятся эпизоотии, наносящие серьезный экономический ущерб и создающие риски для здоровья людей (зоонозы), использование возбудителей болезней животных в качестве биологического оружия;

3) охрана растений (фитосанитарная биобезопасность), отношения, связанные с защитой растений и растительной продукции от карантинных объектов – вредителей, болезней и сорняков. Ключевые объекты: карантинные организмы (насекомые-вредители, фитопатогены, инвазивные виды растений), семена, посадочный материал, древесина. Основные угрозы: проникновение и распространение инвазивных видов, что приводит к гибели урожая, деградации экосистем и экономическим потерям;

4) охрана окружающей среды (эколого-биологическая безопасность), отношения по сохранению биологического разнообразия, предотвращению негативных последствий применения биотехнологий и распространения чужеродных видов для экосистем. Ключевые объекты: генно-инженерно-модифицированные организмы (далее – ГМО), инвазивные биологические виды, коллекции патогенных микроорганизмов. Основные угрозы: неконтролируемое распространение ГМО, биологическое загрязнение природных экосистем, потеря биоразнообразия, нарушение биологического баланса;

5) охрана биологической целостности человека, блок предмета права биобезопасности, которому ранее не уделялось долж-

ного внимания; однако, исходя из предложенного авторами широкого подхода к биобезопасности, его также необходимо включать и исследовать как новый, антропоцентричный модуль в системе права биобезопасности.

В данном случае на первый план выходят угрозы точечного, адресного и зачастую скрытого характера, направленные не против здоровья населения в целом, а против биологической сущности отдельного человека. Ответом на этот вызов должна стать концепция охраны биологической целостности человека.

При этом под *биологической целостностью человека* понимается комплексное право личности на физическую и генетическую неприкосновенность (невозможность какого-либо вторжения в организм и геном без добровольного и информированного согласия); сохранение видовой и индивидуальной идентичности (защиту от модификаций, которые могут привести к необратимому изменению биологической природы человека или его уникальных генетических характеристик); самоопределение в отношении своего тела и биологических данных (право распоряжаться своими биоматериалами, генетической информацией и иными биометрическими данными, а также право на защиту от несанкционированного доступа к ним и манипуляций с ними).

Угрозы биологической целостности носят принципиально новый характер по сравнению с традиционными биологическими рисками, и их представляется возможным дифференцировать на несколько групп: генетические (несанкционированное редактирование генома зародышевой линии (герминативных клеток)), ведущее к наследуемым модификациям человека; кража и использование генетической информации (дискриминация на основе генетических рисков, «генетический предиктивный полицинг»); нейротехнологические (вмешательство в нейронную деятельность мозга с целью манипуляции сознанием, поведением или извлечения информации («мыслечтение») с помощью интерфейсов «мозг-компьютер»); связанные с биохакингом (самостоятельные или несанкционированные эксперименты по имплантации устройств, введению экспериментальных биопрепаратов, направленные на «улучшение» человека без надлежащих мер безопасности и этической оценки; цифро-биологические (принудительная или скрытая биометрическая идентификация (сканирование лица, ДНК-анализ)) и создание «цифровых двойников» на основе биоданных, стирание границ между физической и цифровой личностью). При этом стоит учитывать, что в связи с тем, что данная сфера является

новой и постоянно развивающейся, система рисков также с течением времени будет увеличиваться.

Таким образом, проведенный анализ позволяет сделать вывод, что *предмет права биобезопасности* не является однородным, его логично можно дифференцировать на пять вышеназванных групп отношений, для каждой из которых имеет место свой набор объектов, представляющих биологическую опасность, характерные виды биологических угроз, собственный комплекс правовых средств регулирования.

Признание дифференцированной природы предмета права биобезопасности является необходимым условием для формирования системной и эффективной правовой модели противодействия биологическим рискам в современном мире. Такой подход позволит, как представляется, преодолеть излишнюю абстрактность понятия «биобезопасность» и выстроить более точный и практико-ориентированный правовой инструментарий.

Признание дифференцированной природы предмета права биобезопасности имеет важное теоретическое и практическое значение. Оно позволит более системно формировать нормативную основу, разграничивать компетенцию контрольно-надзорных органов, разрабатывать адресные и эффективные правовые механизмы для противодействия конкретным биологическим рискам, а также выстраивать эффективную систему правового регулирования, избегая дублирования и противоречий между нормами разных институтов.

Полагаем, дальнейшее развитие права биобезопасности должно основываться на синтезе двух подходов: интеграционного, видящего его как целостное правовое образование, и дифференцированного, признающего сложную внутреннюю структуру его предмета.

При этом серьезное внимание должно уделяться разработке правового инструментария в данной сфере, начиная с нормативного оформления соответствующих вопросов. Учитывая взаимосвязь биобезопасности с национальной безопасностью, с одной стороны, и с глобальной международной безопасностью – с другой, формирование рассматриваемого правового образования должно происходить как на уровне национального права, так и в международном праве.

Таким образом, право биобезопасности можно рассматривать как правовое образование, носящее межсистемный и межотраслевой характер. В ряде случаев его характеризуют как ком-

плексную отрасль, которая формируется на стыке нескольких самостоятельных отраслей, объединяя их нормы для регулирования узкоспециализированной группы общественных отношений¹, фундаментом для которой служит Федеральный закон «О биологической безопасности в Российской Федерации», выполняющий в том числе системообразующую функцию, но требующий, по мнению автора, доработки, в первую очередь в части понимания категории «биобезопасность».

Взаимодействие права биобезопасности с другими отраслями права и правовыми образованиями

Формирующееся право биобезопасности не может существовать и развиваться в правовом вакууме. Его фундамент и системообразующие принципы коренятся в конституционном праве, являющемся ядром всей правовой системы. Конституция как нормативный правовой акт высшей юридической силы, закрепляющий основы правового статуса личности и устройства государства, выступает первичным источником и ограничителем для любой отрасли национального права, включая регулирование вопросов биобезопасности.

Базовым началом взаимосвязи конституционного права и права биобезопасности является система конституционных прав человека. Полагаем, что регулирование в сфере биобезопасности непосредственно направлено на обеспечение и защиту следующих фундаментальных прав: во-первых, права на жизнь (ст. 20 Конституции РФ), являющегося абсолютным и составляющего основу всех остальных прав. Биологические угрозы (эпидемии, биотерроризм, неудачные генетические эксперименты), в свою очередь, представляют собой прямую опасность для данного права и его надлежущей реализации. Следовательно, государство, в силу своей конституционной обязанности обеспечивать и защищать право на жизнь, обязано создавать эффективную систему правовых, административных и медицинских мер по предупреждению и нейтрализации таких угроз. Право биобезопасности является конкретной юридической реализацией этой обязанности.

¹ Боголюбов С.А., Кичигин Н.В. Экологическое право и биобезопасность: проблемы и перспективы развития // Журнал российского права. – 2021. – № 12. – С. 45.

Следующее конституционное право, непосредственно лежащее в основе права биобезопасности – *право на охрану здоровья и медицинскую помощь* (ст. 41 Конституции РФ). Биобезопасность является неотъемлемым элементом системы общественного здравоохранения. Нормы, регулирующие обращение с патогенами, работу лабораторий, эпидемиологический надзор, напрямую обеспечивают реализацию данного права на популяционном уровне.

Также необходимо отметить право на благоприятную окружающую среду (ст. 42 Конституции РФ), ведь биобезопасность охватывает не только антропоцентрический, но и экосистемный подход. Неконтролируемое распространение генетически модифицированных организмов (ГМО), инвазивных видов или патогенов, поражающих сельскохозяйственные культуры, может нанести непоправимый ущерб экологическому балансу. Таким образом, право биобезопасности служит инструментом защиты ряда конституционных прав человека.

Наиболее тесная и органичная связь права биобезопасности прослеживается с экологическим правом. Фактически право биобезопасности выросло из его недр, сконцентрировавшись на одном из объектов охраны – биологической составляющей окружающей среды. Оба правовых образования направлены на охрану окружающей среды и обеспечение, в том числе, экологической безопасности. Так, нормы, регулирующие обращение с ГМО, охрану редких и исчезающих видов, предотвращение эпидемий и эпизодов, находятся на стыке экологического права и права биобезопасности. Имеет место и институциональная связь: многие государственные органы (например, Роспотребнадзор, Россельхознадзор, Росприроднадзор) реализуют полномочия как в сфере экологического контроля, так и в сфере биобезопасности. Кроме того, ряд ключевых принципов экологического права (принцип предосторожности, презумпции экологической опасности планируемой деятельности) были адаптированы и включены в арсенал права биобезопасности.

Таким образом, экологическое право можно рассматривать в качестве материнской отрасли для права биобезопасности, которая предоставляет концептуальную основу и часть правового инструментария.

Также представляется возможным проследить взаимосвязь права биобезопасности с административным правом, поскольку обеспечение биобезопасности является прежде всего функцией государства; административное право предоставляет основной

массив инструментов для ее реализации. Именно в рамках административного права устанавливается порядок лицензирования деятельности, связанной с патогенными микроорганизмами; правила административного надзора и контроля (проведение проверок, взятие проб); система государственной регистрации и сертификации биологических агентов, лекарств, вакцин, а также административно-правовой статус уполномоченных органов.

С точки зрения реализации охранительной функции, именно нормы Кодекса РФ об административных правонарушениях предусматривают ответственность за нарушения санитарно-эпидемиологических правил, ветеринарных правил и правил карантина растений (гл. 6, 10 КоАП РФ).

Рассматривая вопросы юридической ответственности, нельзя не отметить нормы уголовного права, в первую очередь ст. 248 УК РФ «Нарушение правил безопасности при обращении с микробиологическими либо другими биологическими агентами или токсинами», которая прямо направлена на защиту от наиболее серьезных биологических угроз; ст. 259 УК РФ криминализует, в свою очередь, уничтожение критических местообитаний для организмов, занесенных в Красную книгу РФ. К смежным составам преступлений можно отнести следующие: нарушение санитарно-эпидемиологических правил (ст. 236 УК РФ); ст. 226.1 «Контрабанда» криминализует незаконное перемещение через государственную границу патогенных биологических агентов; экоцид – массовое уничтожение растительного или животного мира, отравление атмосферы или водных ресурсов, а также совершение иных действий, способных вызвать экологическую катастрофу (ст. 358 УК РФ); ст. 238 УК РФ предусматривает ответственность за производство, хранение, перевозку или сбыт товаров, продукции, работ или услуг, которые не отвечают требованиям безопасности жизни или здоровья человека, включая те, что связаны с биологическими факторами, например фальсифицированные лекарства, биологически активные добавки или продукты питания; ст. 254 УК РФ «Порча земли» предусматривает уголовную ответственность за отравление, загрязнение или иную порчу земли вредными продуктами хозяйственной или иной деятельности вследствие нарушения правил обращения с удобрениями, стимуляторами роста растений, ядохимикатами и иными опасными химическими или биологическими веществами при их хранении, использовании и транспортировке, повлекшими причинение вреда здоровью человека или окружающей среде (ст. 355 УК РФ); ст. 246 «Нарушение правил

охраны окружающей природной среды при производстве работ»; ст. 247 УК РФ «Нарушение правил обращения экологически опасных веществ и отходов». Статья 205 УК РФ «Террористический акт» в части биотерроризма также может быть применена для квалификации деяний, посягающих на биобезопасность.

Уголовное право, в свою очередь, обеспечивает максимальную степень защиты от наиболее опасных форм противоправного поведения и, как показывает анализ, содержит большое количество составов в рамках привлечения к ответственности в части обеспечения биобезопасности.

Несмотря на тот факт, что право биобезопасности непосредственно находится в сфере публичного права, можно выявить и некоторые взаимосвязи с отраслями частного права, прежде всего с гражданским правом, которое опосредует гражданско-правовой оборот в сфере биобезопасности (например отношения, возникающие при выполнении научно-исследовательских работ, поставке медицинского оборудования, оказании услуг по вакцинации и т.д.) и регулирует вопросы возмещения вреда (институт деликтной ответственности (гл. 59 ГК РФ) является ключевым для возмещения вреда, причиненного здоровью граждан или имуществу юридических лиц в результате нарушения правил биобезопасности).

Нельзя упустить из внимания взаимосвязь права биобезопасности с другим новым формирующимся правовым образованием – биоправом. *Биоправо* – формирующееся межотраслевое правовое образование, система норм, направленных на юридическое оформление, упорядочение и охрану соматических прав, оказание медицинской помощи, медицинских услуг, проведение медицинских и фармацевтических исследований и экспериментов, генетические манипуляции с органами и тканями живых и мертвых людей на основе принципов морали и биоэтики.

Предмет биоправа широк и разнообразен, к нему относятся вопросы здравоохранения; вопросы соматических прав; вопросы защиты прав различных категорий пациентов; правовая регламентация контрацепции, аборт, новых репродуктивных технологий; правовое регулирование научных медицинских экспериментов; определение критериев диагностики смерти, регулирование вопросов оказания помощи умирающим; правовое регулирование трансплантации, генетики клонирования, манипуляций со стволовыми клетками; вопросы самоубийств и эвтаназии; и другие вопросы, затрагивающие права человека.

Анализ сущности биоправа и права биобезопасности позволяет выявить их глубокую взаимосвязь, которую в числе прочего можно охарактеризовать как диалектическое единство цели и средства, философии, права и технологии.

Биоправо закладывает основу в части права биобезопасности, касающейся охраны биологической целостности человека: задает ценностный каркас – принципы биоправа являются фундаментом, на котором строится право биобезопасности; определяет легальность – действия в рамках биобезопасности (например принудительная вакцинация или карантин) получают этическое и правовое обоснование именно через призму биоправа; также именно биоправо определяет легальность тех или иных манипуляций в рамках использования биотехнологий.

Право биобезопасности, как представляется, в свою очередь, призвано обеспечить права и интересы, их защиту при использовании биотехнологий; при этом необходимо понимать, что предмет биоправа и права биобезопасности пересекаются, и ученым еще предстоит попытаться их разграничить, насколько это будет возможным.

Представляется, что право биобезопасности в большей степени, нежели биоправо, носит формально-определенный характер, так как на сегодняшний день биоправо в большей его части доктринально. В свою очередь право биобезопасности призвано превратить биоэтические принципы и отдельные правовые нормы в работающие стандарты, регламенты и процедуры, четко прописать права и обязанности, процедуры (наряду с биоправом) и меры ответственности. Биоправо в большей степени направлено на обеспечение регулятивной функции, право биобезопасности – охранительной. Право биобезопасности, на наш взгляд, носит более прикладной характер, не рассуждает о допустимости редактирования генома в целом (это сфера биоправа), но детально регулирует, как должны быть оборудованы лаборатории для таких работ и как оцениваются их потенциальные последствия, как это должно контролироваться и каковы могут быть последствия при нарушении соответствующих правил. Право биобезопасности в этой части потенциально можно рассматривать как институт биоправа; именно здесь происходит пересечение между данными правовыми образованиями.

При этом стоит учитывать, что помимо предмета они отличаются по объекту: биоправо – права и достоинство человека, этические аспекты, право биобезопасности – риски для здоровья че-

ловека, его биологической идентичности и окружающей среды. По цели – представляется, что цель биоправа – гуманизация использования биотехнологий, регулирование, обеспечение и защита прав человека в ходе использования биотехнологий, цель права биобезопасности – управление рисками, обеспечение биобезопасности. Отличается и природа норм, в биоправе они ценностно ориентированные, в ряде случаев основанные на философских началах, в праве биобезопасности – зачастую технико-юридические.

Таким образом, можно сделать вывод, что биоправо и право биобезопасности представляют собой взаимодополняющие, но не тождественные элементы правового регулирования вопросов использования биотехнологий. Биоправо выступает в роли стратегического и этического фундамента. Это мировоззренческая основа, которая отвечает на вопрос – ради чего осуществляется правовое вмешательство в столь чувствительную сферу. Оно защищает человека и человечность от возможных злоупотреблений со стороны науки и технологии. Право биобезопасности является тактическим и операциональным инструментом. Это функциональный механизм, который отвечает на вопрос – как практически обеспечить безопасность, минимизировать риски и создать работающие правовые режимы.

Их диалектическая взаимосвязь является необходимой для формирования сбалансированного, эффективного и гуманного правового регулирования. Отрыв права биобезопасности от биоэтических принципов биоправа грозит превращением регулирования в бесчеловечную технократию. В то же время биоправо, лишённое инструментария биобезопасности, рискует остаться набором благих деклараций, неспособных адекватно ответить на реальные вызовы современности.

Еще раз обратим внимание на непосредственную взаимосвязь права биобезопасности с международным правом, в рамках которого в настоящее время уже существует отрасль права международной безопасности, направленная на поддержание мира и предотвращение угроз существованию государств и человечества в целом. В свою очередь формирующееся право биобезопасности может стать межотраслевым институтом, объединяющим нормы данной отрасли и международного биоправа, позволяя реализовать цели права международной безопасности в специфической сфере биологических рисков.

Заключение

Таким образом, право биобезопасности в настоящее время требует пристального внимания и качественной проработки, при этом дальнейшее развитие данного правового образования видится, с одной стороны, в расширении сферы правового регулирования за счет включения отношений, связанных с охраной идентичности человека, увеличением количества норм права, необходимых для эффективного регулирования и охраны соответствующих отношений, с другой – в углублении межсистемной и межотраслевой интеграции и создании скоординированной, непротиворечивой системы правового регулирования, эффективно обеспечивающей и защищающей жизненно важные интересы личности, общества и государства.

АЛЕШКОВА И.А.¹ ПРИНЦИПЫ БИОБАНКИНГА В СИСТЕМЕ БИОПРАВА: НАУЧНЫЕ ПОДХОДЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ (Обзорная статья)

Аннотация. В обзорной статье рассматриваются принципы и правовые подходы к организации и функционированию биобанкинга. Анализируются международные акты и национальное законодательство, в том числе Российской Федерации, декларирующие принципы биобанкинга в системе биоправа: персональной ответственности при реализации порядка биобанкинга; анонимности (приватности) и конфиденциальности биоданных; доверия к процессу сбора, хранения, обработки и обращения биологического материала; уязвимости человека; устойчивости системы биобанков; некоммерциализации биологического материала, обеспечения биобезопасности человека. Раскрываются позиции ученых из различных областей знаний по вопросам биобанкирования и правового регулирования этого направления в медицине и биологии, связанного со сбором, обработкой, хранением и анализом биологического материала человека и биологических образцов организмов и ассоциированной с ними информации для создания больших биологических коллекций или биобанков.

Ключевые слова: биоправо; принципы биобанкинга; биобанкирование; биобанк; биобанкинг; биологический материал; биоданные.

ALESHKOVA I.A. Principles of biobanking in the biolaw system: scientific approaches and development prospects (Review article)

Abstract. The review article discusses the principles and legal approaches to the organization and functioning of biobanking. The arti-

¹ Аleshkova Ирина Александровна, ведущий научный сотрудник отдела правоведения ИНИОН РАН, кандидат юридических наук, доцент.

cle analyzes international acts and national legislation, including that of the Russian Federation, declaring the principles of biobanking in the bioprave system: personal responsibility in implementing the biobanking procedure; anonymity (privacy) and confidentiality of biodata; trust in the process of collecting, storing, processing and handling biological material; human vulnerability; stability of the biobank system; non-commercialization of biological material, ensuring human biosafety. The positions of scientists from various fields of knowledge on biobanking and the legal regulation of this field in medicine and biology related to the collection, processing, storage and analysis of human biological material and biological samples of organisms and associated information for the creation of large biological collections or biobanks are revealed.

Keywords: biolaw; principles of biobanking; biobanking; biobanking; biological material; biodata.

Для цитирования: Алешкова И.А. Принципы биобанкинга в системе биоправа: научные подходы и перспективы развития (Обзорная статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4: Государство и право. – 2026. – № 1. – С. 40–57. – DOI: 10.31249/iajpravo/2026.01.03

Введение

В современной науке за последние десять лет существенно увеличилось количество публикаций, в которых ученые – специалисты в области медицины, биологии, правоведения исследуют новое направление – биобанкирование¹. Оно охватывает действия по сбору, обработке, хранению и анализу биологических материалов (биологических образцов) организмов, оборот ассоциированной с ними информации и порядок создания биологических коллекций, или биобанков (биорепозиторий). Специалистов интересуют не только вопросы правового режима различных видов биобанков, права собственности на биологические материалы и биологические образцы, но и перспективы развития этих сфер, их безопасность для человека. С учетом интенсивного развития и распространения биотехнологий исследователи обращают внимание на необходимость сохранения в практике биобанкирования согласо-

¹ Биобанкирование как ресурс для широкого спектра научных исследований. – URL: <https://rasls.ru/ru/blog/2025-05-22> (дата обращения 11.11.2025).

ванности этических и юридических аспектов¹. Все более активнее обсуждается важность комплексного правового регулирования правоотношений, возникающих в связи с функционированием биобанков², инструментариев их защиты в механизме правового регулирования отношений, связанных со сбором, хранением, оборотом, исследованием биологического материала и биологических образцов³. Кроме того, обсуждаются вопросы, связанные с применением практики информированного согласия на забор, исследование и хранение образцов биоматериала; на медицинское вмешательство в профилактических, диагностических, терапевтических целях; на обработку персональных данных и др. (далее: информированное согласие) и отказа от них⁴, формирования системы принципов организации и функционирования различных видов биобанков⁵ как хранилищ образцов биоматериалов (кровь, сыворотка крови, плазма, слюна, моча, сперма, волосы, ногти) и ассоциированной с ними личной и медицинской информации – медицинских записей, личного и семейного анамнеза, генетических данных. С этой позиции научный интерес в данной обзорной статье представляют вопросы биобанкинга, т.е. безопасного для человека сбора биологического материала для получения, обработки, хранения и предоставления образцов со связанными данными для использования в текущих исследованиях и в будущем, а также интеграция этических принципов этого процесса в правовые регуляторы и архитектуру принципов биобанкинга и др.

Принципы биоэтики и биоправа как основа организации и функционирования биобанкинга

Прежде чем говорить об особенностях влияния принципов биоэтики и биоправа на формирование правового порядка биобан-

¹ Биобанкирование. Национальное руководство / под ред. А.Н. Мешкова, А.С. Глотова, С.В. Анисимова. – Москва: Триумф, 2022. – 308 с.

² «Живые» активы: проблемы и перспективы регулирования биобанкирования. – URL: <https://rasls.ru/ru/blog/2025-05-22> (дата обращения 11.11.2025).

³ Крюкова Е.С., Рузанова В.Д. Правовое регулирование деятельности биобанков в России // Гражданское право. – 2020. – № 6. – С. 39–42;

⁴ Седова Н.Н. Информированное добровольное согласие пациента на медицинское вмешательство: от морального правила к юридической норме // Медицинское право. – 2021. – № 6. – С. 6–12.

⁵ Рузанова В.Д. Передовые технологии в медицине: вызовы юридической науке // Вестник Пермского университета. Юридические науки. – 2024. – № 4. – С. 664–686.

кинга, представляется целесообразным рассмотреть связанные с ним понятия «биобанк» и «биорепозиторий».

Так, согласно российскому законодательству, термин «биобанк» используется, когда характеризуют коллекцию биоматериалов. В п. 9 ст. 2 Федерального закона от 23.06.2016 № 180-ФЗ (ред. от 04.08.2023) «О биомедицинских клеточных продуктах» *«биологический материал* – это биологические жидкости, ткани, клетки, секреты и продукты жизнедеятельности человека, физиологические и патологические выделения, мазки, соскобы, смывы, биопсийный материал». Этот материал применяется, как правило, к коллекциям образцов, взятых у человека. Иное определение этого же понятия содержится в ст. 1 Федерального закона от 03.12.2008 № 242-ФЗ (ред. от 08.08.2024) «О государственной геномной регистрации в Российской Федерации». В этом Законе *«биологический материал»* определяется как материал, содержащий геномную информацию ткани и выделения человека или тела (останков) умершего человека.

Различие в понятиях можно объяснить стремлением законодателя дифференцировать это многообразное явление, представляющее уникальный и ценный ресурс. Биологический материал содержит различного рода информацию о человеке. Соответственно, его можно рассматривать как источник персонифицированной информации о физиологических, генетических, социальных (поведенческих) и иных особенностях человека. Учитывая многозначность ресурсного фактора биоматериала (биологических образцов), существует проблема обеспечения его особого правового режима и контроля, а также охраны и защиты процесса биобанкинга. В связи с этим при формировании правового режима биобанкинга необходимо четко прописать специфику и особенности биобанков (биорепозиториев)¹.

В научной литературе обращается внимание на то, что «в России 20% от общего числа зарегистрированных репозиториев составляют репозитории по медицинской отрасли знаний». Одной из их разновидностей является радиобиологический репозиторий, который представляет собой хранилище тканей (образцы биологи-

¹ Балашова А.И. Особенности правового режима баз данных, относимых к биобанкам // Интеллектуальная собственность. Авторское право и смежные права. – 2023. – № 3. – С. 18–33.

ческого материала)¹. Существует мнение о том, что «для целей разработки механизма административно-правового регулирования в сфере биобанкирования термин “биобанк” надлежит соотносить с терминами “биорепозиторий” и “хранилище биологических материалов” как частное и целое»².

На наш взгляд, существует потребность, во-первых, в определении четкого правового режима биобанков, исходя из целей их создания; во-вторых, в закреплении принципов, на основе которых будут организовываться и функционировать биобанки; в-третьих, в выработке дифференцированного подхода, учитывающего все многообразие видов информации, биоматериалов и др., выступающих в биобанкинге как объекты складывающихся отношений.

Подходы к определению понятий «биобанкинг» и «биобанк» можно проследить, исходя из международных и национальных стандартов РФ, определяющих эти термины, в следующей *таблице*.

<p>Биобанкинг – сбор, подготовка, хранение, тестирование, анализ и распространение определенного биологического материала, а также связанных с ним информации и данных</p>	<p>Международная организация по стандартизации (ISO) ISO 20387:2018 Биотехнология – Биобанкинг – Общие требования к биобанкингу</p>
<p>Биобанкинг – процесс приобретения и хранение биологического материала, включая конкретные действия или все действия, связанные со сбором, подготовкой, сохранением, испытанием, анализом и передачей определенного биологического материала, а также соответствующей информации и данных</p>	<p>Национальный стандарт Российской Федерации «Биотехнология. Биобанкинг. Общие требования» ГОСТ Р ИСО 20387–2021</p>
<p>Биобанк – организация или подразделение организации, которая может принимать, обрабатывать, хранить и распространять биологические образцы и связанные с ними данные для текущих и будущих исследований, диагностики и терапии в соответствии со стандартными операционными процедурами, и включает в себя полный комплекс мероприятий, связанных с его функционированием</p>	<p>Национальный стандарт Российской Федерации «Биотехнология. Биобанкинг. Термины и определения» ГОСТ Р 71251–2024</p>

¹ Юмашева С.И. Медицинские репозитории открытого доступа: состояние и тенденции развития // Библиосфера. – 2023. – № 2. – С. 83–95.

² Куц С.О. Терминологические проблемы концепции «биобанк»: на стыке административного права и медицины // Административное право и процесс. – 2025. – № 1. – С. 77–80.

Принципы биобанкинга в системе биоправа: научные подходы и перспективы развития

Биобанк – юридическое лицо или часть юридического лица, осуществляющие биобанкинг	Национальный стандарт Российской Федерации «Биотехнология. Биобанкинг. Общие требования» ГОСТ Р ИСО 20387–2021
--	---

Представляется, что использование двойных вариаций обусловлено, во-первых, междисциплинарным характером биобанкирования и биобанкинга, а также множественностью действий, совершаемых в ходе этого процесса, видов формируемых структур для его функционирования, форматов информации и др. Расширение сфер биобанкинга влечет за собой формирование дифференцированного подхода к его правовому регулированию.

Анализ законодательства и научной литературы позволяет выделить три основных подхода к развитию биобанкинга. *Первый подход* определяет порядок, определяющий ряд многообразных действий по развитию этого направления в сфере здравоохранения¹, *второй* – порядок организации различных видов биобанков², *третий* – экономический³.

Учитывая, что биотехнологии развиваются очень интенсивно, основу для реализации биобанкинга первоначально составили принципы медицинской этики и биоэтики. Австралийский специалист в области медицины Салех Аббас, исследуя систему принципов медицинской этики, отмечает, что на протяжении всей истории различные культуры и религии подчеркивали святость и достоинство человеческой жизни. В современный период область медицинской этики существенно расширилась и включает принципы: 1) исследовательской этики; 2) этики общественного здравоохра-

¹ Имеется взаимосвязь между понятиями «биобанк» и «биоресурсные центры», «биологические (биоресурсные) коллекции». Так, в п. 8 ст. 2 Федерального закона от 30.11.2024 № 428-ФЗ «О биоресурсных центрах и биологических (биоресурсных) коллекциях и о внесении изменений в статью 29 Федерального закона “О животном мире”» закреплено понятие «генетический материал», которое по своей природе является частью биологического материала. Вместе с тем в указанном нормативном правовом акте четко определено, что положения этого Закона не применяются к отношениям, связанным с коллекциями биологических материалов человека.

² Гурьева М.Э. Биобанкинг в РФ: пути совершенствования законодательства // Вестник экономики, права и социологии. – 2024. – № 1. – С. 131–134.

³ Мохов А.А. Биобанкинг – новое направление экономической деятельности // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2018. – № 3. – С. 33–40.

нения; 3) организационной этики; 4) клинической этики. Их основу составляют четыре этических принципа: *благодеяния, непричинения вреда, автономии и справедливости*. В то же время значительные достижения в медицине и применение новых технологий привели к тому, что наряду с медицинской этикой появилась биоэтика.

Несмотря на то что биоэтика лежит в основе правового регулирования в области биобанкинга, в правовых системах, существующих в разных странах, вырабатывается самобытный набор принципов, учитывающих культурные, религиозные, экономические и иные факторы.

Культура не статична, замечает С. Аббас, она развивается с течением времени. На нее влияют различные факторы, в том числе технический прогресс, экономический рост, изменения в сфере образования и социально-экономическом статусе, глобализация и эволюция общественных ценностей¹.

Так, например, во *Всеобщей декларации о биоэтике и правах человека* (принята резолюцией Генеральной конференции ЮНЕСКО по докладу Комиссии III на 18-м пленарном заседании 19 октября 2005 г.) (так называемые «Бельмонские принципы»). Эта Декларация провозглашает наряду с вышеуказанными ключевыми принципами биоэтики такие, как: уважение человеческого достоинства и прав человека; оценка риска и вреда; обеспечение самостоятельности в принятии решений при соответствующей ответственности за эти решения и уважение самостоятельности других; информированное согласие, признание уязвимости человека и уважение неприкосновенности личности; конфиденциальность; равенство, справедливость и равноправие; недопущение дискриминации и стигматизации, уважение культурного разнообразия и плюрализма; поощрение солидарности между людьми и международное сотрудничество; социальная ответственность за здоровье населения; совместное использование благ; защита будущих поколений и окружающей среды, биосферы и биоразнообразия.

Европейский вариант представлен в Конвенции о защите прав человека и человеческого достоинства в связи с применением достижений биологии и медицины, называемой «Конвенция о правах человека и биомедицине (ETS N 164)» (принята Комитетом министров Совета Европы 19.11.1997 г.) (далее – Конвенция Овье-

¹ Abbas S. Fundamental Principles of Medical Ethics. In: Medical Ethics. – Singapore: Springer, 2025. – P. 37–62. – URL: https://doi.org/10.1007/978-981-96-9199-9_5 (дата обращения: 11.10.2025).

до). В ст. 1 этой Конвенции провозглашаются и защищаются *достоинство и самобытность всех людей*, гарантируются *неприкосновенность частной жизни, права и основные свободы, связанные с применением биологии и медицины*. В ст. 5 Конвенции Овьедо установлено, что любое медицинское вмешательство должно осуществляться с *свободного и осознанного согласия заинтересованного лица*. Помимо информированного согласия такого лица Конвенция уделяет большое внимание соблюдению права на неприкосновенность частной жизни при осуществлении исследований, управлению новыми биомедицинскими разработками.

Принцип индивидуальной целостности также нашел свое отражение в Рекомендации СМ/Рес (2016) 6 Комитета министров государствам – членам ЕС о проведении исследований биологических материалов человеческого происхождения.

Профессор философии на факультете хорватских исследований Загребского университета Паво Баришич, анализируя Конвенцию Овьедо и Бельмонские принципы, делает ряд важных выводов. По его мнению, в Бельмонских принципах наряду с этическими постулатами присутствует прагматический подход, суть которого в том, что фундаментальные этические принципы должны соблюдаться при проведении исследований с участием людей. Примечательно, что уважение к личности и акцент на принцип информированного согласия помог изменить этическую и правовую среду в здравоохранении, сделав такое согласие глобальным стандартом в медицинских и научных исследованиях. И, несмотря на то что Бельмонская биоэтическая традиция оказала значительное влияние на европейскую биоэтику, П. Баришич считает, что обе модели подчеркивают взаимосвязь между этикой и правом, демонстрируя, что биоэтика подкрепляется и структурируется с помощью правовых норм. Общим в рассматриваемых выше международных документах является также то, что они предоставили национальным законодателям четкую основу для решения различных биоэтических проблем, которая заключена в вышеперечисленных фундаментальных принципах. Так, в обоих документах большое значение придается принципу информированного согласия, особенно в вопросах, касающихся исследований и трансплантации органов и донорства. В них биоэтика и биоправо не конкурируют, а дополняют друг друга¹.

¹ Bioethics and Social Ethics in The Modern World: The Environmental and Social Sustainability / I. Pavić (ed.), N. Alfirević (ed.), S. Vuletić (ed.). – Palgrave

Представляется, что принципы биоэтики, закрепленные в нормативных правовых актах, являются принципами биоправа. Они выступают правовой основой для развития биобанкинга. Вместе с тем на развитие биобанкинга как комплексного института биоправа влияют и принципы биоэтики. Общим у принципов биоэтики и биоправа является то, что них заложен гуманистический смысл. И, несмотря на то что биоправо еще рассматривается как неологизм, его все чаще можно встретить в научных статьях, касающихся регулирования биобанкинга. Это связано главным образом с постоянно растущей потребностью современного общества в правовом регулировании биомедицинской деятельности, обусловленной научно-техническим прогрессом. Представляя собой самостоятельные системы, принципы биоправа и биоэтики пересекаются при регулировании сложных и новых общественных отношений, возникающих в таких областях, как геновая инженерия, соматические и репродуктивные технологии, защита биоразнообразия и здравоохранения.

В изданной в 2021 г. Энциклопедии глобальной биоэтики под ред. Хенк тен Хаве, в разделе, посвященном биобанкингу и биобанкам, представлены модели и теории, закладывающие основу биозаконодательства и биоюриспруденции. Лаура Палаццани, ученый из Италии, будучи одним из авторов данной Энциклопедии, отмечает, что биологическое право, возникшее как ответвление биоэтики, в современный период развивается как самостоятельная дисциплина. В контексте современного общества, считает она, существует настоятельная потребность в биоюридических правилах¹.

Параллельное существование биоэтики при регулировании многих вопросов Л. Палаццани объясняет рядом причин. Во-первых, существует различие в скорости развития научно-технического прогресса и биологического законодательства. Оно имеет объективный характер, так как регулирование новшеств применения биотехнологий предполагает обсуждение между экспертами различных дисциплин, использующих разные языки и методологии. Иногда возникает необходимость определить понятия новых юридических категорий, классифицировать их, переосмыслить

Macmillan, 2025. – P. 43. – URL: https://doi.org/10.1007/978-3-031-86418-6_4 (дата обращения: 12.11.2025).

¹ Encyclopedia of Global Bioethics / eds. Henk ten Have. – Springer, 2021. – P. 338.

традиционные юридические понятия, соответствующие новой реальности.

Во-вторых, имеется потребность поиска разумного и рационального в применении научно-технического вмешательства в жизнь человека, потому что все новые явления могут вызвать непредвиденные и необратимые последствия. И принцип предосторожности предполагает первоначально потребность руководствоваться принципами биоэтики и аккуратное включение в практику правовых предписаний.

В-третьих, существующий плюрализм биоэтических принципов порождает различные теоретические модели (авторы выделяют либертарианскую, либеральную, утилитаристскую и персоналистскую модели) биоправа, которые ведут к различным типам регулирования в рамках национального законодательства¹.

Таким образом, развитие биобанкинга непосредственно связано с принципами биоэтики и биоправа, особенностью которых является наличие своих принципов, выступающих основой регулирования деятельности в сфере здравоохранения в условиях научно-технического прогресса.

Принципы биобанкинга как подсистема биоправа

Биоправо – формирующаяся отрасль права и междисциплинарное явление в науке. В его содержание в основном включаются комплексные институты, формирующиеся на основе различных по своей природе регуляторов – принципов и норм этики, культуры, права. Одним из комплексных институтов биоправа является биобанкинг.

В современный период процесс биобанкинга и правовой режим биобанков регламентируются в основном на международном уровне, на уровне профессиональных объединений, а в ряде государств – непосредственно на законодательном уровне. Так, в Международной декларации о генетических данных человека (принята резолюцией Генеральной конференции ЮНЕСКО по докладу Комиссии III на 20-м пленарном заседании 16.10.2003) закреплены многие ранее отмеченные принципы. Среди них – принцип свободной индивидуальности человека, прозрачных и приемлемых с этической точки зрения процедур; недопущение дискриминации и

¹ Encyclopædia of Global Bioethics / eds. Henk ten Have. – Springer, 2021. – P. 338.

стигматизации; информированного согласия и права на его отзыв и др. Кроме этого, значимым предписанием, установленным в п. «б» ст. 1 указанного международного документа, является то, что «любой сбор, обработка, использование и хранение генетических данных человека, протеомных данных человека и биологических образцов должны соответствовать международному праву в области прав человека». Вместе с тем в данной Декларации уже больше внимания уделяется непосредственно принципам сбора, обработки, использования и хранения биологического материала (биологических образцов), которые условно можно назвать *принципы технического регулирования*, и особенно подчеркивается важность *принципа недопущения дискриминации и стигматизации* при осуществлении научно-исследовательской деятельности. В ст. 15 этой Декларации закреплены *принципы достоверности, надежности, качества и безопасности*, которые признаются базисом для организации биобанков и, соответственно, биобанкинга.

В 2009 г. Организация экономического сотрудничества и развития (ОЭСР) разработала Руководящие принципы по биобанкам человека и базам данных генетических исследований. К такому ОЭСР относит следующие принципы: *принцип управления и защиты биологических материалов и данных человека; принцип доступа к данным и человеческим биологическим материалам; принцип сотрудничества в области биобанкинга*¹.

В Исландии действует Закон № 110 от 25.05.2000 «О биобанках»². В ст. 1 этого Закона определяются принципы биобанкинга: *конфиденциальность; защита и приоритет интересов донора; предназначение биобанков научным и медицинским целям; общественное благо; запрет дискриминации донора на основании информации, полученной из его биологического образца, и др.*

Этот пример показывает, что на законодательном и профессиональном уровнях формируется сложная по своей конструкции подсистема принципов биобанкинга, включающая не только принципы биоэтики и биоправа, но и принципы технического регулирования функционирования биобанков.

¹ Guidelines on Human Biobanks and Genetic Research Databases / OECD. – 2009. – URL: <https://web-archiver.oecd.org/2012-06-14/112430-44054609.pdf> (дата обращения: 10.08.2025).

² Lög um lífsýnasöfn (Þingskjal 1411, 125. Lögjafarþing 534. mál: lífsýnasöfn. Lög nr. 110 25. maí 2000). – URL: <https://www.althingi.is/altext/125/s/1411.html> (дата обращения 12.08.2025).

Развитие биобанкирования происходит параллельно в различных странах и регионах мира со свойственными им особенностями в законодательстве и культуре. И, несмотря на то что ученые выделяют различные модели биоправа: либертарианскую, либеральную и утилитаристскую, их общая конструкция формируется на основе универсальных принципов биоэтики, таких как *принцип уважения человеческого достоинства и его прав*. То есть, все формирующиеся принципы биобанкинга имеют гуманистическую основу.

Рассмотрим некоторые из принципов биобанкинга, исследуемые в научной литературе.

Принцип персональной ответственности при реализации порядка биобанкинга. В подготовленном в 2023 г. Справочнике по биоэтическим решениям под редакцией Эрика Вальдеса, Хуана Альберто Лекароса акцентировано внимание на научной добросовестности и институциональной этике. В частности, Джейкоб Даль, анализируя основы принятия биоэтических решений в области биоэтики и биоправа, отдельное внимание уделяет принципу персональной ответственности, взаимосвязывая его с принципом социальной ответственности¹.

Принцип персональной ответственности имеет важное значение при осуществлении биобанкинга. Он взаимосвязан с *принципом уязвимости человека*. Особенно, когда речь идет о многообразии видов биобанков (выделяют научно-исследовательские, клинические, судебно-медицинские и гибридные биобанки). В последние годы начали появляться структуры, объединяющие биобанки населения из разных географических регионов. Что, соответственно, требует особой ответственности организаций, осуществляющих оборот биологических данных.

Принцип анонимности (приватности) и конфиденциальности биоданных. Учитывая существующие риски, связанные с возможными нарушениями конфиденциальности, бельгийские ученые Крис Дирикс и Кристиан Хенс заметили, что принцип анонимности стал активно применяться в биобанкинге. С их точки зрения, реализация этого принципа возможна при полной анонимности человека и кодировании биоматериала. Полная анонимность человека, как правило, обеспечивает наивысшую форму его безопасно-

¹ Handbook of Bioethical Decisions / eds. E. Valdes, J.A. Lecaros. – 2023. – Vol. 2: Scientific Integrity and Institutional Ethics. – P. 289–310. – (Collaborative Bioethics).

сти. Однако есть определенные сведения, которые невозможно утаить от исследователей. Так, при проведении генетических исследований наряду с исходными анонимными данными часто хранится демографическая информация, информация об образе жизни и медицинская информация. Полная автономность также делает невозможным контакт с донором, если будет обнаружено что-то, имеющее отношение к его здоровью. Система кодирования, в которой ключ необходим для связи пациента с его данными, вероятно, является лучшим решением. Этот ключ может храниться в другом месте и управляться третьим лицом. Однако тот факт, что данные и образцы все больше и больше передаются через национальные границы в юрисдикции стран, где существует различное законодательство, может усложнить проблему конфиденциальности¹.

В Европейском союзе действует Общий регламент по защите данных 2018 г. (General Data Protection Regulation) (далее – GDPR), который предусматривает принципы и правила защиты персональных данных граждан ЕС. Регламент применяется к любой организации, работающей с данными жителей ЕС, независимо от местонахождения. В этом акте заложены *общие* принципы: целостности, конфиденциальности и безопасности, а также *специальные* принципы: *ограничения цели*, т.е. данные должны собираться для конкретных, четко определенных и законных целей и не должны обрабатываться в дальнейшем способом, несовместимым с этими целями; *минимизации данных*, т.е. необходимо собирать только те данные, которые необходимы для достижения заявленных целей, и эти данные должны быть точными и, при необходимости, обновляться; *ограниченного хранения данных*, который предполагает, что данные не должны храниться дольше, чем это необходимо для достижения заявленных целей².

В целом, GDPR направлен на предоставление гражданам ЕС большего контроля над их личными данными; на усиление защиты персональных данных в цифровом пространстве и повышение ответственности организаций за обработку персональных данных.

На наш взгляд, в процессе биобанкинга важно обеспечивать высокий уровень надежности сохранности биологических материалов и связанной с ними информации, с учетом требований

¹ Encyclopedia of Global Bioethics / eds. Henk ten Have. – 2021. – P. 258.

² GDPR Requirements for Biobanking Activities Across Europe / eds. V. Colcelli, R. Cippitani, Ch. Brochhausen-Delius, R. Arnold. – Springer, 2023. – P. 1–20.

конфиденциальности, соблюдения принципа доверия к процессу сбора, хранения, обработки и обращения биологического материала.

Принцип доверия к биобанкингу. Биобанкинг важен для осуществления научно-исследовательской и медицинской терапевтической деятельности, но существуют риски утечки биоинформации. Следовательно, это зачастую останавливает человека от добровольного предоставления биоматериалов. Специалисты отмечают, что несмотря на признание значимости биобанкингов для развития биомедицинской науки, распространение биобанков и непрерывное пополнение биоресурсных коллекций сталкиваются с проблемой недоверия и непонимания их деятельности среди населения. В некоторых странах Северной Европы биобанкирование получило широкую известность, тогда как в Китае, на Ближнем Востоке и в России осведомленность о биобанках остается на низком уровне¹.

Принцип доверия к биобанкингу означает уверенность в честности, надежности и добросовестности другого человека или организации, а также ожидание положительного исхода взаимодействия с ними. В контексте биобанкинга этот принцип имеет свои особенности, но общая суть сводится к вере в порядочность и предсказуемость действий другого. В основе доверия между организациями, осуществляющими оборот биоданных, между врачом и пациентом, а также между иными субъектами, участвующими в процессе забора и хранения биологического материала, лежат четкие правила биобанкинга и функционирование биобанков. Кроме того, для доверия важное значение имеют и отлаженный алгоритм использования полученных сведений, и надежный механизм защиты от несанкционированного доступа к биоданным.

Принцип устойчивости системы биобанков. По мнению экспертов, биобанкам необходима финансовая и организационная устойчивость. Финансовая устойчивость важна для развития, управления персоналом и долгосрочного обслуживания хранилищ биологического материала и защиты баз биологических данных. Организационная устойчивость нужна для их надежности². Биобанки

¹ Проблемы доверия и мотивации в биобанкировании / Ю. Бахарева, Е. Каменских, А. Крыгина, О. Федорова // Журнал исследования социальной политики // The Journal of Social Policy Studies. – 2024. – № 22 (4). – С. 745–756. – URL: <https://doi.org/10.17323/727-0634-2024-22-3-745-756> (дата обращения: 12.11.2025).

² Basic Principles of Biobanking: from Biological Samples to Precision Medicine for Patients / L. Annaratone, G. De Palma, G. Bonizzi [et al.] // Virchows Arch. –

могут быть как государственными, так и частными. Если по государственным биобанкам вопрос с финансовой и организационной устойчивостью гарантируется посредством бюджетного финансирования, то в отношении частных биобанков нет таких гарантий.

Значимым при организации и функционировании биобанкинга является также *принцип некоммерциализации биологического материала*, который, по мнению польских ученых, применяется непоследовательно и нередко нарушается на рынке биологического материала человека. В доказательство этого ученые приводят примеры патентования некоторых продуктов, полученных из биологического материала человека, их коммерческого маркетинга или оплаты донорства крови¹.

Представляется, что принцип устойчивости биобанкинга направлен на обеспечение долгосрочного функционирования биобанка, что предполагает стабильное хранение биологических образцов и сопутствующих данных, а также их доступность для будущих исследований. Это достигается за счет эффективного управления системой биобанков, стабильности в финансировании их деятельности, обеспеченности безопасности биоданных инфраструктурной надежности биобанкинга, а также вовлеченности исследовательского сообщества в развитие биобанкирования.

Безопасность человека – конституционная ценность. Исходя из того, что биологический материал содержит разнообразную информацию, и существуют риски, связанные с ее оборотом, полагаем, что необходимо рассматривать *принцип обеспечения биобезопасности человека* как универсальный элемент комплекса принципов биобанкинга.

Новые тенденции и перспективы развития принципов биобанкинга в России

На необходимость создания биобанков и биоколлекций указано в Стратегии развития медицинской науки в Российской Федерации на период до 2025 г. (утверждена распоряжением Правительства РФ от 28.12.2012 № 2580-р). Реализация этой задачи

2021. – № 479. – P. 233–246. – URL: <https://doi.org/10.1007/s00428-021-03151-0> (дата обращения: 12.11.2025).

¹ Biobanking of Human Biological Material and the Principle of Noncommercialisation of the Human Body and its Parts / J. Pawlikowska, J. Pawlikowski, D. Krekora-Zajac // Bioethics. – 2023. – Vol. 37. – P. 154–164. – URL: <https://doi.org/10.1111/bioe.13127> (дата обращения: 12.11.2025).

предусмотрена распоряжением Правительства РФ от 30.12.2020 № 3680-р «Об утверждении плана мероприятий (“дорожной карты”) по развитию и укреплению системы федерального государственного санитарно-эпидемиологического надзора на 2021–2028 годы». К 2028 г. планируется создание в России биобанка на основе образцов биологического материала, полученных от инфекционных и неинфекционных больных на территории РФ. В Стратегии научно-технологического развития Российской Федерации, утвержденной Указом Президента РФ от 28.02.2024 № 145, в числе приоритетов и перспектив научно-технологического развития указан переход к персонализированной, предиктивной и профилактической медицине, высокотехнологичному здравоохранению и технологиям здоровьесбережения, в том числе за счет рационального применения лекарственных препаратов (прежде всего антибактериальных) и использования генетических данных и технологий.

Российской экспертной группой Национальной ассоциации биобанков и специалистов по биобанкированию (НАСБИО) предложена Концепция национальной информационной платформы биобанков, которая «будет представлять собой информационную систему, предназначенную для консолидации, обработки и использования данных о биологических коллекциях и образцах биобанков страны различных форм собственности и типов в интересах развития биобанкирования и научных исследований в области медицины, биотехнологии, промышленности и др.»¹.

В Российской Федерации, наряду со становлением института биобанкирования, развивается и государственная поддержка этой отрасли здравоохранения. С момента принятия Федерального закона от 05.07.1996 № 86-ФЗ (ред. от 29.12.2022) «О государственном регулировании в области генно-инженерной деятельности» государство уделяет особое значение регулированию как генно-инженерной деятельности, так и развитию биобанкирования. Деятельность в области биобанкирования регулируется следующими федеральными законами: от 23.06.2016 № 180-ФЗ (ред. от 04.08.2023) «О биомедицинских клеточных продуктах» (ч. 3 ст. 37); от 21.11.2011 № 323-ФЗ (ред. от 23.07.2025) «Об основах охраны

¹ От имени экспертной группы НАСБИО. Концепция национальной информационной платформы биобанков Российской Федерации / А.Н. Мешков, О.Ю. Ярцева, А.Л. Борисова, М.С. Покровская, О.М. Драпкина // Кардиоваскулярная терапия и профилактика. – 2022. – Т. 21, № 11. – С. 6–12.

здоровья граждан в Российской Федерации»; от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) «О персональных данных»; от 05.07.1996 № 86-ФЗ (ред. от 29.12.2022) «О государственном регулировании в области генно-инженерной деятельности»; от 03.12.2008 № 242-ФЗ (ред. от 08.08.2024) «О государственной геномной регистрации в Российской Федерации», а также рядом подзаконных нормативных правовых актов, в числе которых приказ Минздрава России от 20.10.2017 № 842 н (ред. от 30.01.2019) «Об утверждении требований к организации и деятельности биобанков и правил хранения биологического материала, клеток для приготовления клеточных линий, клеточных линий, предназначенных для производства биомедицинских клеточных продуктов, биомедицинских клеточных продуктов», предусматривающий комплекс принципов технического регулирования организации и деятельности биобанков. Этот приказ адресован субъектам обращения биомедицинских клеточных продуктов и предусматривает требования к температурно-влажностному, санитарно-гигиеническому и световому режиму и порядку их хранения.

Таким образом, можно утверждать, что правовое регулирование биобанкинга формируется на основе принципов биоэтики. В настоящее время можно говорить о выработывании принципов биобанкинга и становлении биоправа и его комплексного института биобанкинга. Их основу составляют принципы медицинской этики и принципы биоэтики, закрепленные в международных и национальных правовых актах.

Заключение

В течение последних десятилетий область биобанкирования стремительно развивается. Имея комплексный характер, институт биобанкинга способствует формированию крупных информационных биобанков, правовой режим которых регулируется так же, как и сам процесс биобанкинга – на основе принципов биоэтики и биоправа. Наряду с универсальными принципами, тщательно разработанными международными организациями в XX в., появляются новые принципы, обусловленные техническим прогрессом. Но их вариативность влияют многие факторы; в их числе культура, экономика, передовые практики, научные и основанные на принципах биоэтики и биоправа, особенностью которых является наличие своих специальных принципов регулирования деятельности в сфере здравоохранения.

*Принципы биобанкинга в системе биоправа: научные подходы
и перспективы развития*

Исходя из состояния современного законодательства о здравоохранении, полагаем, что развитие принципов биобанкинга можно охарактеризовать как конструктивное, однако нуждающееся в систематизации.

АЛФЕРОВА Е.В.¹ БЕЗОПАСНОСТЬ ЧЕЛОВЕКА В УСЛОВИЯХ ВИРУСНЫХ ПАНДЕМИЙ: МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ (Обзор)

Аннотация. Пандемия COVID-19 наглядно продемонстрировала, насколько мир уязвим перед инфекционными заболеваниями. Кризис, вызванный коронавирусом, показал, что международный режим регулирования в сфере глобального здравоохранения имеет явные недостатки, которые проявились во время пандемии. Прежде всего речь идет об отсутствии должного международного сотрудничества государств при разработке вакцин, инновационных схем медицинского лечения и средств индивидуальной защиты, а также о пренебрежении принципом солидарности со странами со средним и низким уровнем доходов, сбое механизмов подотчетности и системы эпиднадзора. Все это привело к пересмотру Международных медико-санитарных правил 2005 г., расширению полномочий Всемирной организации здравоохранения и необходимости разработки эффективных мер предупреждения и нейтрализации масштабных вирусных заболеваний.

В данном обзоре раскрываются дискуссии ученых о постпандемийных реформах в международном здравоохранении и новом предложении ВОЗ о заключении международного соглашения о борьбе с пандемиями в целях укрепления международной безопасности в сфере здравоохранения.

Ключевые слова: безопасность человека; COVID-19; вирусные пандемии; международное право в области здравоохранения; Международные медико-санитарные правила; Соглашение о пандемии; Всемирная организация здравоохранения; эпиднадзор; рос-

¹ Алферова Елена Васильевна, ведущий научный сотрудник, завотделом правоведения ИНИОН РАН, кандидат юридических наук.

сийское законодательство; защита населения; чрезвычайные ситуации.

ALFEROVA E.V. Human security in the context of viral pandemics: international legal aspects (Review)

Abstract. The COVID-19 pandemic has clearly demonstrated how vulnerable the world is to infectious diseases. The crisis caused by the coronavirus has shown that the international regulatory regime in the field of global health has obvious shortcomings, which manifested themselves during the pandemic. First of all, we are talking about the lack of proper international cooperation between states in the development of vaccines, innovative medical treatment schemes and personal protective equipment, as well as disregard for the principle of solidarity with middle- and low-income countries, failure of accountability mechanisms and surveillance systems. All this led to the revision of the International Health Regulations of 2005, the expansion of the powers of the World Health Organization and the need to develop effective measures to prevent and neutralize large-scale viral diseases. This review highlights scientists' discussions on post-pandemic reforms in international healthcare and the WHO's new proposal to conclude an international agreement on combating pandemics in order to strengthen international health security.

Keywords: human security; COVID-19; viral pandemics; international health law; International Health Regulations; Pandemic Agreement; World Health Organization; surveillance; Russian legislation; public protection; emergency situations.

Для цитирования: Алферова Е.В. Безопасность человека в условиях вирусных пандемий: международно-правовые аспекты (Обзор) // Социальные и гуманитарные науки: Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2026. – № 1. – С. 58–75. – DOI: 10.31249 /iajpravo/2026.01.04

Введение

Международная и национальные системы обеспечения вирусной безопасности, столкнувшись с пандемией COVID-19, подверглись серьезному испытанию. Данные смертности в этот период, а также число людей, переболевших ковидом, говорят о том, что современная система здравоохранения, в том числе система

эпиднадзора, и международная организация ВОЗ оказались не состоятельны¹.

Сегодня, по прошествии пяти лет, продолжают острые дискуссии ученых о том, почему в век прорывных медицинских технологий и цифровых достижений стало возможным это крупнейшее в мире бедствие. Число смертей от COVID-19 – самое высокое в мире со времен испанки и Второй мировой войны. На это указывается не только в официальной статистике ВОЗ, но и во многих научных исследованиях [1; 2; 3; 4; 5; 6; 7; 11 и др.].

Юристы пишут о «многочисленных административных и нормотворческих проблемах, которых можно было избежать, если бы заранее были определены рамки и алгоритмы необходимых действий в сложившейся критической ситуации» (6, с. 106), и преодолеть «неконтролируемое распространение пандемии коронавирусной инфекции COVID-19» [2, с. 106].

Некоторые исследователи сетуют, что до пандемии COVID-19 не хватало юридической литературы, посвященной нормативным вопросам, касающимся отслеживания заболеваний и контактов. Такая относительная неизвестность, пожалуй, неудивительна. К настоящему времени в обширной литературе изучено, как пандемия COVID-19 привела к структурным правовым проблемам во всем мире. Такие темы, как реализация чрезвычайных полномочий уполномоченными органами и выполнение обязательств в области прав человека, были вновь открыты и переосмыслены во время пандемии.

¹ По данным университета Джона Хопкинса, за три года пандемии ковидом в мире переболели 674 млн 186 тыс. 736 человек, или каждый 12-й житель Земли (см.: Три года коронавируса и сколько потеряла Россия. – URL: <https://newizv.ru/news/2023-03-01/tri-goda-koronavirusa-kogo-i-skolko-poteryala-rossiya-398289?ysclid=mhg6srw8tv461204427> дата обращения: 17.11.2025).

По состоянию на 15 октября 2025 г. в мире зарегистрировано 7 101 788 подтвержденных случаев смерти от COVID-19 (см.: Смертность от пандемии COVID-19. – URL: https://en.wikipedia.org/wiki/COVID-19_pandemic_deaths?ysclid=mhg6y6vyyo7532666809; Coronavirus Pandemic (COVID-19) // Our World in Data. – 2025. – 15 October. – URL: https://en.wikipedia.org/wiki/COVID-19_pandemic_deaths?ysclid=mhg6y6vyyo7532666809; Панель мониторинге ВОЗ за последние 28 дн до 12. окт 2025 г. (см.: Данные ВОЗ. – URL: <https://data.who.int/dashboards/covid19/deaths>; По данным Росстата, в 2020 и 2021 гг. в России умерли 2,446 млн человек. – URL: <https://newizv.ru/news/2023-03-01/tri-goda-koronavirusa-kogo-i-skolko-poteryala-rossiya-398289?ysclid=mhg6srw8tv461204427> (дата обращения: 17.11.2025).

В данном обзоре представлены точки зрения исследователей международно-правовых проблем борьбы с коронавирусной инфекцией COVID-19 и дискуссии ученых о реформе Международных медико-санитарных правил (ММСП) 2005 г., в целях успешного преодоления в будущем любых пандемий.

Переосмысление правовых возможностей Всемирной организации здравоохранения

Одной из (вновь) открытых областей юридических исследований является область индивидуальных процедур надзора за общественным здравоохранением, понимаемых как «непрерывный, систематический сбор, анализ и интерпретация данных, связанных со здоровьем», включая, но не ограничиваясь этим, отслеживание заболеваний и контактов. В целом, с помощью обеих этих процедур ВОЗ и национальные органы здравоохранения отслеживают распространение заболевания от человека к человеку, чтобы выявить – и, возможно, разорвать – цепочки передачи [15, р. 604–605].

Быстрое распространение COVID-19 указывает на то, что методов и средств, используемых государствами и международными организациями, прежде всего ВОЗ, в борьбе с этой угрозой во многих случаях было явно недостаточно. Руководство ВОЗ по борьбе с пандемией COVID-19 с самого начала подвергалось критике. Во-первых, ее обвинили в запоздалом реагировании на новую пандемию. Отчасти это было связано с тем, что Китай поначалу не сообщил ВОЗ о вспышке нового инфекционного заболевания, а также с нерешительным подходом ее в ситуации возможной паники из-за неопределенности в отношении нового заболевания. Во-вторых, хотя ВОЗ рекомендовала ввести умеренные ограничения на поездки и грузоперевозки, большинство стран ввели гораздо более жесткие запреты на передвижение и торговлю. В-третьих, только треть государств-участников выполнили свои обязательства по созданию соответствующих средств и условий по борьбе с коронавирусом. В-четвертых, ВОЗ не смогла обеспечить надлежащее сотрудничество в области распределения вакцин, медицинского лечения и средств индивидуальной защиты, что привело к многочисленным смертям в странах со средним и низким уровнем дохода, которых можно было бы избежать [12, р. 744–745].

Обязанность собирать и распространять статистические данные о смертности уполномочена ВОЗ. Однако эти сведения о смертности от COVID-19 во многих странах вызывают у исследо-

вателей сомнения из-за различий в доступе к тестированию, диагностических возможностей и непоследовательной сертификации COVID-19 как причины смерти [11].

В научном журнале *Nature* опубликована обновленная оценка ВОЗ глобальной избыточной смертности в результате COVID-19. По данным ВОЗ, в 2020 и 2021 гг. во всем мире было зарегистрировано около 14,8 млн дополнительных смертей. По оценкам, это почти в три раза превышает число официально зарегистрированных 5,4 млн смертей от COVID-19 за этот период [14; 10].

В связи с этим трудно оценить объективность заявления 5 мая 2023 г. главы ВОЗ доктора Тедроса Гебрейесуса о том, что решением Комитета по коронавирусной инфекции COVID-19 не представляет собой чрезвычайную ситуацию международного значения. То есть, авторитетная международная инстанция установила новый статус данной угрозы безопасности в качестве устойчивой и постоянной проблемы здравоохранения, а не чрезвычайной ситуации [3]. Вместе с тем пандемия привела к серьезным экономическим потрясениям, многим триллионам ущерба ВВП, ввергла миллионы людей в нищету. Пандемия вызвала серьезные социальные потрясения: закрытие границ, введение ограничений на передвижение, пробелы в образовании, изоляцию, тревогу и депрессию. Прав Т. Гебрейесус в том, что «худшее, что сегодня может сделать любая страна – это ослабить бдительность» [ibid.].

Дискуссии о роли Всемирной организации здравоохранения и науки в обеспечении безопасности здоровья человека в условиях масштабных вирусных инфекций

Изучение проблем предупреждения и преодоления масштабных (глобальных) вирусных инфекций, как показывает анализ научной литературы, находится в центре внимания многих ученых, и не только микробиологов и генетиков, но и юристов, социологов и др. Так, по мнению профессора МГЮА В.А. Батыря, «в настоящее время в связи с пандемией коронавирусной инфекции (COVID-19) все более ощутимой стала потребность в принятии неотложных дополнительных мер в сфере международно-правового регулирования медико-санитарной безопасности». Сложилась парадоксальная ситуация, утверждает ученый: с одной стороны, существует понимание угрозы глобальной безопасности, а с другой – наличие серьезного пробела в правовом регулировании взаимодействия государств в борьбе с опасными инфекцион-

ными заболеваниями. Многочисленные правила-рекомендации оказались малоэффективны в период быстрого распространения коронавирусной инфекции [2, с. 107–108]. Проанализировав деятельность отдельных государств и ВОЗ в период пандемии, В.А. Батырь предлагает создать комитет по опасным инфекционным заболеваниям, разработать новую международную конвенцию о борьбе с опасными инфекционными заболеваниями, развивать международное медицинское право как комплексный международно-правовой институт [там же].

Кристофер Лонг, научный сотрудник Центра глобальной политики в области здравоохранения на факультете международных отношений Университета Сассекса (Великобритания), считает, что после публикации пересмотренных Международных медико-санитарных правил (далее – ММСП) 2005 г. значительно расширились полномочия ВОЗ и сфера применения этих Правил. В них предусмотрены обязательства государств – членов ВОЗ по развитию минимального базового потенциала эпиднадзора и реагирования. Эпиднадзор за общественным здравоохранением – одна из (вновь) открытых областей юридических исследований. Его задачей является – непрерывный, систематический сбор, анализ и интерпретация данных, связанных со здоровьем, отслеживание заболеваний и контактов людей в условиях пандемии [13, р. 493–495].

Всемирная организация здравоохранения, согласно ММСП, имеет большие полномочия, в том числе объявлять вспышку заболевания чрезвычайной ситуацией в области общественного здравоохранения международного значения (*Public Health Emergency of International Concern*) (далее – РНЕИС). Определение и объявление существования РНЕИС рассматривается исследователями как новая возможность обеспечения безопасности вспышек инфекционных заболеваний. Посредством объявления РНЕИС страны информируют мир о том, что вспышка заболевания представляет собой чрезвычайное событие и представляет риск для общественного здравоохранения, который требует применения чрезвычайных мер, включая усиление эпиднадзора за заболеваниями, карантин, закрытие границ, введение планов готовности к пандемии и экстренное использование новых вакцин или терапевтических средств. Своевременное объявление вспышки заболевания чрезвычайной ситуацией значительно повышает уровень поддержки со стороны международного сообщества, включая финансовые ресурсы, активизацию дипломатических усилий и обеспечение безопасности [ibid.].

Вместе с тем, как подчеркивает К. Лонг, неспособность ВОЗ последовательно применять PHEIC привела к критике его деятельности, поставило под сомнение эффективность международного права в области здравоохранения, что обусловило необходимость разработки нового договора о борьбе с пандемией [Ibid.].

В своей статье К. Лонг уделяет значительное внимание теории и логике обеспечения безопасности Копенгагенской школы, в том числе в области международного общественного здравоохранения, а также роли науки в процессе обеспечения безопасности. Автор выделяет две ключевые динамики, благодаря которым генетические технологии смогли сыграть такую важную роль в объявлении PHEIC. Во-первых, в отношении H1 N 1, Эболы и SARS-CoV-2 эти технологии выявили новые молекулярные характеристики и распространенность этих вирусов в популяциях, которые сделали их объектами познания. Этот процесс объективизации привел к их категоризации и разработке комплекса мер по безопасности от угрозы, которую они представляют для здоровья людей. Во-вторых, доказательства по всем трем случаям были собраны Генеральным директором ВОЗ и Комитетом по чрезвычайной ситуации для поддержки их программы обеспечения безопасности и объявления PHEIC. В настоящее время научные данные, предоставляемые генетическими технологиями, играют необходимую и важнейшую роль в обеспечении безопасности вспышек инфекционных заболеваний посредством объявления ВОЗ PHEIC [13].

Аника Клафки, исследователь из Юридического факультета Йенского университета имени Фридриха Шиллера (Германия), также считает жизненно важной задачей – анализ изменений, происходящих в генетическом составе вирусов, циркулирующих по всему миру. По мнению автора, главную роль здесь должна играть сеть лабораторий ВОЗ. Их круглогодичный эпиднадзор за сезонным гриппом является основой глобальной системы вирусологического эпиднадзора и ее способности реагировать на пандемию [12].

Для принятия обоснованных решений в отношении вирусов гриппа с пандемическим потенциалом в рамках системы ВОЗ производятся глобальные оценки риска такого типа вируса. Эти оценки используются не только для определения опасности, которую представляет вирус, но также для разработки праймеров для эпиднадзора и диагностических инструментов и тестов, которые могут определить, инфицирован ли человек определенным вирусом, и таким образом сделать измеримыми и видимыми показатели инфицирования среди населения. Такие точные и комплексные диаг-

ностические инструменты имеют центральное значение для эпиднадзора за появляющимися и рецидивирующими вирусами, управления вспышками, а также для раннего противовирусного лечения, профилактики и инфекционного контроля [12].

Всемирная организация здравоохранения разработала руководство для стран по внедрению сети органов эпиднадзора, которые могли бы не только отслеживать распространение вируса среди населения, но и фиксировать изменяющиеся характеристики вирусного генома, что было сделано при выявлении новых его вариантов, обозначенных Альфа, Бета, Гамма, Дельта и Омикрон [ibid.].

Таким образом, исследователи роли и функционирования ВОЗ в период COVID-19 высказывают как критические замечания относительно ее деятельности, так и конкретные предложения и рекомендации ВОЗ и органам здравоохранения национальных государств по предупреждению вирусных инфекций глобального масштаба.

Международное сотрудничество государств в борьбе с пандемиями

Пандемия COVID-19 наглядно продемонстрировала, что международного сотрудничества в борьбе с этой всеохватывающей вирусной эпидемией было явно недостаточно. Ученые отмечают также отсутствие глобальной солидарности и справедливого распределения медицинских ресурсов [11; 12]. Пренебрегая обязательствами по ММСП в отношении международной помощи и сотрудничества, государства в значительной степени вернулись к изоляционистской политике, геополитической конкуренции и глобальному пренебрежению, что, по мнению исследователей, подрывало скоординированные ответные меры, поставило под угрозу поддержку ВОЗ и привело к неравенству в отношении вакцин. Кроме того, международная реакция на разворачивающуюся пандемию COVID-19 выявила серьезные ограничения в обязательствах по ММСП (и соблюдении их государствами), необходимых для формирования эффективного совместного реагирования на глобальные чрезвычайные ситуации в области общественного здравоохранения [11, p. 503–507].

Причины явного отсутствия солидарности развитых стран со странами со средним и низким уровнем дохода, на взгляд А. Клафки, кроются в механизмах подотчетности и контроля в гло-

бальной системе здравоохранения. На международном праве в области здравоохранения по-прежнему сказывается национальный эгоизм многих государств, что снижает глобальную эффективность борьбы с пандемиями.

Таким образом, принципы равенства и солидарности лежат в основе текущих реформ, заключает автор [12].

COVID-19 также выявил отсутствие ясности в отношении обязательств государств и политической воли следовать рекомендациям общественного здравоохранения, недостаточность реальной ответственности за нарушение ММСП. Все это ослабляло руководство ВОЗ в условиях пандемии.

В связи с этим в постковидный период широко обсуждается вопрос укрепления полномочий ВОЗ по руководству международными мерами реагирования на новые вспышки вирусных заболеваний. Лоуренс О. Гостин, профессор Джорджтаунского университета, директор Центра ВОЗ по национальному и глобальному здравоохранению, Бенджамин Мейсон Мейер, профессор глобальной политики в области здравоохранения в Университете Северной Каролины, и Барбара Стокинг, старший научный сотрудник Института национального и глобального здравоохранения имени О'Нил, в своем исследовании «Разработка инновационного договора о борьбе с пандемией для укрепления глобальной безопасности в сфере здравоохранения» [11] подчеркивают: «Пандемия как никогда ранее проверила лидерские качества ВОЗ. Хотя международное право в области здравоохранения зависит от эффективного управления, ВОЗ не смогла обеспечить глобальной солидарности на протяжении всей пандемии, поскольку ей не хватает юридических полномочий и финансовых ресурсов для эффективной координации ответных мер общественного здравоохранения. Не имея возможности независимо проверять отчеты государств, инспектировать обстановку на местах или привлекать государства к ответственности, ВОЗ временами оказывалась в затруднительном положении, прибегая к “мягкой силе” для руководства мерами глобального здравоохранения» [11].

Эти недостатки в руководстве ВОЗ авторы статьи ставят под сомнение, как и сохраняющуюся эффективность международного права в области здравоохранения. Они поддерживают идею разработки нового договора о борьбе с пандемией [ibid.].

Реформа Международных медико-санитарных правил 2005 г.

Опираясь на опыт борьбы с пандемией COVID-19, в 2022 г. ВОЗ решила провести реформу основного правового документа в области общественного здравоохранения – Международных медико-санитарных правил 2005 г. Эти Правила признаются основным юридическим документом, обеспечивающим глобальную безопасность в области здравоохранения. Они основаны на ст. 21(а) Устава ВОЗ. Согласно ст. 22 Устава ВОЗ, нормативные акты, принятые в соответствии со ст. 21 Устава ВОЗ, являются юридически обязательными для всех членов после надлежащего уведомления об их принятии, если только государства-члены прямо не отвергнут их или не сформулируют оговорки в установленный срок [12].

Кроме того, Всемирная ассамблея здравоохранения (далее – ВА3) разрабатывает новое соглашение (договор) о борьбе с пандемиями для дальнейшего укрепления международного сотрудничества. В этих целях на специальной сессии ВА3 в декабре 2021 г. был учрежден Межправительственный переговорный орган, которому было поручено провести переговоры по конвенции, соглашению и другим документам ВОЗ, касающимся профилактики пандемий и обеспечения готовности и реагирования на них.

Л.О. Гостин, Б.М. Мейери и Б. Стокинг, признавая пробелы в ММСП, особенно в том, что касается производства необходимого оборудования, лекарств и вакцин, а также в обеспечении доступа к ним, приветствуют принятие ВА3 договора, который укрепит ВОЗ, наделит его новыми полномочиями по мобилизации финансовых ресурсов для борьбы с пандемией. Учитывая, что ММСП сосредоточены на выявлении вспышек, а не на профилактике заболеваний, ученые настаивают на том чтобы основной мандат договора о пандемии включал «глубокую профилактику», обеспечивал жизненно важную перспективу «единого здравоохранения» (особенно в отношении зоонозных заболеваний) и уделял особое внимание первичным детерминантам вспышек заболеваний. Помимо этих ключевых положений исследователи признают, что основой такого договора должны служить фундаментальные принципы равенства, подотчетности и права человека [11].

Возможность разработки новых международных норм в области пандемических угроз, по мнению Педро А. Вильярреал, сотрудника Немецкого института международных отношений и безопасности и Института сравнительного публичного права и международного права им. Макса Планка (Германия), актуализи-

рует нормативные дебаты по использованию инструментов эпиднадзора за здоровьем в разных странах. Однако возникает вопрос: будут ли новые правила учитывать многочисленные соображения ученых, связанные с отслеживанием заболеваний и контактов, который еще предстоит выяснить [15].

В результате реформы в МССП появилось юридическое определение «чрезвычайная ситуация, связанная с пандемией». Это новая, более высокая категория предупреждений в рамках чрезвычайных ситуаций общественного характера, вызывающих обеспокоенность международного сообщества. В дополнение к требованиям, предъявляемым к чрезвычайным ситуациям, представляющим международный интерес, категория «чрезвычайная ситуация, связанная с пандемией» предполагает, что она вызвана инфекционным заболеванием и сопряжена как минимум с высоким риском географического распространения на территории нескольких государств и внутри них, с превышением возможностей системы здравоохранения в затронутых государствах, с существенными социальными и / или экономическими потрясениями. Такая ситуация требует быстрых, справедливых и усиленных скоординированных международных действий с привлечением всего общества, международных организаций и правительств стран. Однако, по мнению П. Вильярреала, этот новый термин имеет скорее политическое, а не юридическое значение в действующей системе регулирования ВОЗ [15].

Новые поправки к МССП, считает А. Клапки, направлены на укрепление принципов равенства и солидарности. ВОЗ определяет равенство в отношении здоровья как отсутствие несправедливых, предотвратимых или устранимых различий между группами людей. Равенство в отношении здоровья достигается, когда каждый может полностью реализовать свой потенциал в области здоровья и благополучия [12].

Всемирная организация здравоохранения не дает четкого определения солидарности. Однако из использования этого термина в документах ВОЗ можно сделать вывод, что *солидарность* подразумевает международное сотрудничество для достижения глобального равенства в сфере здравоохранения. Солидарность в международном праве не ограничивается гуманитарной помощью, а понимается в широком смысле, как устойчивые международные отношения и справедливое распределение выгод и бремени. Тем не менее особое внимание уделяется международной помощи странам с низким уровнем дохода. С этой целью ключевым эле-

ментом реформы МССП является создание координационного финансового механизма для укрепления финансового сотрудничества между государствами-участниками и обеспечения эффективного использования средств для наращивания потенциала в области медицины в соответствии со ст. 5 МССП, чтобы все государства могли выполнять существующие обязательства по надзору, обмену информацией и контролю [ibid.].

Кроме того, ВОЗ уполномочена оказывать поддержку государствам-членам и координировать международные ответные меры в чрезвычайных ситуациях в области общественного здравоохранения, имеющих международное значение, в том числе в чрезвычайных ситуациях, связанных с пандемиями. ВОЗ должна в первую очередь содействовать справедливому доступу к соответствующим медицинским товарам посредством консультаций, координационных мероприятий, через сети ВОЗ и путем обмена соответствующей информацией. К соответствующим медицинским товарам относятся товары, необходимые для реагирования на чрезвычайные ситуации в области общественного здравоохранения, имеющие международное значение. Они могут включать в себя лекарства и вакцины, а также средства индивидуальной защиты или генные технологии.

Наконец, пересмотренные МССП положения направлены на усиление ответственности государств-участников за выполнение своих обязательств. Для этого государства-члены обязаны создать национальные органы по координации реализации правил, предусмотренных МССП. Кроме того, предусмотрено создание Комитета по реализации, который будет собираться не реже одного раза в два года для более эффективного отслеживания реализации правил и усиления ответственности.

В ходе внесения изменений в МССП была утверждена схема принятия решений о признании чрезвычайной ситуации в области общественного здравоохранения, имеющей международное значение (Приложение 2 к МССП). В целях улучшения выявления всплеск острых респираторных заболеваний и информирования о них, теперь предписано, что группы случаев тяжелых острых респираторных заболеваний неизвестной или новой этиологии должны приводить к применению схемы принятия решений (называемой «алгоритмом»), чтобы национальные органы могли решить, нужно ли уведомлять ВОЗ об этом событии [12].

Таким образом, при определении конкретных стратегий профилактики будущих пандемий и реагирования на них, по мне-

нию А. Клафки, международный договор или глобальная конвенция в области здравоохранения предоставляют уникальную возможность сформулировать ключевые обязательства государств, предусматривающие строгое соблюдение и механизмы подотчетности в отношении здоровья населения. В рамках комплексного подхода «единое здоровье» во всех секторах – новый международный договор, полагает автор, может снизить вероятность встречающихся в природе новых угроз [12].

Вместе с тем, несмотря на то что реформа МСП движется в правильном направлении, она, полагает А. Клафки, не решает существующих проблем, связанных с фундаментальным конфликтом интересов между бедными и богатыми государствами. Страны с высоким уровнем дохода, с одной стороны, крайне заинтересованы в том, чтобы обязательства по наращиванию потенциала и предоставлению отчетности были с высокой степенью ответственности исполнены всеми государствами, чтобы защитить собственное население от будущих пандемий. С другой стороны, более бедные государства считают себя жертвами. Если они выполняют свои обязательства по предоставлению отчетности и обмену информацией о вирусах, то несут значительные финансовые потери из-за чрезмерных ограничений передвижения населения, на приобретение вакцин и других медицинских товаров. Поэтому они требуют более четких правил распределения выгод от соответствующих медицинских товаров, а также более высокой подотчетности и большей обязательности ВОЗ [ibid.].

Так называемое «пандемическое соглашение» еще предстоит ратифицировать, но, по мнению исследователей, оно обладает гораздо большим потенциалом для улучшения глобального управления в условиях пандемии в будущем, так как его основная цель – способствовать применению межправительственного и общесоциального подхода, укреплять национальный, региональный и глобальный потенциал и повышать устойчивость к будущим пандемиям¹.

Важными элементами этого соглашения являются повышение уровня готовности к пандемии за счет совершенствования систем эпиднадзора, лабораторных сетей и инфраструктуры общест-

¹ WHO: COVID-19 shows why united action is needed for more robust international health architecture. – URL: <https://www.who.int/news-room/commentaries/detail/op-ed---covid-19-shows-why-united-action-is-needed-for-more-robust-international-health-architecture> (дата обращения: 15.10.2025).

венного здравоохранения во всех странах. Кроме того, частью соглашения является концепция «Единое здравоохранение», а также общегосударственный и общесоциальный подход. Ключевым руководящим и контролирующим органом «пандемического соглашения», считает А. Клафки, является не Всемирная ассамблея здравоохранения, а Конференция сторон, в которой каждое государство – участник этого соглашения – имеет один голос [12].

Российское законодательство в условиях возникновения опасных пандемий

Российские исследователи рассматривают возникновение опасных инфекционных заболеваний, эпидемий и пандемий как природно-биологические (природно-социальные, биосоциальные и т.п.) явления, которые до сих пор не имеют единой классификации, критериев и точного нормативного определения в федеральном законодательстве, а также в ведомственных нормативных правовых актах, регулирующих деятельность органов публичной власти и органов здравоохранения в предупреждении и ликвидации чрезвычайных ситуаций. На данное обстоятельство обращают внимание исследователи, изучающие актуальные проблемы управления в условиях чрезвычайных ситуаций, механизм обеспечения конституционных прав граждан в период пандемии, гибридный характер угрозы системе прав человека в период пандемии COVID-19 и при установлении уголовной и административной ответственности в условиях ограничений, связанных с пандемией, и др. [4; 1; 6; 7; 8].

Как отмечают В.В. Головки и А.И. Сахно, при разработке структуры и базовых положений Федерального закона от 21.12.1994 № 68-ФЗ (действует в ред. от 08.08.2024) «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» законодателем вообще не были учтены особенности предупреждения и ликвидации чрезвычайных ситуаций биологического характера. Поэтому источники возникновения чрезвычайных ситуаций биологического характера – инфекционные заболевания, представляющие опасность для окружающих (как разновидность опасных природных явлений), появились только в 2020 г. в период пандемии COVID-19, – что было продиктовано прежде всего необходимостью обеспечить законность применения режима повышенной готовности и мер государственного принуждения в условиях сложной эпидемиологической обстановки.

Анализ содержания этого Закона свидетельствует об отсутствии иных правовых норм, предназначенных для предупреждения и ликвидации чрезвычайных ситуаций биологического характера [4, с. 99].

Федеральным законом, подчеркивают авторы, детально не определены и не разграничены понятия «карантин» и «ограничительные мероприятия», «самоизоляция» и др., нарушение которых влечет наступление юридической ответственности и ограничение прав граждан. Несовершенство правовых конструкций и противоречивость ст. 6.3, 20.6.1, 10.1–2, 13.15 КоАП РФ создают, по их мнению, почву для конкуренции с нормами уголовного права, например с нормами ст. 207.1, 207.2, 236 УК РФ, и требуют правовых новелл с целью их доработки и согласования, на что обоснованно обращают внимание многие исследователи [там же].

Комплексный анализ актуальных проблем теории и практики применения российского законодательства, изучение зарубежного опыта позволяют определить основные направления совершенствования российского законодательства о санитарно-эпидемиологическом благополучии населения. К таковым В.В. Головкин и А.И. Сахно предлагают отнести: 1) совершенствование законодательства о защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера в мирное время, о санитарно-эпидемиологическом благополучии населения, о биологической безопасности, а также о применении мер публичного принуждения с учетом опыта пандемии COVID-19. Согласование и систематизация ведомственной нормативной базы по всем аспектам взаимодействия во время предупреждения, локализации и ликвидации последствий эпидемиологических угроз; 2) разработку и формирование правовых основ системы государственного управления в чрезвычайных ситуациях биологического характера с учетом требований стратегического планирования и опыта работы временных гибких структур управления по координации и предупреждению угроз возникновения и распространения опасных инфекционных заболеваний; 3) создание механизма правового регулирования стратегического планирования деятельности субъектов РФ по обеспечению биологической безопасности подведомственных территорий и санитарно-эпидемиологическому благополучию населения; 4) развитие национального законодательства о санитарно-эпидемиологическом благополучии населения в области международного сотрудничества; 5) кодификацию законодательства о санитарно-эпидемиологическом благополучии населения с учетом новых целей и задач стратегии обеспечения биологической

безопасности, опыта применения отечественных и Международных медико-санитарных правил в условиях пандемии [4, с. 101].

Заключение

Несмотря на то что дискуссии экспертов и ученых о постковидной оценке и анализе деятельности ВОЗ и реформировании международного права и внутригосударственного законодательства в сфере здравоохранения продолжают и приносят свои плоды – совершенствуются международный режим здравоохранения и национальное законодательство о пандемиях, ключевой задачей остается готовность к глобальным вирусным инфекциям, их предотвращение и реагирование на них. Ее можно решить, только если все страны будут работать сообща, эффективно и результативно. Горький опыт пандемии COVID-19 показал, что только за счет наращивания потенциала в области здравоохранения в странах со средним и низким уровнем дохода можно остановить распространение новых инфекций до того, как они перерастут в пандемию. Только при своевременном поступлении вакцин и медицинских препаратов в места вспышек можно предотвратить распространение болезни. И только при достижении достаточного уровня вакцинации во всем мире можно снизить риск появления новых вариантов вируса, которые смогут преодолеть существующую защиту от вакцин.

Таким образом, строгое соблюдение обязательств, предусмотренных пересмотренными Международными медико-санитарными правилами, и справедливое распределение ресурсов – это не только вопрос равенства и солидарности. Скорее, это вопрос укрепления здоровья человека, сохранения его жизни, и касается он каждого жителя на нашей планете Земля. Общий лейтмотив изученных в ходе подготовки данного обзора источников заключается в следующем утверждении, выраженном А. Клапки: «Если идея о глобальном здравоохранении как об общем благе станет общепринятой, появится шанс, что следующая пандемия станет поводом для реальных коллективных действий» [12, р. 751].

Список литературы

1. Алимов А.А. К вопросу об истории развития международно-правового регулирования противодействия угрозе распространения инфекционных заболе-

- ваний // Правопорядок: история, теория, практика. – 2023. – № 3. – С. 143–150. – DOI: 10.47475/2311–696 X-2023–38–3-143–150
2. Батырь В.А. Разработка международной конвенции о борьбе с опасными инфекционными заболеваниями – требование современности // *Lex russica*. – 2020. – Т. 73, № 8. – С. 106–123. – DOI: 10.17803/1729–5920.2020.165.8.106–123.
 3. ВОЗ: COVID-19 больше не является чрезвычайной ситуацией международного значения // Официальный сайт ООН. – URL: <https://news.un.org/ru/story/2023/05/1440702?ysclid=mhjgvdkdik13243854> (дата обращения: 20.10.2025).
 4. Головкин В.В., Сахно А.И. Основные направления совершенствования законодательства о санитарно-эпидемиологическом благополучии населения Российской Федерации // *Правоприменение*. – 2023. – Т. 7, № 2. – С. 96–104. – DOI 10.52468/2542–1514.2023.7(2).96–104
 5. Кашкин С.Ю., Тищенко С.А., Алтухов А.В. Правовое регулирование применения искусственного интеллекта для борьбы с распространением COVID-19: проблемы и перспективы с учетом мирового опыта // *Lex russica*. – 2020. – Т. 73, № 7. – С. 105–114. – DOI: 10.17803/1729–5920.2020.164.7.105–114
 6. Литовко К.С. Предотвращение распространения инфекционных заболеваний как гарантия конституционных прав на охрану здоровья и медицинскую помощь в Российской Федерации // *Правоприменение*. – 2023. – Т. 7, № 2. – С. 105–115. – DOI 10.52468/2542–1514.2023.7(2).105–115
 7. Маличенко В.С. Международно-правовые механизмы противодействия чрезвычайным ситуациям в сфере здравоохранения // *Право. Журнал Высшей школы экономики*. – 2021. – № 1. – С. 174–197. – DOI: 10.17323/2072–8166.2021.1.174.197
 8. Мошников Д.К. Становление и развитие международно-правового противодействия инфекционным заболеваниям // *Право. Журнал Высшей школы экономики*. – 2021. – № 1. – С. 198–217. – DOI: 10.17323/2072–8166.2021.1.198.217
 9. Digital Surveillance Trends and Chinese Influence in Light of the COVID-19 Pandemic / M.A. Germanò, Ava Liu J., Skebba B. Jili // *Asian Journal of Comparative Law*. – 2023. – Vol. 18, Special Issue 1: China's Global Capital and the Coronavirus: Views from Comparative Law and Regulation. – P. 91–115. – URL: <https://www.cambridge.org/core/journals/asian-journal-of-comparative-law/article/abs/digital-surveillance-trends-and-chinese-influence-in-light-of-the-covid-19-pandemic/205F0BB849AD4CFCA3E4F9C51F8B7B82> (дата обращения: 07.11.2025).
 10. Globale Übersterblichkeit durch COVID-19. – URL: <https://www.sciencemediacenter.de/angebote/22192> (дата обращения: 07.11.2025).
 11. Gostin L.O., Meier B.M., Stocking B. Developing an Innovative Pandemic Treaty to Advance Global Health Security // *Journal of Law, Medicine & Ethics*. – 2021. – Vol. 49, N 3: Malinger & Health Policy. – P. 503–508. – URL: <https://www.cambridge.org/core/journals/journal-of-law-medicine-and-ethics/article/abs/developing-an-innovative-pandemic-treaty-to-advance-global-health-security/9FAE425795D8B9DC129A49BFA0C7FA0D> (дата обращения: 07.11.2025).
 12. Klafki A. Post-Pandemic Reform Discussions in International Health Law: The Reform of the International Health Regulations and the New WHO Pandemic Agreement Proposal // *European Journal of Risk Regulation*. – 2025. – Vol. 16,

- N 2. – P. 744–752. – URL: <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/postpandemic-reform-discussions-in-international-health-law-the-reform-of-the-international-health-regulations-and-the-new-who-pandemic-agreement-proposal/40BA3DC878ACA8EAE545D9631F8FC64A> (дата обращения: 07.11.2025).
13. Long Ch. Securitising infectious disease outbreaks: The WHO and the visualisation of molecular life // *European Journal of International Security*. – 2023. – Vol. 8, N 4. – P. 493–512. – URL: <https://www.cambridge.org/core/journals/european-journal-of-international-security/article/securitising-infectious-disease-outbreaks-the-who-and-the-visualisation-of-molecular-life/75311840B08A09D7115BBFA07AAE375D> (дата обращения: 07.11.2025).
14. The WHO estimates of excess mortality associated with the COVID-19 pandemic / W. Msemburi, A. Karlinsky, V. Knutson, S. Aleshin-Guendel, S. Chatterji S., J. Wakefield // *Nature*. – 2023. – Jan., Vol. 613, N 7942. – P. 130–137. – URL: <https://pubmed.ncbi.nlm.nih.gov/36517599/> (дата обращения: 07.11.2025).
15. Villarreal P.A. International Law and Digital Disease Surveillance in Pandemics: On the Margins of Regulation // *German Law Journal*. – 2023. – Vol. 24, Special Issue 3: International Law and Digitalization. – P. 603–617. – URL: <https://doi.org/10.1017/glj.2023.26> (дата обращения: 07.11.2025).

КАРЦХИЯ А.А.¹ ЭНЕРГОБЕЗОПАСНОСТЬ КАК ФАКТОР НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Аннотация. В статье анализируются особенности и современное состояние энергобезопасности на основе сравнительного исследования этого института в России и за рубежом. Энергобезопасность, устойчивость и антитеррористическая защищенность топливно-энергетического комплекса (ТЭК) являются ключевыми аспектами обеспечения стабильного функционирования энергетической системы российского государства. Комплексный подход к обеспечению энергетической безопасности должен выходить за рамки традиционных подходов и охватывать безопасную трансформацию энергетического сектора и устойчивость цепочек поставок экологически чистой энергии. Автор приходит к выводу о том, что энергетическая безопасность в современных условиях представляет собой состояние защищенности экономики и населения страны от угроз национальной безопасности в сфере энергетики.

Ключевые слова: энергобезопасность; устойчивость энергетики; возобновляемые источники энергии; энергетическая трилемма; энергоэффективность; национальная безопасность; декарбонизация; топливно-энергетический комплекс.

KARTSKHIYA A.A. Energy security as a factor of national security

Abstract. The article analyzes the features and current state of energy security based on a comparative study of this institute in Russia and abroad. Energy security, sustainability and anti-terrorist security of the fuel and energy are key aspects of ensuring the stable functioning of the energy system of the Russian state. An integrated approach to energy security should go beyond traditional approaches and encompass

¹ © Карцхия Александр Амиранович, профессор РГУ нефти и газа (НИУ) имени И.М. Губкина, доктор юридических наук, доцент.

the safe transformation of the energy sector and the sustainability of clean energy supply chains. The author comes to the conclusion that energy security in modern conditions is a state of protection of the economy and the population of the country from threats to national security in the energy sector.

Keywords: energy security; energy sustainability; renewable energy sources; energy trilemma; energy efficiency; national security; decarbonization; fuel and energy complex.

Для цитирования: Карцхия А.А. Энергобезопасность как фактор национальной безопасности (Статья) // Социальные и гуманитарные науки: Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2026. – № 1. – С. 76–89. – DOI: 10.31249/iajpravo/2026.01.05

Введение

В начале XXI в. появилось принципиально новое понятие в области безопасности – *энергетическая безопасность*. Это комплексное явление не только охватывает стабильные поставки энергоресурсов для национальных экономик, но также обеспечивает свободный доступ зарубежных производителей к внутренним рынкам стран-импортеров.

Сегодня обеспечение энергетической безопасности стало важнейшим глобальным приоритетом, без которого невозможно стабильное развитие государств. Для решения этой задачи Мировой энергетический совет создал концепцию «энергетической трилеммы», состоящую из трех ключевых компонентов:

1) *безопасность энергоснабжения* – подразумевает надежную организацию поставок энергии как из внутренних, так и из внешних источников, стабильную работу инфраструктуры и способность удовлетворить текущий и будущий спрос;

2) *справедливое распределение* – гарантирует достаточное количество доступной энергии для всех слоев населения;

3) *экологическая ответственность* – включает эффективное использование энергоресурсов и развитие «зеленых» технологий, в том числе переход к возобновляемым источникам энергии.

В современных условиях особую роль играет государственное регулирование в сфере энергетики. Оно направлено на достижение баланса между тремя основными целями: 1) формирование устойчивой, энергоэффективной и экологически чистой энергетической системы; 2) обеспечение доступности энергоресурсов по

приемлемым ценам для потребителей; 3) поддержание надежных поставок энергетических ресурсов для гарантированной безопасности.

Современное понимание энергетической безопасности

Энергетическая безопасность – многогранное понятие, которое традиционно включает три ключевых аспекта: стабильное обеспечение потребителей энергоресурсами, доступные цены на энергоносители, экологичность способов производства и доставки энергии.

Исторически сложилось так, что энергетическая безопасность строилась на балансе интересов двух групп стран. Страны-импортеры заинтересованы в надежности поставок энергоресурсов и приемлемом ценовом уровне. Страны-экспортеры, в свою очередь, стремятся к гарантированному спросу на свою продукцию, справедливой оплате за поставляемые энергоресурсы и наличию достаточного спроса для окупаемости крупных энергетических проектов.

Существует несколько фундаментальных условий, обеспечивающих энергетическую безопасность: ценовая доступность энергоресурсов для промышленности и населения; экологическая безопасность производства и потребления энергии, включая меры по снижению углеродного следа; стабильность поставок, устойчивость к различным угрозам (природные катастрофы, военные конфликты, террористические акты); разнообразие источников энергоресурсов через расширение базы поставщиков; соответствие предложения текущему спросу.

Комплексный подход к энергетической безопасности объединяет три основных компонента: 1) доступность ресурсов достигается через разнообразие видов топлива, развитие альтернативных технологий производства энергии и снижение зависимости от импорта; 2) ценовая доступность подразумевает обеспечение населения и предприятий энергоресурсами в рамках их финансовых возможностей и справедливое ценообразование; 3) эффективность использования включает оптимизацию работы энергетического оборудования, рационализацию потребления и минимизацию рисков политического, социального и экологического характера.

Таким образом, современная концепция энергетической безопасности направлена на создание устойчивой системы, обес-

печивающей баланс между экономическими, экологическими и социальными интересами всех участников энергетического рынка¹.

Место энергетической безопасности в достижении устойчивого развития

Энергетическая безопасность и устойчивое развитие – это два тесно связанных между собой направления, которые работают над созданием эффективной системы энергоснабжения. Их главная цель заключается в том, чтобы обеспечить потребителей энергией, которая будет надежной (бесперебойной и стабильной), доступной (по приемлемым ценам для всех категорий потребителей) и экологически безопасной (с минимальным негативным воздействием на окружающую среду). Достижение баланса между этими целями имеет решающее значение для экономической стабильности, защиты окружающей среды и социального благополучия. Энергетическая безопасность означает бесперебойное наличие источников энергии по приемлемой цене, обеспечивающих функционирование экономики и общества.

Энергетика имеет решающее значение для обеспечения высокого качества жизни и является основой реализации Повестки дня в области устойчивого развития на период до 2030 г. и соответствующих целей устойчивого развития (ЦУР), которая закреплена в резолюции Генеральной Ассамблеи ООН A/RES/70/1 от 25.09.2015 г. Устойчивая энергетика определяется на основе трех компонентов, охватывающих наиболее близкие к энергетике ЦУР, и в частности: а) энергетическая безопасность, т.е. обеспечение энергии, необходимой для экономического развития; в) энергетика для качества жизни, т.е. предоставление экономически доступной энергии, которая в любое время имела бы в наличии для всех; с) энергетика и окружающая среда, т.е. сведение к минимуму влияния энергетической системы на климат, экосистемы и здоровье человека.

В современном мире формируется инновационная экономическая модель, построенная на идеях устойчивого развития. Это

¹ Sustainable Energy Development: History of the Concept and Emerging Themes / L. Gunnarsdottir, B. Davidsdottir, E. Worrell, S. Sigurgeirsdottir // Renewable and Sustainable Energy Reviews. – 2021. – N 141; Карцхия А.А. Технологический суверенитет и энергетическая безопасность // Предпринимательское право. – 2024. – № 1. – С. 39–45.

привело к появлению принципиально нового подхода к обеспечению энергетической безопасности. В основе новой концепции лежит идея устойчивой энергетики, которая предполагает обеспечение населения необходимым объемом энергоресурсов, сохранение возможностей для энергопотребления будущих поколений и максимальное снижение негативного воздействия на экологию. Ключевым элементом этой системы становится гармоничное сочетание трех компонентов: эффективного использования энергетических ресурсов, защиты окружающей среды и обеспечения долгосрочного энергетического развития¹. Устойчивое развитие в энергетическом контексте предполагает минимизацию воздействия на окружающую среду, стимулирование использования возобновляемых ресурсов и обеспечение их доступности в долгосрочной перспективе. Устойчивая энергетическая безопасность объединяет обе концепции и направлена на предоставление энергетических услуг доступным, справедливым, эффективным и экологически безопасным способом в краткосрочной и долгосрочной перспективе. В ней рассматривается вся энергетическая система, включая предложение, спрос и три аспекта устойчивого развития: социальный, экономический и экологический.

В современном мире наблюдается активное развитие экологического направления в энергетической политике². Главной задачей этого направления является борьба с глобальным потеплением через переход к низкоуглеродной энергетике. Этот процесс, известный как энергетический переход, направлен на значительное уменьшение выбросов углекислого газа и стабилизацию уровня парниковых газов в атмосфере. Это необходимо для предотвращения негативных климатических изменений на Земле. Достижение этих целей осуществляется через комплекс мер, основанных на внедрении инновационных технологий, таких как повышение энергоэффективности и общее снижение энергопотребления в мировом масштабе; существенное сокращение использования ископаемого топлива и активное развитие и внедрение возобновляемых источников энергии.

¹ Локтионов В.И. Устойчивая энергетика: новый взгляд на факторы становления // *Мировая экономика и международные отношения*. – 2023. – Т. 67, № 8. – С. 16–25.

² Мастепанов А.М. Энергетический переход как новый вызов мировой нефтегазовой отрасли // *Энергетическая политика*. – 2019. – Вып. 2. – С. 62–69.

Примечательно, что эти меры не только способствуют решению экологических проблем, но и напрямую связаны с обеспечением энергетической безопасности. В результате эти два направления все чаще рассматриваются как взаимодополняющие и взаимосвязанные.

Основой успешного энергетического перехода становится развитие рынка современных технологий и оборудования. Ключевую роль здесь играет концепция трех «Д»: декарбонизация, децентрализация и диджитализация¹.

Как отмечают последние исследования², энергетика и устойчивое развитие по-прежнему тесно взаимосвязаны, поскольку выбросы углерода в результате потребления ископаемого топлива напрямую влияют на изменение климата. За 2024 г. выбросы достигли рекордно высокого уровня, что еще больше увеличило разрыв в ограничении повышения глобальной температуры – на 1,5°C по сравнению с доиндустриальным уровнем, что является одной из центральных целей Парижского соглашения по климату 2015 г. Несмотря на прогнозируемое снижение выбросов к 2050 г., оценки выбросов превышают целевые показатели «чистого нуля» и существенно снизятся только после 2030 г. Ископаемые виды топлива сохраняют значительную долю в структуре энергопотребления после 2050 г.

Следует признать, что за последние десятилетия энергетический ландшафт значительно изменился, в том числе благодаря стремлению стран мира «декарбонизировать» свои энергетические системы, чтобы справиться с последствиями изменения климата. Еще в 1990 г. возобновляемые источники энергии составляли всего 3% от общего объема мировой энергетики. С 2000 г. ежегодные темпы роста использования возобновляемых источников энергии неизменно превышают темпы роста всех других видов энергии. С 2006 г. темпы их роста в среднем примерно в четыре раза превышали среднегодовые темпы роста общего мирового спроса на энергию. За последние пять лет этот показатель увеличился более

¹ Стенников В. Устойчивое развитие энергетики: тенденции и вызовы // Энергетическая политика. – 2023. – № 2. – С. 32–39.

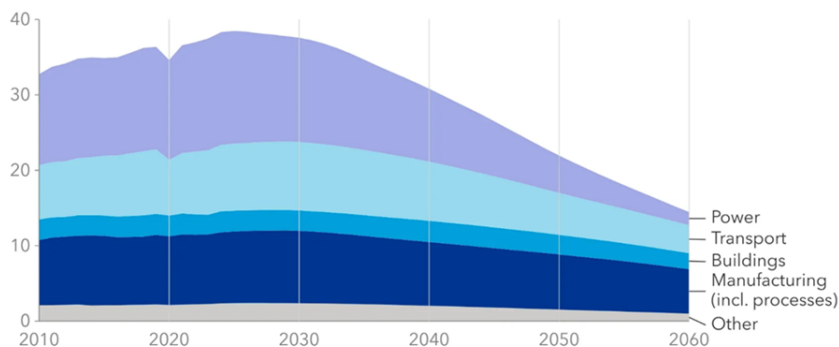
² Global Energy Outlook 2025: Headwinds and Tailwinds in the Energy Transition: Report / Yuqi Zhu, D. Raimi, E. Joiner, B. Holmes, B.C. Prestio. – 2025. – URL: <https://www.rff.org/publications/reports/global-energy-outlook-2025/>; McKinsey's Global Energy Perspective. – 2025. – URL: <https://www.mckinsey.com/industries/energy-and-materials/our-insights/global-energy-perspective> (дата обращения: 10.10.2025).

чем в пять раз¹. Использование ископаемого топлива тоже растет, но не так быстро. Глобальные выбросы парниковых газов медленно сокращаются. Распределение глобальных выбросов углекислого газа по отраслям приведены в *таблице 1 (World CO₂ emission by sector (GtCO₂/yr))*.

Таблица 1

World CO₂ emissions by sector (GtCO₂/yr)

DNV Energy Transition Outlook 2025



HIGHLIGHT 5 |

**Концепция энергетической безопасности
в зарубежных странах**

В современных зарубежных доктринах энергетическая безопасность получает более широкое толкование. Энергетическая безопасность тесно связана с экономической безопасностью, характеристика которой приводится, как правило, по критериям оценки рисков безопасности. К примеру, в Стратегии европейской экономической безопасности (European Economic Security Strategy)² определены такие категории рисков, как риски в цепочках поставок, риски безопасности и риски милитаризации, экономической зависимости или экономического принуждения. Европейская

¹Energy Institute Statistical Review of World Energy. – 2025. – URL: <https://www.energyinst.org/statistical-review> (дата обращения: 10.10.2025).

²Joint Communication to the European Parliament, the European Council and the Council on “European Economic Security Strategy”, EC, 2023. – URL : <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020> (дата обращения: 10.10.2025).

стратегия предусматривает подход к снижению рисков посредством содействия развитию экономической инфраструктуры, конкурентоспособности и роста, защиты от рисков экономической безопасности и сотрудничества в вопросах экономической безопасности.

Энергетическая безопасность часто определяется решением экологических вопросов в сфере «зеленой» энергетики, широкого применения возобновляемых энергетических ресурсов (энергии солнца, ветра, воды и т.п.), реализации задач энергетического перехода от ископаемых к возобновляемым источникам энергии (ВИЭ), решения вопросов климатической повестки в соответствии с Парижским соглашением по климату 2015 г.¹ Особенно активно решаются эти вопросы в документах ЕС. Так, Европейская стратегия (The European Green Deal)² была принята как долгосрочная стратегия роста ЕС, направленная на достижение климатической нейтральности к 2050 г. и формирование политики ЕС в области климата, энергетики, транспорта и налогообложения в целях сокращения чистых выбросов парниковых газов не менее чем на 55% к 2030 г. по сравнению с уровнем 1990 г. Стратегия также предусматривает увеличить обязательный целевой показатель доли ВИЭ в энергобалансе ЕС до 40% и добиться общего сокращения конечного и первичного потребления энергии на 36–39% к 2030 г. Европейское климатическое законодательство (European Climate Law)³ устанавливает, в частности, рамки для достижения климатической нейтральности в ЕС (т.е. баланса между общеевропейскими выбросами парниковых газов и их устранением, регулируемым законодательством ЕС) к 2050 г. и к отрицательным выбросам в ЕС в последующий период.

В условиях геополитической нестабильности Великобритания заявила о создании энергетической безопасности и энергетической независимости страны, необходимости стать независимым,

¹ The geopolitics of the European Green Deal // International Organisations Research Journal / M. Leonard, J. Pisani-Ferry, J. Shapiro, S. Tagliapietra, G. Wolff. – 2021. – Vol. 16, N 2. – P. 204–235.

² The European Green Deal. – URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en#actions (дата обращения: 10.10.2025).

³ Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 Establishing the Framework for Achieving Climate Neutrality and Amending Regulations (EC) No 401/2009 and (EU) 2018/1999 ('European Climate Law'). – URL: <https://eur-lex.europa.eu/EN/legal-content/summary/european-climate-law.html> (дата обращения: 20.10.2025).

безопасным и устойчивым к последствиям политических потрясений государства, что нашло свое отражение в Стратегии энергетической безопасности Британии (British energy security strategy)¹, Национальном плане энергетической безопасности (Powering Up Britain – Energy Security Plan) и новом Законе об энергетике Великобритании 2023 г. (The Energy Act).

В США подходы к энергобезопасности подчеркивают все более широкий идеологический раскол между администрацией США и правительствами многих других западных стран в отношении глобальной энергетической политики и могут повлиять на международное сотрудничество и внутренние энергетические стратегии. В 2025 г. администрация Президента США определила, что энергетическая безопасность находится на стыке проблем изменения климата, геополитики и национальной безопасности. Модернизация энергосистемы – важнейший шаг на пути к повышенной устойчивости, достижению целевых показателей по выбросам и укреплению энергетической безопасности. Главная задача – обеспечение критически важной энергетической безопасности страны, что подразумевает, с позиции Министерства энергетики США, укрепление режима нераспространения ядерного оружия и обеспечение безопасности арсенала ядерного оружия США, управление Стратегическим нефтяным резервом и защите энергетической инфраструктуры США от кибератак и физических нападений, реализацию программы по обеспечению здоровья и безопасности работников, а также организацию обучения по реагированию на чрезвычайные ситуации и обеспечению готовности к ним². Вместе с тем, как отмечают эксперты³, для сохранения своей сжимающейся ниши в мировой экономике с начала нынешнего века США проводят целенаправленную политику по устранению ЕС из глобальной конкуренции как самого слабого звена.

¹ British energy security strategy 2022. – URL: <https://www.gov.uk/government/publications/british-energy-security-strategy> (дата обращения: 20.10.2025).

² Declaring a National Energy Emergency / The White House. – 2025. – 20 Jan. – URL: <https://www.whitehouse.gov/presidential-actions/2025/01/declaring-a-national-energy-emergency/> (дата обращения: 20.10.2025).

³ Конопляник А. Новое измерение внешней энергетической политики России // Энергетическая политика. – 2024. – № 12. – С. 6–19.

Энергетическая безопасность в условиях новой геополитической реальности

Результаты последних исследований показывают, что геополитическая неопределенность, изменения в политике и растущий спрос на электроэнергию меняют энергетический ландшафт¹. Геополитическая неопределенность, как отмечается в докладе Международного энергетического агентства (МЭА) за 2024 г.², является важным фактором, определяющим перспективы мировой энергетики наряду с проблемами безопасности энергоснабжения, меняющейся климатической политикой, рисками рецессии, ростом цен на энергоносители, тарифов и технологических инноваций. Все чаще доступность и безопасность энергоресурсов ставится в приоритет перед выполнением задач Парижского соглашения по климату 2015 г. Геополитическая и политическая нестабильность добавила неопределенности в краткосрочную эволюцию энергетических систем, что привело к замедлению перехода к чистой энергетике. Одним из примеров такой неопределенности является потенциальное влияние тарифов на потребление экологически чистой энергии. Глобальный спрос на энергоносители продолжает расти, отчасти благодаря быстрому экономическому росту и повышению уровня жизни во многих густонаселенных странах с низким и средним уровнем дохода. При этом повышение внимания к безопасности энергоснабжения не обязательно происходит за счет декарбонизации. Во многих регионах эти два фактора взаимосвязаны, и безопасность поставок определяет более активную политику в области возобновляемых источников энергии.

Мировой спрос на первичные энергоносители, по прогнозам, вырастет примерно на 10% к 2050 г. при сохранении динамичного развития событий. Ожидается, что большая часть этого роста придется на Индию, страны АСЕАН и Африку. Вместе с тем нестабильность на современных энергетических рынках, как отмечается в докладе МЭА, напоминает о непреходящей важности энергетической безопасности, которая должна охватывать безопасную

¹ Global Energy Perspective 2025: Report. – 2025. – 13 oct. – URL: <https://www.mckinsey.com/industries/energy-and-materials/our-insights/global-energy-perspective> (дата обращения: 20.10.2025).

² World Energy Outlook 2024, IEA. – URL: <https://www.iea.org/reports/world-energy-outlook-2024/> (дата обращения: 20.10.2025).

трансформацию электроэнергетического сектора и устойчивость цепочек поставок экологически чистой энергии.

Кроме того, нужно иметь ввиду, что энергетическая отрасль порождает крупные, сложные международные споры ввиду особой чувствительности энергетических рынков к политическим и экономическим потрясениям. В долгосрочной перспективе вопросы влияния энергетического перехода и стремление к энергетической безопасности, очевидно, приведет к появлению новых споров в международном арбитраже, который стал предпочтительным способом разрешения споров, несмотря на свою дороговизну и длительность сроков рассмотрения споров.

Изменение современного энергетического ландшафта и национальная безопасность России

Энергетическая безопасность России формируется на основе стратегических документов национального уровня. Ранее действовавшая Энергетическая стратегия Российской Федерации до 2035 г. определяла ключевые направления государственной политики в сфере энергетики, включая обеспечение безопасности на федеральном и региональном уровнях, особенно в стратегически важных регионах.

Новая Стратегия до 2050 г. нацелена на создание современной энергетической системы, которая обеспечит надежное и доступное энергоснабжение населения и экономики при оптимальных затратах, выполнение экологических целей и повышение энергоэффективности, а также технологический суверенитет и конкурентоспособность энергетического сектора.

Топливо-энергетический комплекс России сталкивается с двойными вызовами: внешними (трансформация экспортных рынков) и внутренними (модернизация и удовлетворение растущего спроса). Россия занимает лидирующие позиции в мире по запасам углеводородов, объемам производства и экспорта энергоресурсов и развitiю атомной энергетики.

Доктрина энергетической безопасности РФ, утвержденная Указом Президента РФ от 13.05.2019 № 216, определяет энергобезопасность как защищенность экономики и населения от угроз в энергетической сфере. Документ выделяет потенциальные угрозы и факторы риска, которые могут как стимулировать развитие энергетики, так и создавать новые вызовы для безопасности.

Стратегическое развитие ТЭК неразрывно связано с национальной безопасностью страны. Доктрина энергетической безопасности РФ и Концепция технологического суверенитета РФ, утвержденная распоряжением Правительства РФ 20.05.2023 № 1315-р, определяют основные направления его развития.

Помимо этих стратегических документов, правовую основу обеспечения безопасности ТЭК составляют федеральные законы: от 21.07.2011 № 256-ФЗ № 256-ФЗ (ред. от 07.07.2025) «О безопасности объектов топливно-энергетического комплекса» и от 26.07.2027 № 187-ФЗ (ред. от 07.04.2025) «О безопасности критической информационной инфраструктуры Российской Федерации».

В современных условиях энергетическая безопасность стала не только частью государственной политики, но и одним из ключевых системных вызовов для развития мировой энергетики¹.

Энергобезопасность, устойчивость и антитеррористическая защищенность топливно-энергетического комплекса (ТЭК) являются ключевыми аспектами обеспечения стабильного функционирования энергетической системы российского государства. Эти понятия тесно связаны, но имеют разные акценты. *Энергобезопасность ТЭК* обеспечивает противодействие широкому спектру угроз, включая геополитические, макроэкономические и техногенные факторы, и подразумевает: (1) бесперебойное и надежное снабжение экономики топливно-энергетическими ресурсами в необходимом объеме и по приемлемым ценам; (2) гарантированное энергоснабжение в условиях стихийных бедствий и техногенных катастроф; (3) защиту от дефицита энергоресурсов при нормальном развитии и в результате внутренних или внешних катаклизмов технического, экономического или политического характера.

Устойчивость топливно-энергетического комплекса представляет собой способность энергетической системы поддерживать свою работу в заданных параметрах под влиянием различных внешних и внутренних факторов на протяжении определенного периода. Эта способность включает в себя несколько ключевых аспектов: ресурсную обеспеченность (возможность как нынешнего, так и будущих поколений получать доступ к необходимым энергетическим ресурсам); рациональное использование (внедрение принципов неистощительного потребления как возобновляе-

¹ Масепанов А., Чингарев Б. The Energy Trilemma Index как оценка энергетической безопасности // Энергетическая политика. – 2020. – № 8. – С. 66–83.

мых, так и невозобновляемых источников энергии) и сбалансированное развитие (согласование объемов потребления ресурсов, инвестиций и научно-технических достижений с текущими и перспективными потребностями общества). Таким образом, устойчивость ТЭК – это комплексная характеристика, которая отражает способность системы адаптироваться к изменениям, сохраняя при этом свою функциональность и обеспечивая энергетические потребности общества в долгосрочной перспективе.

Антитеррористическая защищенность объектов ТЭК – комплекс мер, обеспечивающих безопасность зданий, сооружений и других объектов ТЭК от возможных террористических угроз. Данная защита включает в себя следующие ключевые направления: комплексную систему безопасности, которая объединяет правовые, экономические и организационные меры по защите объектов; классификацию объектов с разработкой индивидуальных требований к их защите в зависимости от степени важности и уязвимости; систему физической охраны, включающую современные инженерно-технические средства защиты; профессиональную подготовку кадров, специализирующихся на обеспечении безопасности объектов. Все эти меры направлены на предотвращение возможных террористических актов и других форм незаконного вмешательства. Они реализуются через конкретные действия и мероприятия, которые создают надежный барьер против потенциальных угроз безопасности объектов ТЭК. Таким образом, антитеррористическая защищенность представляет собой многоуровневую систему превентивных мер, цель которой – максимально обезопасить объекты топливно-энергетического комплекса от возможных террористических угроз.

При разработке Энергетической стратегии учитывалась *принципиальная связь развития энергетики и обеспечения национальной безопасности*, прежде всего энергетической безопасности. Направления развития энергетики согласованы с основными направлениями деятельности по обеспечению энергетической безопасности, определенными в Доктрине энергетической безопасности.

Энергетическая безопасность сегодня – это комплексная система защиты экономической сферы и граждан государства от различных рисков и угроз в области энергетики. Ее главная миссия заключается в решении важнейших задач, которые стоят перед топливно-энергетическим комплексом страны. Энергетическая безопасность выступает как фундаментальный элемент национальной безопасности, обеспечивающий устойчивое развитие

страны и благополучие ее граждан, и включает: способность ТЭК надежно обеспечивать обоснованные потребности в энергии экономически доступными ресурсами приемлемого качества; устойчивость энергетического сектора к внешним экономическим, политическим, техногенным и природным угрозам, а также способность минимизировать ущерб; устойчивость объектов ТЭК к угрозам техногенного, природного и террористического характера, заблаговременное планирование мер по ликвидации чрезвычайных ситуаций.

Заключение

В настоящее время международная обстановка существенно влияет на формирование энергетической политики России. Введение экономических и политических санкций со стороны ряда государств привело к значительным изменениям в стратегических приоритетах энергобезопасности, структуре энергетического баланса и системах поставки углеводородной продукции.

Глобальная геополитическая напряженность породила новые вызовы в сфере энергетической безопасности. Наблюдается усиление роли политических факторов в правовом регулировании, экономических отношениях и международных взаимодействиях.

Отдельные страны активно используют различные инструменты для достижения своих геополитических целей, включая экономическое давление, финансовую политику, торговую стратегию, инвестиционные механизмы, технологический контроль.

Согласно Стратегии национальной безопасности РФ 2021 г., подобные действия подрывают стабильность мировой экономической системы. Текущая ситуация подтверждает прогнозы документа, указывая на негативные последствия ограничительных мер против России, глобальных экономических кризисов, усиления недобросовестной конкуренции и использования юридических инструментов в политических целях.

Все эти факторы создают комплексную угрозу экономической безопасности государства и требуют выработки новых подходов к обеспечению энергетической стабильности страны.

КОДАНЕВА С.И.¹ ПРАВОВОЕ РЕГУЛИРОВАНИЕ И ИНСТИТУЦИОНАЛЬНЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ И В ЗАРУБЕЖНЫХ СТРАНАХ (Статья)

Аннотация. Кибербезопасность стала одной из наиболее важных областей политики в XXI в., выходящей за рамки традиционных национальных границ и переплетающейся с экономическими, социальными и геополитическими вопросами. Большинство стран мира принимает собственное правовое регулирование в данной сфере. Хотя реализуемые в национальном праве подходы и различаются в зависимости от правовых традиций и иных особенностей, однако нормативные акты в области информационной безопасности охватывают широкий спектр вопросов: от законов о защите данных и безопасности критически важной инфраструктуры до предотвращения киберпреступлений и защиты от информационно-психологического воздействия. В настоящей статье на основе анализа правовых подходов в различных странах мира формулируются общие тенденции развития права информационной безопасности.

Ключевые слова: кибербезопасность; защита данных; защита критической информационной инфраструктуры; информационная безопасность; киберсуверенитет; киберинциденты.

KODANEVA S.I. Legal regulation and institutional framework of information security in Russia and abroad. (Article)

Abstract. Cybersecurity has become a critical policy area in the 21 st century, transcending national borders and becoming intertwined with economic, social, and geopolitical issues. Many countries have

¹ *Коданева Светлана Игоревна*, ведущий научный сотрудник отдела правоведения ИНИОН РАН, кандидат юридических наук, доцент.

adopted their own legal frameworks in this area, although the specific approaches implemented may vary depending on local legal traditions and other factors. Regulatory acts in the information security field cover a wide range of topics, from laws protecting data and critical infrastructure to preventing cybercrime and protecting against information and psychological impacts. Based on an analysis of legal frameworks from various countries, this paper identifies general trends in the development of information security legislation.

Keywords: cybersecurity; data protection; protection of critical information infrastructure; information security; cyber sovereignty; cyber incidents.

Для цитирования: Коданева С.И. Правовое регулирование и институциональные основы информационной безопасности в России и в зарубежных странах (Статья) // Социальные и гуманитарные науки: Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2026. – № 1. – С. 90–108. – DOI: 10.31249/iajpravo/2026.01.06

Введение

Глобальная цифровая трансформация, стимулируя беспрецедентный экономический рост и развитие социальных связей, привела к всеобщей зависимости от цифровой инфраструктуры. Оцифровка критически важных областей – от энергетических сетей и финансовых систем до здравоохранения и государственных услуг – в геометрической прогрессии усилила воздействие киберинцидентов на общество, поскольку их последствия носят все более массовый характер. Так, например, кибератаки привели к серьезным сбоям в работе ключевых коммунальных служб (таких как система газоснабжения из-за атаки вируса-вымогателя на трубопроводную компанию Colonial Pipeline в США в 2022 г. или попытка отравления водоочистных сооружений во Флориде, 2021 г.), морских портов (например DP World Australia, 2023 г.), банковских услуг (например банк Nonghyup в Южной Корее, 2011 г.), служб здравоохранения (например кибератака на немецкую больницу, приведшая к смерти пациента скорой помощи, 2020 г.)¹ и др.

Все эти примеры демонстрируют эволюцию характера как киберинцидентов, так и их организаторов – от хакеров-одиночек до преступных и террористических группировок и даже госу-

¹ Seng N. Cybersecurity Regulation – Types, Principles, and Country Deep Dives in Asia // International Cybersecurity Law Review. – 2024. – Vol. 5. – P. 87–411.

дарств, использующих подобные инструменты в своих гибридных войнах. Это превращает информационную безопасность из технической проблемы в ключевой вопрос национальной и общественной безопасности, а также экономической стабильности.

В ответ на этот растущий перечень угроз страны по всему миру активно принимают правовое регулирование, направленное на повышение уровня защищенности информации и критической инфраструктуры. Безусловно, подходы к регулированию довольно сильно различаются как по истории формирования, так и по структуре и лежащей в его основе философии. Однако наметилась тенденция к глобальной конвергенции этих разнообразных подходов вокруг нескольких ключевых принципов. Это сближение обусловлено общими вызовами: необходимостью защиты критической инфраструктуры, персональных данных, управления рисками цепочки поставок и развития международного сотрудничества в сфере, где злоумышленники действуют на международном уровне.

Национальные подходы к регулированию информационной безопасности

Правовое регулирование информационной безопасности в разных странах мира не только различается, как было отмечено выше, но и опирается на общие подходы, основанные на общих принципах. Помимо этого, в последнее время, как отмечает Э. Фахи, наметилась тенденция к конвергенции этих подходов даже в таких разных правовых порядках, как США и ЕС, что обусловлено единством угроз, с которыми сталкиваются все правительства¹.

В частности, представляется возможным выделить три группы нормативных правовых актов, регулирующих вопросы информационной безопасности:

1) законы, направленные на криминализацию противоправных действий в Интернете. Это форма правового регулирования исторически появилась одной из первых в ответ на случаи мошенничества, взлома и кибератак. Такие акты, как Закон США о компьютерном мошенничестве и злоупотреблениях (The Computer Fraud and Abuse Act, 1986), Закон Китая о кибербезопасности (The Cybersecurity Law of the People's Republic of China (Chinese:

¹ Fahey E. The Evolution of EU–US Cybersecurity Law and Policy: on Drivers of Convergence // Journal of European Integration. – 2024. – Vol. 46, N 7. – P. 1073–1088.

中华人民共和国网络安全法), 2016), Закон Индии об информационных технологиях (Information Technology Act, 2000) и Закон Соединенного Королевства о неправомерном использовании компьютеров (Computer Misuse Act, 1990), криминализируют несанкционированный доступ, повреждение и неправильное использование компьютерных систем. Однако слабостью данного подхода был трансграничный характер кибератак, в результате чего возникали проблемы юрисдикции;

2) законодательство, содержащее требования по управлению рисками и обеспечению устойчивости инфраструктуры. Эта категория представляет собой наиболее значительную и растущую область регулирования кибербезопасности, смещающую акцент с наказания злоумышленников на предписание владельцам информационной инфраструктуры принимать меры по защите конфиденциальности, целостности и доступности своих систем и данных, т.е. на предотвращение инцидентов. Подобного рода акты приняты во многих странах, включая Регламент ЕС № 2022/2555 о сетях и информационных системах (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union), Закон Сингапура о кибербезопасности (Cybersecurity Act, 2018), Закон Австралии о безопасности критической инфраструктуры (Security of Critical Infrastructure Act, 2018) и др. Эти законы обычно определяют меры организационного и технического характера по защите данных и инфраструктуры;

3) законодательство, предписывающее отчитываться об инцидентах. Эта тенденция регулирования возникла позже двух предыдущих. Суть ее заключается в требовании, чтобы организации сообщали об инцидентах в области кибербезопасности государственным органам и, в некоторых случаях, общественности. Яркими примерами являются правила Комиссии по ценным бумагам и биржам США 2023 г., требования к отчетности в рамках указанного выше Регламента ЕС, а также инструкции по сертификации Индии. Цели данного рода актов двоякие: с одной стороны, повысить осведомленность органов власти о ландшафте киберугроз, а с другой – стимулировать компании повышать уровень и качество их информационной безопасности.

Соединенные Штаты Америки имеют сложную и фрагментированную систему регулирования кибербезопасности. Модель США характеризуется ориентацией на конкретный сектор, сочетанием полномочий федерального уровня и уровня штатов и акцентом на государственно-частное партнерство и частный сектор. Это

означает, что для ряда секторов специальными законами устанавливаются единые требования (например, Закон об управлении информационной безопасностью (Federal Information Security Management Act, 2002), уделяющий особое внимание безопасности систем федерального правительства; Закон о переносимости и подотчетности медицинского страхования (Health Insurance Portability and Accountability Act, 1996) устанавливает стандарты защиты конфиденциальной медицинской информации пациентов, Закон Грэмма-Лича-Блайли (Financial Services Modernization Act (Gramm-Leach-Bliley Act), 1999) обязывает финансовые учреждения разъяснять свои методы обмена информацией и защищать конфиденциальные данные клиентов и т.д.). В отношении остальных сфер применяются необязательные стандарты, хотя недавно принятый в 2022 г. Закон об отчетности о киберинцидентах для критической инфраструктуры (Cyber Incident Reporting for Critical Infrastructure Act, 2022) представляет собой значительный шаг на пути к более унифицированному стандарту отчетности для соответствующих объектов.

Наиболее значимой системой добровольной стандартизации является система кибербезопасности Национального института стандартов и технологий (National Institute of Standards and Technologies, NIST) – основанный на оценке рисков набор руководящих принципов, передовой практики и стандартов для управления рисками кибербезопасности. Показательно, что пять основных направлений, предложенных NIST (идентификация, защита, обнаружение, реагирование, восстановление), используются большинством стран мира и многими компаниями частного сектора как основа при создании собственных систем кибербезопасности.

Правоприменительная практика в США столь же фрагментирована, поскольку опирается на ведомственные акты или регулирование штатов. Все это, а также необходимость учитывать более жесткие обязательные стандарты, например ЕС, создает для американских компаний проблемы и сложности, хотя делает систему гибкой и адаптивной¹.

Европейский союз претендует на роль глобального центра регулирования в области кибербезопасности. Он придерживается всеобъемлющей, согласованной и быстро расширяющейся право-

¹ Assessing the Effectiveness of Current Cybersecurity Regulations and Policies in the US / E. Oluomachi, A. Ahmed, W. Ahmed, E. Samson // International Journal of Scientific and Research Publications. – 2024. – Vol. 14, N 2. – P. 78–85.

вой базы, основанной на приоритете прав человека. Правовую основу образуют Общий регламент по защите данных (General Data Protection Regulation 2016/679, GDPR, 2016)¹ и Директива по сетевой и информационной безопасности (Network and Information Security Directive (EU) 2022/2555, NIS2, 2022)².

Политика кибербезопасности ЕС прошла в своем развитии три этапа: генезис, институционализацию и «фазу регулирования». Этот третий этап, на котором ЕС находится сегодня, характерен тем, что кибербезопасность представлена как вопрос «европейского суверенитета». При этом реализуется концепция «нормативного меркантилизма»³, объединяющая вопросы экономики, безопасности и суверенитета и направленная не только на защиту внутреннего рынка, но и на распространение норм ЕС по всему миру. Соответственно, объем правотворчества активно растет в последние годы. В частности, принят Регламент ЕС 2019/881/EU о кибербезопасности (Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity), 2019), который закрепил мандат Агентства ЕС по кибербезопасности и создал общеевропейскую систему сертификации продуктов и услуг в области кибербезопасности. Также разработаны проекты регламентов о киберустойчивости (направлен на обеспечение того, чтобы продукты с цифровыми элементами (от интеллектуальных холодильников до промышленного программного обеспечения) продавались со встроенной сис-

¹ Хотя формально он касается персональных данных, но установленные в нем требования к безопасному хранению, передаче и обработке данных фактически оказали преобразующее влияние на кибербезопасность не только в ЕС, но и во всем мире, поскольку за нарушение этих требований предусмотрены серьезные штрафы в размере до 4% от мирового годового оборота компании – GDPR's Impact on Cybersecurity: A Review Focusing on USA and European Practices / O.O. Amoo, A. Atadoga, F. Osasona, T.O. Abrahams, B.S. Ayinla, O.A. Farayola // International Journal of Science and Research Archive. – 2024. – Vol. 11, N 1. – P. 1338–1347.

² Первый ее вариант, принятый в 2016 г., был адресован операторам основных услуг (OES) и поставщикам цифровых услуг (DSP), но новая Директива NIS2, принятая в 2022 г., значительно расширила сферу применения, охватывая гораздо более широкий круг секторов, включая энергетику, транспорт, банковское дело, здравоохранение, цифровую инфраструктуру и государственное управление, налагая строгие обязательства по управлению рисками, отчетности и обеспечению безопасности цепочки поставок.

³ Carrapico H., Farrand B. Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics // Journal of Common Market Studies. – 2024. – Vol. 62. – P. 147–158.

темой кибербезопасности, охватывающей весь их жизненный цикл), о киберсолидарности (направлен на создание «киберщита ЕС» из операционных центров безопасности и укрепление совместных возможностей обеспечения готовности к инцидентам и реагирования на них) и о цифровой операционной устойчивости (направлен на финансовый сектор, гарантируя, что он сможет противостоять всем типам сбоям и угроз, связанных с ИКТ).

Правоприменение в ЕС децентрализовано, но опирается на общие правила, устанавливающие как общие требования, так и меры наказания. Институциональную основу образует сеть органов, включая ENISA (которая обеспечивает экспертизу и координацию), национальные группы реагирования на инциденты компьютерной безопасности (National Computer Security Incident Response Teams (CSIRTs)) и компетентные органы в каждом государстве-члене. Однако увеличение объема нормативного регулирования и бюрократической нагрузки в сфере кибербезопасности ослабляют мотивацию к получению прибыли и мешают предпринимателям использовать инновационные решения в области безопасности, что тормозит их развитие. В результате компании направляют свою энергию от продуктивных инноваций в области безопасности к непродуктивному соблюдению формальных требований¹.

Российский подход к тому, что на Западе принято называть «кибербезопасностью», имеет существенные отличия. Он шире и глубоко интегрирован в парадигму национальной безопасности, воплощаясь в термине «информационная безопасность». Эта концепция выходит далеко за рамки технической защиты компьютерных систем и охватывает защиту национального суверенитета, социальной стабильности общества² и психологического благополучия населения от информационно-психологических манипуляций³.

Краеугольным камнем российского подхода является его доктринальная основа, которая определяет информацию как клю-

¹ Kianpour M., Raza Sh. More than Malware: Unmasking the Hidden Risk of Cybersecurity Regulations // International Cybersecurity Law Review. – 2024. – Vol. 5. – P. 169–212.

² Салов И.В., Байрушин Ф.Т., Абрамов И.Р. Информационная безопасность как фактор обеспечения социальной стабильности в российском обществе // Евразийский юридический журнал. – 2023. – № 8 (183). – С. 427–428.

³ Матюхин О.И. Информационная безопасность сквозь призму теории Джеймса Биллингтона: «Пожар в сознании» и угрозы цифровой эпохи // Вопросы безопасности. – 2025. – № 2. – С. 41–52.

чевой элемент национальной безопасности и вектор потенциальных угроз¹. При этом существует фундаментальное концептуальное расхождение между российским дискурсом «информационной безопасности» и западным дискурсом «кибербезопасности». Российский подход является более целостным, но сложным и спорным. Поэтому научные дебаты о содержании данного понятия до сих пор не стихают. Одни авторы анализируют состояние технической защищенности как таковой, включая противодействие кибератакам и проблематику защиты данных². Другие же основное внимание уделяют последствиям влияния неконтролируемого распространения информации на традиционные духовные ценности, состояние морали в обществе и национальную безопасность³. Так, М.В. Конохов связывает борьбу с «фейками» с национальной безопасностью, особенно в контексте СВО, утверждая, что ложная информация является ключевым инструментом информационных операций против России⁴. А.И. Толстой выделяет информационно-психологическую безопасность человека как самостоятельную область информационной безопасности и даже полагает, что данное понятие следует использовать исключительно для этой ориентированной на человека области, и что нынешнее широкое понимание информационной безопасности является исторической ошибкой при переводе международных стандартов⁵.

Некоторые авторы, в частности А.К. Дубень, опираясь на положения Стратегии национальной безопасности России, предла-

¹ Сосновская Ю.Н., Клементьева В.С. К вопросу о содержании информационной безопасности как приоритетного компонента национальной безопасности // Вестник экономической безопасности. – 2023. – № 6. – С. 156–161.

² Tereschenko L.K., Starodubova O.E., Nazarov N.A. New Information Technologies and Data Security. A review // Legal Issues in the Digital Age. – 2023. – Vol. 4, N 2. – P. 158–175; Пекарева В.В., Фроловская Ю.И. Конфиденциальность, целостность, доступность данных как основные принципы информационной безопасности // Аграрное и земельное право. – 2024. – № 4 (232). – С. 104–106.

³ Tsvyk V.A., Tsvyk I.V. Personal Information Security as a Social Problem // RUDN journal of sociology. – 2023. – N 23. – С. 590–599.

⁴ Конохов М.В. О некоторых вопросах правового обеспечения информационной безопасности Российской Федерации: международные и внутригосударственные аспекты // Право и государство: теория и практика. – 2024. – № 4 (232). – С. 173–176.

⁵ Толстой А.И. Обеспечение безопасности объектов в информационной сфере // Безопасность информационных технологий. – 2024. – Т. 31, № 3. – С. 105–123.

гают использовать комплексный подход, объединяющий под единым термином «информационная безопасность» как состояние защищенности в информационном пространстве, так и защиту конституционно значимых ценностей и суверенитета государства¹.

Как можно видеть, информационная безопасность в российском понимании включает:

– информационно-техническую безопасность (защиту информационных систем, сетей и данных от несанкционированного доступа, сбоя или уничтожения, что соответствует западной концепции кибербезопасности);

– информационно-психологическую безопасность (защиту индивидуального и общественного сознания от манипулятивного информационного воздействия, «фейков» и нарративов, дестабилизирующих общество, подрывающих традиционные ценности или дискредитирующих государственные институты и вооруженные силы);

– информационная безопасность как основа национальной безопасности (опирается на идею информационного суверенитета как состояния защищенности национальных и общественных интересов, интересов личности). Именно это понимание информационной безопасности Россия стремится продвигать на международном уровне в качестве концептуальной основы для международных соглашений и договоров с другими странами, стараясь с помощью юридически обязывающих соглашений ограничить информационные операции и распространение дестабилизирующего контента, чему западные страны сопротивляются, ссылаясь на свободу слова.

Российское законодательство является в высшей степени централизованным и детализированным. Его концептуальную основу составляют Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ от 05.12.2016 № 646, которая определяет четыре основные сферы национальных интересов (личность, общество, государство, стратегическое сдерживание); Стратегия национальной безопасности РФ, утвержденная Указом Президента РФ от 02.07.2021 № 400, согласно которой информационная безопасность является одним из ключевых компонентов национальной безопасности, а внешние информационные кампании представлены как угроза конституционному строю России, и

¹ Дубень А.К. Информационная безопасность: определение понятия, место в системе национальной безопасности // Аграрное и земельное право. – 2023. – № 11 (227). – С. 93–95.

обозначена необходимость защиты населения от деструктивных информационно-психологических воздействий; а также Концепция Государственной системы обнаружения, предотвращения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, утвержденная Указом Президента РФ от 12.12.2014 № К 1274, заложившая основу защиты и мер реагирования государства на киберинциденты, создав систему ГосСОПКА, за функционирование которой отвечает Федеральная служба безопасности РФ.

Положения этих стратегических концептуальных документов детализируются в федеральных законах: от 26.07.2017 (ред. 07.04.2025) № 187-ФЗ «О безопасности критически важной информационной инфраструктуры»; от 27.07.2006 (ред. от 24.06.2025) № 149-ФЗ «Об информации, информационных технологиях и защите информации»; от 27.07.2006 (ред. от 24.06.2025) № 152-ФЗ (ред. от 24.06.2025) «О персональных данных»; от 25.07.2002 (ред. от 27.10.2025) № 114-ФЗ «О противодействии экстремистской деятельности») и многочисленных подзаконных актах¹.

В целом в российской правовой системе используются подходы, схожие с европейскими, хотя и с большей степенью конкретизации и обязательности регулирования. Процесс защиты объектов критически важной информационной инфраструктуры является методичным и четким. Ее владельцы обязаны осуществлять категоризацию принадлежащей им инфраструктуры в зависимости от значимости для государственной безопасности, общественного порядка и экономической стабильности. Для наиболее значимых объектов разрабатывается система безопасности. Это не просто набор программного обеспечения, а интегрированная система, включающая технические (сертифицированное программное и аппаратное обеспечение), организационные (персонал, подразделения внутренней безопасности) и нормативные (политики, процедуры и планы) элементы. Кроме того владелец инфраструктуры должен выполнять набор мер, утвержденный ФСТЭК, которая проводит постоянные проверки, и подключаться к системе ГосСОПКА.

¹ Подробнее см.: Структура действующих нормативных правовых актов в области обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации / А.В. Бондаренко, К.В. Мушовец, С.В. Поршнев, О.К. Рогова // Безопасность информационных технологий. – 2023. – Т. 30, № 3. – С. 126–148.

Учитывая сложность и обширность правовой базы, касающейся информационной безопасности, в России сложилась сложная система уполномоченных органов: Минцифры России отвечает за широкий сектор информационных технологий и телекоммуникаций, регулирует безопасность сетей связи общего пользования, которые эксплуатируются значимыми объектами критически важной инфраструктуры. Оно выпускает рекомендации по сертификации коммуникационного оборудования и организационно-техническим мерам обеспечения сетевой безопасности. Федеральная служба по техническому и экспортному контролю (ФСТЭК) обеспечивает защищенность критически важной информационной инфраструктуры, также как ФСБ России, пользующаяся системой ГосСОПКА и управляющая ею, обеспечивающая сертификацию инфраструктуры, лицензирование криптографической деятельности, координирующая реагирование на инциденты на объектах критически важной инфраструктуры.

Правоохранительные органы также принимают участие в обеспечении информационной безопасности. Так, прокуратура осуществляет надзор за законностью деятельности указанных выше государственных органов, включая ФСБ России и ФСТЭК, а также частных организаций в области информационной безопасности¹. Полиция осуществляет контроль за соблюдением законодательства в области информационной безопасности предприятиями и гражданами, налагает штрафы за административные правонарушения в данной сфере, а также занимается пропагандой и повышением осведомленности, информируя общественность об информационных угрозах (например видеоролики в метро о киберпреступности)².

Кроме того, Роскомнадзор и прокуратура наделены полномочиями по контролю за распространяемой в сети Интернет информацией.

В то же время Россия сталкивается с серьезными проблемами в данной сфере. Прежде всего, это зависимость от западных

¹ Соколов И.А. Особенности определения пределов деятельности прокуратуры по обеспечению информационной безопасности государства // *Власть закона*. – 2023. – № 3 (55). – С. 338–350.

² Федорова И.В., Калинина С.В., Самохвалов В.В. Особенности административной деятельности полиции в сфере обеспечения информационной безопасности // *Вестник московского университета МВД России*. – 2023. – № 6. – С. 238–242.

технологий, уход западных компаний из страны и санкции¹. На решение этих проблем направлены Указ Президента РФ от 30.03.2022 (ред. 07.04.2025) № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации», запрещающий госзаказчикам закупать иностранное программное обеспечение при наличии российских альтернатив, внесенные в Гражданский кодекс РФ и узаконившие параллельный импорт критически важных для страны технологий, а также комплекс мер, направленных на поддержку отечественных разработчиков и производителей ИТ-технологий.

Таким образом, нормативно-правовая база РФ по информационной безопасности является всеобъемлющей, детализированной и постоянно развивается. Она основана на следующих принципах: холизм²; суверенитет; централизация; устойчивость к киберинцидентам; обязательность государственного регулирования (в противовес американской модели саморегулирования).

Эта система не лишена внутренних противоречий и проблем, однако она представляет собой последовательную и целенаправленную стратегию управления рисками и использования возможностей информационной эпохи на своих собственных условиях.

Азиатско-Тихоокеанский регион демонстрирует широкий спектр подходов, от достаточно хорошо развитых моделей Китая, Сингапура, Японии и Австралии и до развивающихся структур Индонезии.

Подход *Китая* к регулированию кибербезопасности основан на принципе киберсуверенитета (утверждении абсолютного национального контроля над Интернетом в пределах своих границ), что резко контрастирует с западными моделями. Эти различия носят не только технический, но и философский характер, оказывая влияние на все – от управления данными и защиты критически важной инфраструктуры до самого определения безопасности, ко-

¹ Вершинин А.Н. Цифровая трансформация информационной безопасности критической информационной инфраструктуры в условиях импортозамещения // Научный аспект. – 2023. – Т. 2, № 5. – С. 209–217.

² Отказ от узкой модели «кибербезопасности» в пользу целостной парадигмы «информационной безопасности», которая объединяет техническую и психологическую защиту.

торое в Китае включает в себя не только техническую целостность, но и политическую и социальную стабильность¹.

В Китае система регулирования вопросов информационной безопасности действует по принципу «сверху вниз» и имеет двоякую цель – обеспечение национальной безопасности и стабильности режима. основополагающим является Закон о кибербезопасности (The Cybersecurity Law of the People's Republic of China (Chinese: 中华人民共和国网络安全法), 2016), базирующийся на принципе сочетания кибернетического суверенитета (предоставляющего государству широкие полномочия по регулированию и контролю интернет-инфраструктуры и контента) и «безопасных и контролируемых» сетей (расплывчатый термин, который интерпретируется как предписывающий использование отечественных технологий для снижения зависимости от иностранных поставщиков, что позволяет получать доступ ко всем данным органам власти для обеспечения государственной безопасности). Этот закон, как и во многих других странах, основное внимание уделяет защите критически важной информационной инфраструктуры. Однако китайское определение включает в себя «общественные коммуникационные и информационные службы» и «другие важные сферы, которые в случае разрушения, потери функций или утечки данных могут серьезно угрожать национальной безопасности, национальному благосостоянию, средствам к существованию людей или общественным интересам», что фактически ставит под государственный контроль практически всю цифровую экономику страны. Помимо этого, закон содержит требование локализации данных и существенные ограничения по их трансграничной передаче. Эти нормы значительно строже, чем в ЕС, поскольку передача личной информации за рубеж возможна только «по требованию бизнеса» и подлежит обязательной оценке безопасности, проводимой Управлением по киберпространству Китая (Cyberspace Administration of China, САС). Закон также обязывает сетевых операторов требовать от пользователей предоставления реальных идентификационных данных, что фактически прекращает анонимность в Интернете. Это является уникальной отличительной чертой китайской модели, отсутствующей в других рассмотренных правовых моделях.

¹ Creemers R. The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy // Journal of Contemporary China. – 2024. – Vol. 33, N 146. – P. 173–188.

В дополнение к Закону о кибербезопасности в Китае приняты Закон о защите данных (Data Security Law of the People's Republic of China (Chinese: 中华人民共和国数据安全法) (DSL), 2021) и Закон о защите личной информации (Personal Information Protection Law of the People's Republic of China (Chinese: 中华人民共和国个人信息保护法) (PIPL), 2021). Первый создает систему секретной и дифференцированной защиты всех данных, основанную на их важности для национальной безопасности и общественных интересов. Это еще больше расширяет возможности государства по контролю за данными и доступу к ним, создавая правовую основу для наказания за действия, которые считаются наносящими ущерб государственной безопасности. Второй, часто называемый «Общим регламентом по защите данных Китая», предоставляет гражданам страны право на конфиденциальность. Однако это право в значительной степени ограничено исключениями, касающимися национальной безопасности и общественных интересов и требованием к операторам данных сотрудничать с органами общественной безопасности и ведомствами госбезопасности.

На подзаконном уровне в Китае принята Многоуровневая схема защиты (Multi-Level Protection Scheme (MLPS 2.0), 2020), которая требует от всех сетевых операторов в Китае классифицировать свои системы по одному из пяти уровней безопасности, и применять соответствующие меры защиты. В целом система похожа на американскую систему NIST, но в отличие от нее является обязательной.

Основным правоприменительным органом в рассматриваемой сфере является Управление по киберпространству Китая – влиятельный партийный орган, обладающий широкими полномочиями. Его решения не подлежат судебному пересмотру. Помимо этого Положение о надзоре и проверке интернет-безопасности органами общественной безопасности 2018 г. наделило правоохранительные органы полномочиями на доступ (в том числе удаленный) и копирование данных, имеющих отношение к кибербезопасности.

Китай не просто разрушает западную модель глобального и открытого Интернета у себя в стране, но активно экспортирует свою модель «кибернетического суверенитета» через такие площадки, как ООН, и через свою инициативу «Цифровой шелковый путь», предлагая альтернативу западной либеральной модели управления Интернетом. Следует отметить, что вопросы информационной безопасности становятся инструментом не только в

информационной войне между США и Китаем, но и конкурентных войн между транснациональными корпорациями этих двух стран. Причем эти два аспекта очень тесно переплетены, делая вопросы кибербезопасности политическими. Например, в 2024 г. в США был принят Закон о защите американцев от приложений, контролируемых иностранными противниками (Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA), 2024), направленный против TikTok, согласно которому социальная сеть или должна быть продана американской компании, или будет заблокирована. Правительство Китая предпочло второй вариант¹.

Стратегия кибербезопасности *Сингапура* 2021 г. отличается ясностью, централизацией и нацеленностью на технологическое развитие. Она включает четыре основных компонента: создание устойчивой инфраструктуры, создание безопасного киберпространства, развитие динамичной экосистемы кибербезопасности и укрепление международных партнерств. Правовую основу информационной безопасности в этой стране составляет Закон о кибербезопасности 2018 г., который предоставляет Агентству кибербезопасности (Cyber Security Agency of Singapore, CSA) широкие полномочия в отношении защиты критической информационной инфраструктуры в 11 ключевых секторах. Закон содержит «Кодекс практики», в котором излагаются конкретные технические и организационные требования к владельцам инфраструктуры, охватывающие управление, защиту, обнаружение, реагирование и восстановление. Закон о защите персональных данных (Personal Data Protection Act (PDPA) 2012), как и его европейский аналог, включает требования относительно разумных мер безопасности персональных данных. Комиссия по защите персональных данных (Personal Data Protection Commission, PDPC) приняла множество решений, которые содержат практические рекомендации касательно того, что считается «разумным». Денежно-кредитное управление Сингапура (Monetary Authority of Singapore, MAS) выпускает обязательные уведомления по управлению технологическими рисками и кибергигиене для финансового сектора, создавая надежный уровень регулирования для этого сектора.

Таким образом, в Сингапуре реализован смешанный подход: Закон о защите персональных данных содержит принципы обеспе-

¹ Петрунин Ю.Ю., Бухарин В.В. От информационной безопасности к национальной: противоборство IT-компаний США и КНР // Безопасность цифровых технологий. – 2024. – № 2 (113). – С. 25–54.

чения их безопасности для всех операторов данных, Закон о кибербезопасности и принятые в его развитие акты CSA устанавливают четкие предписания для владельцев критической инфраструктуры, что сочетается с отраслевым подходом в деятельности MAS.

Система *Японии* основана на сочетании законов, содержащих общие принципы и нормы (Закон о защите личной информации (The Act on the Protection of Personal Information (APPI), 2003), требует от предприятий принимать «необходимые и уместные» меры безопасности; Закон о телекоммуникационном бизнесе (Telecommunications Business Act (TBA), 1984) содержит требования по кибербезопасности для операторов связи, включая разработку «правил обращения с информацией», назначение главного контролера и ежегодные самооценки, и подробные, но не имеющие обязательной силы рекомендации регулирующих органов. Таким образом, японская система сочетает в себе общие подходы к регулированию на уровне законов, закладывающие основу для правоприменительной сферы, с гибкостью, обеспеченной подробностью, но необязательностью подзаконных рекомендаций.

В *Австралии* основу правового регулирования составляют Австралийская стратегия и план действий в области кибербезопасности на 2023–2030 гг. и Закон о безопасности критически важной инфраструктуры (Security of Critical Infrastructure Act (SOCI), 2018); использованный в нем подход похож на российскую модель – на владельца критически важной инфраструктуры наложено «позитивное обязательство по обеспечению безопасности», включающее требование по принятию программы управления рисками для критически важной инфраструктуры (Critical Infrastructure Risk Management Programs (CIRMP)), основанной либо на стандартах NIST, либо на «модели зрелости» Австралийского управления сигналами «Essential Eight»¹. Это гибридный подход: обязательные стандарты без чрезмерной детализации. Кроме того, Закон о неприкосновенности частной жизни (The Privacy Act, 1988) налагает обязательство предпринимать «разумные шаги» для защиты личной информации, соблюдение которых обеспечивается Управлением Австралийского комиссара по информации (Oaic).

Правовой ландшафт *Индонезии* в области кибербезопасности является символом проблем, с которыми сталкиваются многие

¹ Digital Resilience. International and Domestic Legal Responses to Cyber Security and Artificial Intelligence / eds. D. Stephens, M. Stubbs, S. White. – Singapore: Springer Nature Singapore, 2025. – 209 p.

развивающиеся цифровые экономики. Закон об электронной информации и транзакциях (Law on Electronic Information and Transactions (ITE Law), 2008) обеспечивает правовую основу, криминализируя киберпреступность и устанавливая принципы электронных транзакций. Однако в целом нормативно-правовая база раздроблена на множество законов, актов правительства и министерств. При этом полномочия Министерства связи и информации, Национального агентства по кибербезопасности и криптографии и полиции частично совпадают. Индонезийское общество плохо информировано о вопросах информационной безопасности и связанных с ней рисках. Ресурсы как органов власти, так и компаний крайне ограничены, что не позволяет им реализовать полноценные системы киберзащиты. Основной проблемой является нехватка квалифицированных кадров¹.

В системах *Индии* и *Пакистана* акцент смещен на криминализацию цифровых атак и кибертерроризма. Закон Индии об информационных технологиях (Information Technology Act, 2000) направлен на борьбу с киберпреступностью, также как и Закон Пакистана о предотвращении электронных преступлений (Prevention of Electronic Crimes Act, 2016)².

Заключение

Как можно видеть, несмотря на существующие различия в правовых подходах к регулированию информационной безопасности, можно обнаружить и ряд сходств:

1. Важность защиты критически важных объектов инфраструктуры (существует общее признание того, что определенные сектора настолько жизненно необходимы, что киберинциденты на них представляют угрозу национальной безопасности, поэтому законодательство всех стран направлено на защиту такой инфраструктуры, хотя масштабы регулирования и конкретные обязательства различаются).

¹ Rhogust M. Legal Framework for Cybersecurity in the Digital Economy: Challenges and Prospects for Indonesia // Journal of Law, Social Science and Humanities. – 2024. – Vol. 1, N 2. – P. 166–180.

² A Survey of Cybersecurity Laws, Regulations, and Policies in Technologically Advanced Nations: a Case Study of Pakistan to Bridge the Gap / B. Saleem, M. Ahmed, M. Zahra, F. Hassan, M.A. Iqbal, Z. Muhammad // International Cybersecurity Law Review. – 2024. – Vol. 5. – P. 533–561.

2. Рост числа обязательных отчетов об инцидентах (переход от добровольного обмена информацией к обязательному своевременному сообщению о значительных инцидентах в настоящее время является глобальным трендом даже в таких странах, как США).

3. Цепочка поставок и управление рисками сторонних производителей (не только для России важно обеспечение бесперебойных поставок качественного оборудования, другие страны также озабочены данной проблемой, что отражается в их законодательстве: например, указы президента США о безопасности цепочки поставок программного обеспечения или «Кодекс практики» Сингапура налагают обязательства по управлению рисками на поставщиков и сервис-провайдеров).

4. Влияние системы NIST (хотя эта система стандартизации и является рекомендательной и добровольной в США, но де-факто она стала глобальным стандартом кибербезопасности).

5. Слияние защиты данных и кибербезопасности (принятие GDPR стало поворотным моментом в правовых подходах к кибербезопасности – все больше стран мира рассматривают данную область через призму защиты персональных данных).

Основными принципами информационной безопасности, которых придерживаются большинство стран мира, являются:

1. Регулирование, основанное на оценке рисков: требования должны быть пропорциональны ущербу, который может нанести инцидент в области кибербезопасности. Возлагать одинаковое бремя на международный банк и мелкого розничного продавца неэффективно. Поэтому правовое регулирование, как правило, направлено на операторов критически важной информационной инфраструктуры или «основных услуг» (организации в таких секторах, как энергетика, водоснабжение, финансы, здравоохранение и транспорт, где последствия сбоя могут иметь опасные последствия для всего общества, повлечь существенный экономический ущерб).

2. Технологическая нейтральность: нормативные акты содержат только требования к результату принимаемых мер (например, «обеспечивать безопасность»), но не к используемым для этого технологиям (например «использовать шифрование AES-256»). Этот принцип отражает то, что технологии очень быстро развиваются и устаревают, поэтому технологическая нейтральность правового регулирования позволяет организациям адаптировать свои средства защиты к возникающим угрозам и инновациям.

3. Отказ от чрезмерно детализированного регулирования и фрагментации: чрезмерно подробные правила могут быть негибкими и не учитывать уникальный контекст организации. Более того, когда разные страны принимают совершенно разные требования, это создает дополнительную нагрузку на транснациональные корпорации, вынужденные подстраиваться под множество национальных правовых порядков. Соответственно, некоторые страны предпочитают закреплять только общие положения и принципы, которые могут способствовать международной гармонизации правового регулирования. Однако, как было показано выше, этот принцип не является универсальным, поскольку такие страны, как Китай и Россия, напротив, стремятся защитить свой киберсуверенитет, в том числе посредством детализации и фрагментации правового пространства.

4. Приоритет в законодательстве мер стимулирования использованию передовых практик перед криминализацией: эффективное правовое регулирование нацеливает организации внедрять самые современные и передовые подходы к информационной безопасности, применяя для этого различные меры стимулирования. Например, Закон США об обмене информацией о кибербезопасности (Cybersecurity Information Sharing Act, 2015) предоставляет юридические убежища компаниям, делящимся с органами власти данными о киберугрозах, тем самым укрепляя коллективную защиту.

СКУРКО Е.В.¹ БЕЗОПАСНОСТЬ, КИБЕРБЕЗОПАСНОСТЬ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПРАВОВЫЕ АСПЕКТЫ (Обзор)

Аннотация. Искусственный интеллект повсеместно в мире приобретает все более важную роль в общественной жизни. Системы ИИ, несмотря на их безусловные возможности, подвержены различным уязвимостям, которые могут поставить под угрозу безопасность их применения. Эти уязвимости, помимо этики ИИ, можно разделить на два основных типа: случайные сбои и преднамеренные атаки. Понимание этих потенциальных уязвимостей имеет основополагающее значение для разработки надежных и устойчивых механизмов противодействия, в особенности в правовой сфере. В обзоре анализируется безопасность и кибербезопасность применения ИИ в различных аспектах, юридические принципы и подходы к ответам на современные вызовы ИИ, рассматриваются международные акты и примеры актов национального законодательства, регулирующих использование ИИ в различных сферах социальной жизни и отношений.

Ключевые слова: искусственный интеллект; правовое регулирование; безопасность искусственного интеллекта; кибербезопасность.

SKURKO E.V. Security, cybersecurity of artificial intelligence applications: legal aspects (Review)

Abstract. Artificial intelligence becomes increasingly important in public life all-over the world. AI systems, despite their unconditional capabilities, are subject to various vulnerabilities that may compromise the security of their use. In addition to the ethics of AI, these vulner-

¹ Скурко Елена Вячеславовна, старший научный сотрудник отдела правоведения ИНИОН РАН, кандидат юридических наук.

abilities can be divided into two main types: accidental failures and deliberate attacks. Understanding these potential vulnerabilities is fundamental to develop reliable and sustainable countermeasures, especially in the legal field. The review analyzes the security and cybersecurity of the use of AI in its various aspects, legal principles and approaches responding to contemporary AI challenges, and examines international acts and examples of national legislation regulating the use of AI in various areas of social life and relationships.

Keywords: artificial intelligence; legal regulation; artificial intelligence security; cybersecurity.

Для цитирования: Скурко Е.В. Безопасность, кибербезопасность применения искусственного интеллекта: правовые аспекты (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4: Государство и право. – 2026. – № 1. – С. 109–124. – DOI: 10.31249/rgpravo/2026.01.07

Введение

Искусственный интеллект сегодня выполняет сложные функции в качестве основы для принятия решений человеком в различных сферах жизни, либо в сфере управления техническими процессами – без участия человека. Такого рода «автономные системы», как ИИ, создают проблемы для правовой системы. Они непригодны в качестве носителей юридических обязанностей и прав. В результате, заменяя людей, они оставляют пробелы в правовой сфере, особенно в области юридической ответственности. По мнению ряда специалистов, законодатели смогут устранить эти пробелы инновационным способом только в том случае, если регулирование искусственного интеллекта будет специфичным для каждой отдельной области его применения, как например это частично достигнуто в сфере автономного транспорта и вождения [2, p. 9].

Потенциальные уязвимости в системах искусственного интеллекта и кибербезопасность

Системы искусственного интеллекта, несмотря на их большие и многоплановые способности, подвержены различным рискам и уязвимостям, которые могут создать угрозу их безопасности. Авторы книги «Агентский искусственный интеллект: теории и практики» под редакцией Кен Хуанга [1] разделяют уязвимости

ИИ на два основных типа: случайные сбои и преднамеренные атаки. Понимание этих угроз позволяет разрабатывать формы противодействия им – как техническими, так и юридическими средствами и методами [1, р. 369].

Случайные сбои в системах ИИ могут возникать из-за множества факторов, часто из-за непреднамеренных ошибок в их разработке, реализации или эксплуатации. Это:

– программные и логические ошибки представляют собой один из источников уязвимостей в системах ИИ. По мере того, как технологии ИИ становятся все более сложными, совершенствуются алгоритмы принятия решений и расширяются возможности обучения и взаимодействия различных систем ИИ, вероятность ошибок при принятии решений резко возрастает. Эти проблемы могут приводить к неожиданным системным сбоям и к серьезным последствиям в критически важных областях;

– аппаратные сбои. «Агенты» ИИ, особенно те, которые встроены в физические системы, такие как мобильные телефоны, умные часы, другие носимые устройства, умный дом, человекоподобные роботы и т.п., используют различные аппаратные компоненты для распознавания данных, их обработки и приведения прибора в действие. Сбои в работе этих компонентов могут нарушить способность «агента» точно воспринимать окружающую среду или выполнять действия по назначению;

– проблемы с качеством данных и предвзятость. Модели машинного обучения, используемые ИИ, хороши ровно настолько, насколько точны данные, на которых они обучены, а недостатки в данных обучения могут привести к предвзятому или неверному принятию решений. Эта уязвимость особенно важна для «агентов» ИИ, поскольку они часто работают автономно в динамичных средах, где последствия предвзятых решений со временем могут усугубиться [1, р. 370–372].

Преднамеренные атаки. Помимо случайных сбоев, системы ИИ сталкиваются с угрозами преднамеренных атак, направленных на использование их уязвимостей или манипулирование их поведением. Это:

– перехватывающие атаки на модели ИИ представляют значительную угрозу для систем ИИ, поскольку они могут манипулировать восприятием «агента» и процессами принятия решений. Эти атаки включают в себя создание входных данных, специально разработанных для того, чтобы обмануть системы ИИ и заставить их принимать неверные решения;

– атаки с использованием вредоносных данных – еще одна форма преднамеренного манипулирования ИИ. В ходе этих атак злоумышленники вводят поврежденные или вводящие в заблуждение данные в набор обучающих данных системы ИИ или в потоки онлайн-обучения. Для «агентов» ИИ, которые постоянно обучаются и адаптируются к своей среде, заражение данных представляет собой серьезную долгосрочную угрозу. Злоумышленник может постепенно влиять на поведение агента, вводя вредоносные данные;

– хищение моделей и обратное проектирование представляют угрозу для интеллектуальной собственности и безопасности систем ИИ. Злоумышленники могут попытаться извлечь базовую модель или ее параметры с помощью различных методов, включая атаки с использованием инверсии модели или логического вывода о ее принадлежности. Для «агентов» ИИ риски хищения моделей выходят за рамки проблем, связанных с интеллектуальной собственностью, поскольку извлеченные модели могут быть использованы для разработки более эффективных перехватывающих атак на систему ИИ; похищенные модели могут быть использованы, чтобы прогнозировать стратегии агента и противодействовать им; для «агентов» ИИ, работающих с конфиденциальными данными (например, в сфере здравоохранения или финансов), кража модели потенциально может привести к раскрытию персональных данных и т.п.;

– атаки на визуальные и языковые модели посредством всплывающих окон. Автономные системы ИИ, работающие на базе больших визуальных и языковых моделей (Vision and Language Models, VLM), показали значительные перспективы в выполнении различных задач, включая просмотр веб-страниц для бронирования поездок или управление программным обеспечением в персональном компьютере. Эти задачи требуют от систем ИИ понимания графических пользовательских интерфейсов и эффективного взаимодействия с ними, что обеспечивается интеграцией визуальной и лингвистической обработки. Поскольку визуальные входные данные становятся все более важными для приложений с ИИ, понимание рисков и уязвимостей, связанных с такими системами, становится критическим. При этом последствия такой визуальной интеграции для безопасности остаются недостаточно изученными [1, р. 373–375].

Безопасность ИИ в таких случаях – часть предмета кибербезопасности. Кибербезопасность организуется технически, а также все больше гарантируется юридически. Так, в современном взаи-

мосвязанном мире международные подходы и национальное нормативное регулирование в сфере кибербезопасности выступает на передний план. Как указывают эксперты в сфере кибербезопасности Джейсон Эдвардс и Гриффин Вивер, в значительной степени это связано с тем, что компании и организации, в том числе коммерческой направленности, по мере своего развития расширяют свое цифровое присутствие за пределами национальных границ, работая одновременно в нескольких юрисдикциях. Это расширение подпитывается многочисленными достижениями в области цифровых технологий, которые делают трансграничные операции не просто стратегическим преимуществом, но и необходимостью в мире, где конкуренция и сотрудничество больше не ограничены географическими рамками [3, p. 299].

Нормативные правовые акты в области кибербезопасности приняты и действуют во многих странах, и каждый из них разработан в соответствии с потребностями, вызовами и культурными особенностями соответствующих стран. Законы и другие нормативные правовые акты применяются правительствами государств для обеспечения безопасности цифровых операций в пределах своей юрисдикции и защиты персональных данных своих граждан. Эти законы могут охватывать широкий спектр таких вопросов, как конфиденциальность персональных данных, суверенитет данных, уведомление об их утечке и требования к мерам кибербезопасности и др. Главной целью является создание более надежной цифровой среды, в которой предприятия могут безопасно работать, а граждане – доверять цифровой экономике [3, p. 300].

При активном участии Российской Федерации была разработана и принята резолюцией 79/243 ГА ООН от 24.12.2024 г. Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (далее – Конвенция). Хотя Конвенция не содержит прямых положений, регулирующих вопросы безопасности ИИ, она создает основу для решения ряда важных аспектов эффективного регулирования безопасного ИИ. Целями данной Конвенции являются: «а) содействие принятию и укреплению мер, направленных на повышение эффективности и результативности предупреждения киберпреступности и борьбы с ней; б) поощрение, облегчение и укрепление международного сотрудничества в предупреждении киберпреступности и борьбе с

ней; и с) поощрение, облегчение и поддержка технической помощи и создания потенциала в целях предупреждения киберпреступности и борьбы с ней, особенно в интересах развивающихся стран» (ст. 1).

Конвенция, «если иное не указано в ней, применяется: а) к предупреждению и расследованию уголовных правонарушений, признанных таковыми в соответствии с настоящей Конвенцией, и преследованию за них, включая замораживание, арест, конфискацию и возвращение доходов от таких правонарушений; б) к сбору, получению, сохранению и передаче доказательств в электронной форме для целей уголовного расследования или судопроизводства, как это предусмотрено в статьях 23 и 35 настоящей Конвенции» (ст. 3).

Пока рано делать прогнозы и выводы об эффективности предложенных Конвенцией подходов и методов, однако ее потенциал в сфере борьбы с киберпреступностью в мире несомненен.

Безопасное применение искусственного интеллекта в правовой сфере

Стефан Майер из Технического университета прикладных наук Вилдау (Германия) (The Technical University of Applied Sciences) рассматривает «правовые вызовы» ИИ на примере трех сфер его применения в правовой системе: в сфере государственного управления и судебной деятельности; в сфере автономного транспорта; в сфере интеллектуальных прав [4, р. 9–22].

1. *Искусственный интеллект в сфере государственного управления и в судебной деятельности.* Уровень развития и потенциал ИИ делают его привлекательным для использования в государственном управлении, а также в судебной деятельности, правоохранительными органами, юридическим сообществом. Так, ИИ более десятилетия активно привлекается в качестве системы поддержки принятия решений правоохранительными органами в разных странах. Например, в ФРГ с 2019 г. судебные органы земли Северный Рейн-Вестфалия реализуют проект по проверке изымаемых файлов на содержание детской порнографии с помощью ИИ-технологий. Тем не менее автоматически отобранные файлы, которые, по оценке ИИ, могут содержать информацию об уголовном преступлении, должны подвергаться окончательной проверке человеком. Как отмечает автор, перспективы использования ИИ в правоохранительной деятельности – это достижение момента, ко-

гда оценки ИИ будут составлять окончательное решение, т.е. ИИ будет окончательно определять доказанность по составу преступления и определять вытекающие из этого правовые последствия [4, р. 20].

Огромные исследовательские усилия сегодня направлены на то, чтобы алгоритмически «имитировать» понимание текста и его юридический анализ в целях решения задач, стоящих перед органами судебной власти и практикующими юристами [ibid.].

Учитывая риски в связи с применением ИИ в правовой сфере, в законодательстве ряда государств предусматривается прямой запрет безусловного применения ИИ в правовой практике, например ст. 35а Закона об административном судопроизводстве Германии (Verwaltungsverfahrensgesetz (BVwVfG) = Administrative Procedures Act) [Ibid]. Аналогичным образом, например, ст. 22 Общего регламента ЕС по защите данных (General Data Protection Regulation) (GDPR) и ст. 11 Директивы (ЕС) 2016/680 о защите физических лиц в связи с обработкой персональных данных компетентными органами в целях предотвращения, расследования, выявления или судебного преследования уголовных преступлений или исполнения уголовных наказаний (Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties) по общему правилу запрещают «автоматизированное индивидуальное принятие решений».

По мнению С. Майера, такой консервативный подход со временем станет нежизнеспособным. Учитывая потенциал ИИ, процесс принятия решений с помощью ИИ в будущем позволит избежать предвзятости со стороны человека, а также обеспечить единообразное применение закона при принятии юридически значимых решений [4, р. 21].

В связи с расширяющимся применением ИИ в правовой сфере экспертов и общественность беспокоят: во-первых, непредсказуемость функционирования ИИ; во-вторых, непрозрачность решений ИИ – как факторы, ограничивающие его широкое использование.

Вместе с тем, по утверждению С. Майера, чем больше ИИ будет «применять» закон, тем в большей степени он окажется способен соблюдать конкретные юридические требования при осуществлении властных полномочий, и, хотя «непредсказуемость» ИИ

может поставить под угрозу законность решений, которые он потенциально способен сформулировать, чиновники тоже подвержены риску принятия незаконных решений – будь то на основе ошибки либо в силу личной мотивации, которых нельзя исключить даже при самой тщательной подготовке государственных служащих. То есть, ограничение использования ИИ для осуществления государственной власти в силу «непредсказуемости» этой технологии может быть обосновано только тщательным сравнительным анализом склонности человека, с одной стороны, и ИИ – с другой, к ошибкам в правоприменении [ibid.].

Фактор «непрозрачности» ИИ составляет основание для ограничения использования ИИ в правовой сфере, поскольку, по общему правилу, правореализующие решения должны быть юридически понятными и поддающимися проверке. Поэтому, например, государственные органы должны дополнять принимаемые ими решения изложением причин, их обосновывающих. Однако алгоритмический путь, который выбирает самообучающийся ИИ для достижения искомого результата, технически невозможно сделать прозрачным во всей полноте. По этой причине «алгоритмическое управление» критикуется юристами, а в области компьютерных наук предпринимаются попытки решить эту проблему «непрозрачности» ИИ путем проведения исследований в области «объяснимого ИИ» («Explainable AI») ¹ [4, p. 21].

Вывод, к которому приходит С. Майер, – препятствия к безопасному применению ИИ в правовой сфере в принципе преодолимы, если не относиться к нему как «постоянному препятствию» для использования ИИ органами власти различного уровня и компетенции [Ibid].

2. *Применение искусственного интеллекта в автономном вождении.* В качестве интересного примера вызовов, возникающих вследствие применения ИИ, С. Майер выделяет проблематику автономного вождения в сфере дорожного движения на дорогах общего пользования. Это связано с заинтересованностью в широком внедрении автономного транспорта в повседневную жизнь, с одной стороны, и дискусионностью вопроса юридической ответ-

¹ *Объяснимый искусственный интеллект* – набор процессов и методов, которые позволяют пользователям-людям понимать и доверять результатам и выводам, созданным алгоритмами машинного обучения (см.: Что такое объяснимый ИИ? – URL: <https://www.ibm.com/think/topics/explainable-ai>) (дата обращения: 15.11.2025).

ственности в случае ДТП с участием автономных транспортных средств – с другой.

Вопросы массового внедрения автономных ТС в дорожном движении, а также юридической ответственности в случае ДТП с их участием находятся в фокусе внимания законодательных органов многих стран мира. Тем не менее в большинстве юрисдикций, если автономное ТС становится причиной аварии с травмами и / или материальным ущербом из-за нарушения правил дорожного движения, уголовная ответственность не предусмотрена: пользователь системы автономного ТС ей не управляет, а, следовательно, не несет ответственности за небрежность; производитель, по крайней мере в том случае, если возник «просто» риск автономного вождения, не несет уголовной ответственности, поскольку такие риски считаются «допустимыми». Аналогичным образом не существует третьих сторон, которые могли бы быть привлечены к уголовной ответственности за нарушение правил дорожного движения [4, р. 19]. С. Майер проводит – в этом случае – аналогию с естественным причинам повреждения (например, смерть от удара молнии на открытом воздухе). Так, в случае естественных причин общество не ожидает, что кто-то будет привлечен к уголовной ответственности. В отличие от этого, подчеркивает автор, автомобиль – это артефакт, который используется в интересах отдельных людей. Поэтому сомнения в приравнивании его к «естественным» причинам повреждений представляются обоснованными. Возникает вопрос, готово ли общество признать, что никто не должен нести уголовной ответственности в случае серьезных дорожно-транспортных происшествий, вызванных автономным транспортным средством?

С. Майер полагает, что это – очевидный пробел в законодательстве об уголовной ответственности, и он может стать косвенным препятствием для развития и внедрения инноваций вообще, не говоря о том, что является существенным упущением законодателя и требует скорейшего устранения в глазах общественного мнения и этики [ibid.].

Решением отчасти может быть обязанность производителя постоянно контролировать свои автономные системы вождения после их появления на рынке (и дорогах). Нарушение этой обязанности, по мнению С. Майера, может получить квалификацию уголовного преступления. Кроме того это послужит дополнительной мотивацией для производителя надлежащим образом проводить мониторинг, что, в свою очередь, дополнительно повысит вероят-

ность устранения выявленных недостатков конструкции (например, путем обновления программного обеспечения и т.п.). В итоге предлагаемый подход к назначению уголовной ответственности, как утверждает С. Майер, дополнительно будет скорее способствовать инновациям, чем препятствовать им [ibid.].

3. *Искусственный интеллект и интеллектуальные права.* По общему правилу, законодательство большинства стран мира требует факта личного интеллектуального творчества (человека) – для того чтобы какое-либо произведение получило защиту авторского права. Например, Европейский суд (European Court of Justice) рассматривает это требование как принцип законодательства ЕС.

Согласно законодательству Германии, для получения правовой защиты произведения должны быть «личными интеллектуальными творениями», о чем говорит раздел 2(2) Закона об авторском праве и смежных правах 1965 г. (Urheberrechtsgesetz (UrhG) = Act on Copyright and Related Rights, UrhG). То есть, для признания авторского права требуется творческая активность конкретного человека, интеллектуальный и личный труд автора (соавторов). При этом, даже если отдельные компоненты произведения были созданы автоматически, оно может заслуживать правовой охраны.

В последнее время, однако, как обращает внимание С. Майер, появляется все больше «художественных» и «литературных» произведений, созданных исключительно ИИ. Например, «Следующий Рембрандт»¹ («The Next Rembrandt») – произведения, созданные самообучающимся ИИ на основе подражания стилю этого художника. В качестве обучающих данных для них использовалась коллекция картин Рембрандта. Еще один пример: в 2018 г. сгенерированная с помощью ИИ картина «Эдмонд де Белами» была продана на аукционе за 432 тыс. долл.² Она была сформирована из анализа около 15 тыс. картин, созданных в период с XIV по XIX в.

Оценка охраноспособности таких «произведений» ИИ, как указывает С. Майер, на практике схожа с решениями, принимающимися в отношении произведений, созданных случайным генера-

¹ The Next Rembrandt. – URL: <https://www.vml.com/work/next-rembrandt> (дата обращения: 15.11.2025).

² Obvious and the Interface Between Art and Artificial Intelligence: As Christie's Becomes the First Auction House to Offer an Artwork Created by an Algorithm, We Ask if AI is Set to Become Art's Next MEdium. 12 December 2018. – URL: <https://www.christies.com/en/stories/a-collaboration-between-two-artists-one-human-one-a-machine-0cd01f4e232f4279a525a446d60d4cd1> (дата обращения: 15.11.2025).

тором: согласно сложившимся подходам, такого рода произведения, чтобы получить правовую охрану, требуют определенного уровня человеческого участия, т.е. интеллектуального вклада человека в конечный продукт. Например, автор может создать несколько шаблонов, которые затем обрабатываются при помощи генератора случайных чисел. Работа самого генератора случайных чисел при этом расценивается лишь как имитация шаблонов художника-автора, т.е. стиля данного художника [4, р. 11].

Сам по себе стиль как таковой не подлежит правовой охране, и конкретное творческое влияние человека на конечный продукт, как например в вышеописанном случае, отсутствует. На практике зачастую применяется метод введения дополнительного требования к произведению, чтобы признать его соответствующим уровню охраноспособности: «автор» должен выбрать, какой из различных результатов работы генератора случайных чисел может быть представлен в качестве «произведения искусства». Другой подход состоит в том, что достаточно простого предъявления «произведения» – «объекта», который кажется «художественным», – чтобы предоставить по нему защиту авторских прав. С. Майер указывает на еще один существующий подход, при котором защита авторских прав на «произведение» ИИ будет предоставляться, если данные для обучения ИИ при создании этого произведения были основаны на работах художника – человека, который использует данное приложения ИИ, и т.п. [ibid.].

Приведенные выше примеры «произведений» ИИ, – «Следующий Рембрандт» и «Эдмонд де Белами», – как указывает С. Майер, не отвечают ни одному из приведенных подходов, предоставляющих защиту авторских прав произведениям, выполненным средствами ИИ. Эффективное правовое признание «произведений» ИИ охраноспособными, по мнению С. Майера, – принятие в юридической практике так называемой «доктрины отбора» (т.е. когда человек выбирает, какое из сгенерированных ИИ «произведений» заслуживает таковым являться). Сегодня, однако, приходится признать, что защита авторских прав в отношении «произведений», созданных с помощью ИИ, практически отсутствует [Ibid].

Актуальный вопрос для правоведов состоит в том, должны ли в принципе «произведения», созданные с помощью ИИ, подпадать каким-либо образом под авторское право: очевидно, что «творческий ИИ» будет становиться все более мощным и, возможно, в ближайшее время выйдет за рамки простой эклектики. С. Майер подчеркивает, что законодатель сегодня располагает

значительной свободой действий в сфере распределения интеллектуальных прав по различным аспектам инновационной политики, включая произведения ИИ [4, р. 12].

Правовые решения по безопасности искусственного интеллекта

С. Майер полагает, что имеющиеся проблемы и недостатки как в части правотворчества, так и в плане правоприменения в отношении ИИ и вопросах его безопасного использования, подразумевают, что в развитии законодательства об ИИ требуется четко учитывать два аспекта: 1) соразмерность интересов третьих лиц в ИИ и гарантий базовых прав граждан; 2) оценка рисков от внедрения технологий ИИ [4, р. 22–23].

Так, на первый взгляд, развитие правового регулирования в сфере технологий предполагает обеспечение баланса основных экономических прав производителей и распространителей технологий в отношении основных прав тех, кому такие технологии могут причинить вред, будь то права на защиту персональных данных или физическую неприкосновенность и др.

Однако новые технологии выгодны не только производителям и дистрибьюторам, но и массам их пользователей – в повседневной жизни в том числе. Этот аргумент, безусловно, признается регулируемыми органами и порой используется в качестве обоснования в поддержку внедрения новых технологий (например, снижение смертности на дорогах благодаря автономному вождению). При этом законодатели уделяют недостаточно внимания ограничивающему регулированию технологий, когда юридически оказывается допустимым, что будут ущемлены основные права (например пациенты, которые умирают из-за того, что медицинский ИИ, который мог бы в противном случае спасти им жизнь, стал доступен слишком поздно). Неопределенность относительно того, действительно ли новая технология могла быть доступна ранее в отсутствие ее нормативного регулирования, не может служить аргументом против юридической значимости причинения вреда третьей стороне, вызванного этим (отсутствием) регулированием, полагает С. Майер. Речь идет о принципе предосторожности, основная цель которого, особенно в вопросе о применении технологий ИИ, состоит в том чтобы разрешать применение этой технологии до того, как будет выявлен и установлен (потенциальный) вред, ею наносимый [4, р. 23].

Однако, в том числе на международном уровне, получил распространение «подход, основанный на оценке рисков» (risk-based approach), которому следует, например, Евросоюз. Этот подход имеет два элемента. Во-первых, требуется научное подтверждение потенциальной способности технологии причинять вред («опасность»). Во-вторых, должна существовать некоторая вероятность того, что юридический актив, который должен быть защищен нормативным актом, действительно может подвергнуться такой опасности в связи с планируемым использованием технологии («воздействие»). Поэтому требуется оценка конкретного использования технологии («оценка воздействия»).

Следуя этой «схеме», например, Евросоюз, как правило, ориентируется на создание процедуры допуска продукта на рынок, а не на свойства и качество самого продукта. Это относится и к системам и технологиям ИИ, которые, если будут отнесены к категории «высокого риска», будут регулироваться наложением множества стандартных нормативных обязательств на поставщиков, импортеров, дистрибьюторов и пользователей [4, p. 24].

Безопасность и конфиденциальность искусственного интеллекта в стандартах и правилах международных организаций

Авторы книги «Понимание принципов работы ИИ в сфере кибербезопасности и безопасного ИИ: проблемы, стратегии и тенденции (прогресс в сфере ИИ)» [5] – Дилли Прасад Шарма из Университета Торонто (University of Toronto), Араш Хабиби Лашкари, Йоркский университет (York University), Махди Дагмехчи Фирузджаи, Университет Макьюэн (MacEwan University), Самане Махдавифар, Университет Макгилла (McGill University), Пулей Сюн, Национальный исследовательский совет Канады (National Research Council of Canada) – в своем исследовании обращают внимание на то, что безопасность и конфиденциальность ИИ стали важнейшими приоритетами в развитии нормативного регулирования, по мере того как технологии ИИ все больше интегрируются в глобальные отрасли и повседневную жизнь. В связи с этим были разработаны определенные международные стандарты и нормы, дающие рекомендации по снижению рисков и обеспечению этичного использования ИИ – для государств и частных компаний и организаций [5, p. 216–220]. Это, в частности, проекты ISO – ISO/IEC DIS 27090 «Кибербезопасность – Искусственный интеллект – Руководство по устранению угроз безопасности и компро-

метации систем искусственного интеллекта»¹; ISO/IEC DIS 27091 «Кибербезопасность и конфиденциальность – Искусственный интеллект – Защита конфиденциальности»². Эти стандарты охватывают все этапы жизненного цикла ИИ, от сбора данных до системной интеграции, обеспечивая надежное руководство для государств и организаций, соответствующее глобальным требованиям безопасности и этики.

Важную роль в разработке стандартов, обеспечивающих безопасное и прозрачное внедрение технологий ИИ, играет Европейский институт по стандартизации в области телекоммуникаций (European Telecommunications Standards Institute) (далее – ETSI). Рекомендации ETSI особенно востребованы для таких отраслей, как телекоммуникации, где надежность систем ИИ имеет первоочередное значение. Они направлены на предотвращение злоупотреблений и уязвимостей, повышают доверие к приложениям ИИ, используемым для критически важной инфраструктуры и сервисов.

Технический комитет ETSI по защите искусственного интеллекта (TC SAI) ориентируется в своей работе на то, чтобы повысить безопасность ИИ путем разработки высококачественных технических стандартов и рассматривает четыре основных аспекта стандартизации безопасности ИИ: 1) техническая защита ИИ от атак; 2) смягчение последствий, вызванных техническими проблемами с ИИ; 3) применение ИИ для противодействия техническим атакам; 4) аспекты общественной безопасности при использовании и применении ИИ³.

Работы по стандартизации ETSI адресованы всем заинтересованным сторонам, включают конечных пользователей, производителей, операторов и правительства [5, p. 214].

Принципы ИИ ОЭСР (OECD AI Principles⁴) представляют собой первый межправительственный стандарт в области ИИ, ус-

¹ ISO/IEC DIS 27090 Cybersecurity – Artificial Intelligence – Guidance for Addressing Security Threats and Compromises to Artificial Intelligence Systems. – URL: <https://www.iso.org/standard/56581.html> (дата обращения: 15.11.2025).

² ISO/IEC DIS 27091 Cybersecurity and Privacy – Artificial Intelligence – Privacy protection. – URL: <https://www.iso.org/standard/56582.html> (дата обращения: 15.11.2025).

³ Securing Artificial Intelligence (SAI). – URL: <https://www.etsi.org/technologies/securing-artificial-intelligence> (дата обращения: 15.11.2025).

⁴ OECD AI Principles. – URL: <https://www.oecd.org/en/topics/ai-principles.html> (дата обращения: 15.11.2025).

танавливающий глобальный ориентир для разработки и внедрения надежных систем ИИ.

Принципы ИИ ОЭСР основаны на пяти ключевых ценностях: 1) инклюзивный рост, устойчивое развитие и благополучие: ИИ должен вносить позитивный вклад в прогресс общества, поддерживая устойчивое развитие и повышая благосостояние; 2) ориентированные на человека ценности и справедливость: системы искусственного интеллекта должны уважать человеческое достоинство и права личности, обеспечивая справедливость при их разработке и применении; 3) прозрачность и объяснимость: системы искусственного интеллекта должны работать прозрачно и их решения должны быть понятны, укреплять доверие и подотчетность; 4) надежность и защищенность: системы искусственного интеллекта должны быть устойчивыми, защищенными и безотказными, сводя к минимуму риски и обеспечивая безопасную эксплуатацию; 5) подотчетность: организации и разработчики должны нести ответственность за воздействие и конечные результаты своих систем искусственного интеллекта, обеспечивая эффективный надзор [5, р. 216–217].

Чтобы содействовать реализации этих принципов, ОЭСР предлагает пять практических рекомендаций для правовой политики в сфере ИИ национальных государств: 1) инвестиции в исследования и разработки в области искусственного интеллекта; 2) содействие созданию цифровой экосистемы для ИИ; 3) формирование благоприятной политической среды; 4) наращивание человеческого потенциала и подготовка к трансформации рынка труда; 5) международное сотрудничество для обеспечения надежности ИИ [5, р. 217].

Заключение

Безопасность применения ИИ в общественной и правовой жизни определяется, с одной стороны, особенностями систем ИИ, с другой – особенностями сфер их приложения в социальной практике.

Системы ИИ могут создавать социальные риски, но и сами при этом подвержены рискам и уязвимостям, что ставит под угрозу их безопасность. Уязвимости ИИ в техническом плане подразделяются на: случайные сбои и преднамеренные атаки. Риски ИИ в социально-правовой сфере определяются сферой применения ИИ.

Существует экспертное мнение, что в том случае, если регулирование искусственного интеллекта будет специфичным для каждой отдельной области его применения, как например это происходит в сфере автономного транспорта, угрозы и риски безопасности его эксплуатации могут быть существенно снижены, – с чем, в целом, можно согласиться.

Сегодня разрабатываются первые нормативные акты и международные стандарты в области безопасности применения ИИ, однако остается много вопросов в развитии правового регулирования применения ИИ как на национальном, так и на международном уровнях.

Список литературы

1. Agentic AI: Theories and Practices / ed. Ken Huang. – Cham: Springer, 2025. – 438 p.
2. Artificial intelligence in application: Legal aspects, application potentials and use scenarios / ed. T. Barton, C. Müller. – Wiesbaden: Springer, 2024. – 208 p.
3. Edwards J., Weaver G. The Cybersecurity Guide to Governance, Risk, and Compliance. – Hoboken: Wiley, 2024. – 672 p.
4. Meyer S. Legal Challenges of Artificial Intelligence and How to Manage Them // Artificial intelligence in application: Legal aspects, application potentials and use scenarios / ed. T. Barton, C. Müller. – Wiesbaden: Springer, 2024. – P. 9–30.
5. Understanding AI in Cybersecurity and Secure AI: Challenges, Strategies and Trends / D.P. Sharma, A.H. Lashkari, M.D. Firoozjaei, S. Mahdaviifar, Pulei. Xiong. – Cham: Springer, 2025. – 255 p.

АЛФЕРОВ О.Л.¹, АЛФЕРОВА Е.В.² ИНТЕГРАЦИЯ НАДЕЖНЫХ МЕХАНИЗМОВ ПРАВОВОЙ ЗАЩИТЫ В СИСТЕМУ УПРАВЛЕНИЯ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ (Обзор)

Аннотация. В обзоре представлены точки зрения некоторых исследователей на взаимосвязи между нормативно-правовой базой, этическими концептами и развивающимися технологиями, на пробелы и противоречия в законодательстве в области управления ИИ и на механизмы защиты прав человека, предотвращения или смягчения потенциального вреда, связанного с ИИ. Анализ законодательства позволяет авторам предложить эффективные правовые меры против необоснованного вторжения в частную жизнь, дискриминационной практики, несправедливых решений в сфере жилья, уголовного правосудия и многих других областей. Предлагается четко урегулировать ответственность за вред, причиненной искусственным интеллектом, упорядочить правила возмещения вреда и устранения негативных последствий функционирования систем искусственного интеллекта.

Ключевые слова: искусственный интеллект; генеративный искусственный интеллект; правовая защита; юридическая ответственность; справедливость; закон об искусственном интеллекте; фундаментальные права; управление искусственным интеллектом; правовое регулирование технологий искусственного интеллекта.

ALFEROV O.L., ALFEROVA E.V. Integration of reliable legal protection mechanisms into the artificial intelligence management system (Review)

¹ *Алферов Олег Леонидович*, ведущий редактор отдела правопведения ИНИОН РАН.

² *Алферова Елена Васильевна*, ведущий научный сотрудник отдела правопведения ИНИОН РАН, кандидат юридических наук.

Abstract. The review presents the views of some researchers on the relationship between the regulatory framework, ethical concepts and emerging technologies, gaps and contradictions in AI management legislation, and mechanisms to prevent or mitigate potential harm associated with AI. The analysis of legislation allows the authors to propose effective legal measures of liability for damage caused by artificial intelligence, and compensation for damage, as well as elimination of negative consequences of the functioning of artificial intelligence systems.

Keywords: artificial intelligence; generative artificial intelligence; legal protection; legal responsibility; justice; law on artificial intelligence; fundamental rights; artificial intelligence management; legal regulation of artificial intelligence technologies.

Для цитирования: Алферов О.Л., Алферова Е.В. Интеграция надежных механизмов правовой защиты в систему управления искусственным интеллектом (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2026. – № 1. – С. 125–141. – DOI: 10.31249/iajpravo/2026.01.08

Введение

Системы ИИ все больше интегрируются во многие ключевые отрасли, такие как здравоохранение, финансы, трудоустройство, уголовное судопроизводство, образование и другие. Преимущества, связанные с повышением эффективности их функционирования в эпоху ИИ, идут рука об руку со значительными проблемами, обусловленными многочисленными рисками нарушения основных прав и причинения вреда в результате необоснованного вторжения в частную жизнь, дискриминационной практики, несправедливых решений в сфере жилья, уголовного правосудия и многих других областей. К сожалению, люди, которые становятся жертвами правонарушений с помощью искусственного интеллекта, могут оказаться бессильными без эффективных средств правовой защиты их прав.

В данном обзоре представлены точки зрения некоторых исследователей – участников Кембриджского форума «Искусственный интеллект: право и управление» [2], указывающих на настоятельную потребность интеграции надежных механизмов правовой защиты основных прав человека в систему управления ИИ, поскольку технологии ИИ все шире внедряются в жизнь государства

и общества и представляют определенную угрозу. Технологии ИИ могут ограничивать личную свободу, разрушительно влиять на индивидуальное самоопределение; они уязвимы для некоторых людей, неспособных понять и работать с ИИ, и др. Управление ИИ должно защищать права и интересы всех людей, на которых влияют системы ИИ, регулировать способы предотвращения вреда, причиняемого ИИ, и обеспечивать возмещение ущерба, когда вред уже нанесен.

Индивидуальные меры защиты в эпоху искусственного интеллекта: справедливые алгоритмы, справедливое регулирование, справедливые процедуры

Традиционная правовая доктрина требует, чтобы для предотвращения или смягчения рисков нарушения основных прав были созданы новые меры защиты, а существующие – усилены. Защита основных прав лежит в основе международного права и национальных нормативных правовых актов и академических идей, связанных с технологиями ИИ. *Люпчо Гродзановский* и *Джером Де Куман Аннот* из Льежского университета (Бельгия) считают, что в условиях внедрения ИИ в разные сферы жизни возникает необходимость в усилении индивидуальных мер защиты с помощью реализации субъективных прав человека, закрепленных в законе [3].

Понятие «индивидуальная защита» авторы рассматривают как *нормативную цель защиты* индивидуальных прав и *право требовать* определенного вида защиты или охраны. Предполагается, что «справедливый» закон защищает свободу и равенство личности. В социальных и гуманитарных науках «справедливость» всегда рассматривалась как основополагающее, но неуловимое понятие. По мере того как технологии ИИ демонстрировали свою способность причинять вред, ученые поднимают вопросы о справедливости, которые не могли должным образом охватить стандартные нормативные и научные теории. Реакция специалистов по этике заключалась в том, чтобы вернуться к классике и заложить основы «новой» этической системы, в рамках которой в конечном итоге можно было бы ввести в действие законодательство об ИИ. Так называемая «классика» – это три основных направления в этике: добродетельное, утилитаристское и деонтическое [3].

Учитывая роль ИИ, Л. Гродзановский и Дж. Де Куман утверждают, что «защита личности» как цель *справедливого* регули-

рования оправдана именно потому, что технологии ИИ могут подорвать ключевые требования справедливости (свободу и равенство личности), порождая новые формы неравенства и ограничивая способность людей свободно и осмысленно действовать [3].

О каких угрозах идет речь?

Во-первых, *об ограничении личной свободы*. По мнению авторов, угроза того, что ИИ будет принуждать людей принимать решения, которые они вероятно не приняли бы, если бы обладали полной (свободной от ИИ) проницательностью, стала чемто обыденным.

Во-вторых, *о разрушительном влиянии ИИ на индивидуальное самоопределение и непрозрачности ИИ* и отсутствии должного человеческого контроля и надзора.

В-третьих, *об уязвимости некоторых людей из-за их неспособности понять и работать с новыми технологиями*. Конечно, не все люди одинаково осведомлены об угрозах, связанных с технологиями ИИ. Некоторые группы характеризуются особенностями, которые повышают вероятность того, что они станут жертвами манипуляций со стороны ИИ. В своей книге Джанклаудио Мальджери¹, на которую ссылаются авторы, выделил четыре архетипические «неспособности», которые характеризуют или усиливают уязвимость людей: неспособность понять информацию об обработке данных; неспособность понять риски, их значение и последствия; неспособность дать действительное согласие и неспособность надлежащим образом реализовать права на защиту данных (цит. по: [3]).

Среди примеров несправедливости, которую могут вызывать технологии ИИ, наиболее заметным и актуальным примером признается дискриминация, которая приводит к исключению и маргинализации определенных групп². Есть ряд секторов, таких как биометрия, критически важная инфраструктура, образование и профессиональная подготовка, трудоустройство и доступ к основным государственным услугам, общей чертой которых является вероятность дискриминации.

В-четвертых, *об угрозе справедливости, исходящей от ИИ*. Здесь Л. Гродзановский и Дж. де Куман усматривают два ключе-

¹ Malgieri G. Vulnerability and Data Protection Law. – Oxford: Oxford Univ. Press, 2023. – 308 p.

² Ethics guidelines for trustworthy AI. – URL: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (дата обращения: 11.10.2025).

вых аспекта. Первый – *инструментальный*: справедливость выступает как средство достижения индивидуальной защиты. Ключевую роль здесь играют концепции, заложенные в законы об ИИ. В качестве положительного примера авторы приводят Закон ЕС об ИИ (AI Act), положения которого направлены на защиту разумных и добровольных действий людей, а также их равного доступа к различным правам и льготам и пользования ими (например, право на объяснение, льготы в так называемых секторах повышенного риска).

Второе измерение взаимосвязи гарантий и справедливости – *консеквенциалистское*: при эффективном применении материальные и процессуальные индивидуальные гарантии направлены на достижение справедливых результатов. Действительно, материальные права (защита данных, неприкосновенность частной жизни, недискриминация и т.д.) и процессуальные права (доступ к средствам правовой защиты и правосудию, эффективное судебное возмещение ущерба) обеспечивают гарантии и защитные механизмы, на которые люди могут полагаться, чтобы либо предотвратить несправедливый исход (например нарушение основного права), либо исправить его, если он уже произошел (например, возместить причиненный ущерб) [ibid.].

Право на возмещение ущерба является основополагающим правом человека, необходимым для устранения нарушений прав и свобод. Важность механизмов возмещения ущерба закреплена в международных документах по правам человека, таких как ст. 8 Всеобщей декларации прав человека, ст. 2 Международного пакта о гражданских и политических правах и др.

Расширение возможностей управления искусственным интеллектом с помощью механизмов возмещения ущерба

Управление ИИ, подчеркивают *Юлу Пи* (Центр междисциплинарных методологий Уорикского университета (Великобритания)) и *Мэдди Проктор* (Центр социальных исследований Гарвардского университета (США)), должно защищать права и интересы всех людей, на которых влияют системы ИИ, предусматривая возможность предотвращения вреда, причиняемого ИИ, и возмещения ущерба, когда вред уже нанесен. Обеспечить условия для устранения как индивидуального, так и коллективного вреда, причиненного ИИ, по их мнению, можно двумя важнейшими способами: 1) создание надежных механизмов возмещения ущерба,

которые предоставляют отдельным лицам и сообществам официальные возможности для получения компенсации или принятия корректирующих мер; и 2) гарантия возмещения ущерба для всех, кто пострадал от систем ИИ [4].

Возмещение ущерба – комплекс мер, направленных на устранение вреда или негативных последствий, с которыми сталкиваются отдельные лица или сообщества в результате неправомерных действий. Цель возмещения ущерба – устранить или исправить нежелательную или несправедливую ситуацию. Пострадавшие лица могут добиваться принятия этих мер различными способами, включая судебные механизмы (национальные или региональные суды, международные правозащитные организации), государственные внесудебные механизмы (регулирующие органы, омбудсмен, органы по рассмотрению жалоб) и внутренние механизмы подачи жалоб в компаниях. Хотя возмещение ущерба может ассоциироваться у людей с денежной компенсацией, результат процесса возмещения ущерба может принимать различные формы, включая реституцию, компенсацию, реабилитацию, удовлетворение и гарантии неповторения.

В контексте несправедливости, связанной с искусственным интеллектом, Ю. Пи и М. Проктор (со ссылкой на других исследователей) выделяют два типа результатов возмещения ущерба: *восстановительный* и *карательный*. Восстановительное возмещение ущерба направлено на «возмещение материального возмещения ущерба стороне или жертве в результате неправомерного действия в результате нарушения ее прав, в то время как карательное возмещение ущерба предполагает наказание правонарушителя, часто в судебном порядке. Доступ к механизмам возмещения ущерба способствует всестороннему расследованию нарушений прав человека и причиненного вреда, позволяя надлежащим образом устранять ущерб, выплачивать компенсацию жертвам и привлекать к ответственности виновных» [ibid.].

Для управления ИИ с целью защиты отдельных лиц и общества от потенциального вреда, причиняемого ИИ, авторы предлагают использовать два основных подхода: *упреждающий* и *постфактумный*. Различие между этими механизмами регулирования ИИ состоит в предмете спора и времени его возникновения. Так, механизмы *ex-ante* (с лат. – до события) – это перспективные инструменты, которые вступают в силу до развертывания системы ИИ и начала ее воздействия на пользователей, в то время как механизмы *ex-post* применяются после развертывания системы и начала ее

работы. Акцент на важности механизма возмещения ущерба как постфактумной меры по устранению вреда, связанного с ИИ, по мнению авторов, не призван умалить легитимность и значимость превентивных мер. Скорее, речь идет о необходимости комплексного подхода к защите общества от потенциальных рисков и последствий, связанных с ИИ. Предварительные меры, такие как оценка рисков, этические рекомендации, например Организации экономического сотрудничества и развития¹; Организация Объединенных Наций по вопросам образования и организации² и технические стандарты проектирования и разработки Международной организации по стандартизации³, играют решающую роль в понимании, предотвращении и смягчении вреда, связанного с ИИ. Эти меры помогают обеспечить ответственное проектирование, разработку и внедрение систем ИИ с целью минимизации вероятности негативных последствий [4].

Признавая важный пробел в комплексном подходе к защите общества от потенциальных рисков и последствий, Ю. Пи и М. Проктор отмечают появление существенных законодательных новелл, например в последней версии Закона ЕС об ИИ⁴ и Белой книге о регулировании ИИ в Великобритании⁵. Эти акты, по их мнению, значительно усилили внимание к механизмам защиты и возмещения ущерба в ответ на вред, наносимый ИИ. Изначально Закон ЕС об ИИ, предложенный Еврокомиссией в апреле 2021 г.

¹ Organisation for Economic Co-operation and Development // OECD AI principles. – 2019. – URL: <https://oecd.ai/en/ai-principles> (дата обращения: 11.10.2025).

² United Nations Educational, S., & Organization, C. Recommendation on the ethics of artificial intelligence. – 2021. – URL: <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics> (дата обращения: 11.10.2025).

³ International Organization for Standardization. ISO/IEC TR 24027:2021 information technology – Artificial. – 2021. – URL: <https://www.iso.org/standard/81230.html> (дата обращения: 11.10.2025).

⁴ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). – URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (дата обращения: 11.10.2025).

⁵ UK's Department for Science, I. and Technology. Implementing the UK's AI regulatory principles: Initial guidance for regulators. – 2024. – URL: https://assets.publishing.service.gov.uk/media/65c0b6bd63a23d0013c821a0/implementing_the_uk_ai_regulatory_principles_guidance_for_regulators.pdf (дата обращения: 11.10.2025).

(вступил в силу 1 августа 2024 г.), подвергался критике за то, что в нем не были должным образом учтены проблемы, связанные с правами человека, из-за отсутствия надежного механизма подачи жалоб и возмещения ущерба. Однако последующие изменения значительно улучшили ситуацию¹. В пересмотренном Законе теперь учитываются права отдельных лиц. В частности, для гарантии этих прав в Закон ЕС об ИИ были добавлены ст. 85, 86 и 99(10). Статья 85 позволяет отдельным лицам или группам лиц подавать жалобы в органы надзора за рынком, если их права, предусмотренные Законом, нарушаются системой ИИ. Статья 86 обеспечивает право на получение разъяснений по результатам работы систем ИИ с высоким уровнем риска, которые влияют на законные права, здоровье, безопасность, социально-экономический статус или другие основные права. Статья 99(10) предусматривает эффективные средства правовой защиты и надлежащую правовую процедуру в отношении действий органов по надзору за рынком. Этих прав не было в первоначальном проекте закона, что является важным шагом на пути к эффективному индивидуальному возмещению ущерба [4].

Аналогичным образом в Белой книге по регулированию ИИ, «пропорциональной и ориентированной на инновации нормативно-правовой базе», опубликованной правительством Великобритании 29 марта 2023 г., подчеркивается, что состязательность и возмещение ущерба являются важнейшими принципами².

Ю. Пи и М. Проктор выделяют несколько обязательных шагов достижения успехов в споре и возмещению вреда. *Первый – инициирование процесса*, который начинается с определения конкретных задействованных систем ИИ и понимания причиненного ими вреда. Однако, предупреждают они, этот шаг часто оказывается сложным из-за недостаточной прозрачности использования ИИ и запоздалого признания его негативных последствий. Отдельная проблема видится в том, что люди нередко не осознают, что они стали участниками процесса принятия решений на основе ИИ или столкнулись с контентом, созданным ИИ. Системы ИИ

¹ Engler A. Key enforcement issues of the AI act should lead EU trilogue debate. – URL: <https://www.brookings.edu/articles/key-enforcement-issues-of-the-ai-act-should-lead-eu-trilogue-debate/> (дата обращения: 11.10.2025).

² UK Department for Science, I. and Technology 2023. A pro-innovation approach to AI regulation. – URL: <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper> (дата обращения: 11.10.2025).

часто внедряются без публичного уведомления, из-за чего людям сложно идентифицировать эти системы и понять их последствия. Такое неосознание особенно проблематично в случаях ошибочных решений или институциональных нарушений. В связи с этим, полагают авторы, необходимо обеспечить введение правила информирования пользователей и заинтересованных лиц о том, как они должны взаимодействовать с системой ИИ. Такое правило имеет решающее значение, поскольку без него люди могут не понять, когда система ИИ причиняет вред, и им будет сложно начать процесс возмещения ущерба [4].

Еще одной серьезной проблемой, препятствующей началу процесса возмещения ущерба, является запоздалое признание вреда, причиненного ИИ.

Второй шаг после выявления ущерба – *определение наиболее подходящих способов возмещения ущерба*. Это могут быть внутренние механизмы подачи жалоб в компании, государственные внесудебные механизмы, такие как службы омбудсменов, и судебные органы.

Рассматривая проблемы, с которыми сталкиваются люди, стремящиеся к возмещению ущерба, Ю. Пи и М. Проктор на реальных примерах демонстрируют различные препятствия, возникающие на каждом этапе возмещения ущерба в ЕС и США. Отмечается, что подходы к регулированию в ЕС и США часто сравнивают из-за различий в моделях управления ИИ: в ЕС особое внимание уделяется нормативному надзору, а в США предпочтение отдается более рыночному и децентрализованному подходу. Изучив эти разные системы, авторы замечают, что ни одна из них в полной мере не удовлетворяет потребность в эффективных средствах правовой защиты для лиц, пострадавших от систем ИИ. Невершенство существующих механизмов правовой защиты подвергает людей значительным рискам, будь то утечка данных, аварии с участием автономных транспортных средств или алгоритмическая предвзятость.

Вывод исследователей: механизмы правовой защиты в условиях использования ИИ-технологий являются жизненно важными гарантиями, предоставляющими пострадавшим лицам возможность требовать компенсацию, исправления ошибок или, по крайней мере, пересмотр решений, принятых системами ИИ. Такие механизмы не только защищают права отдельных лиц, но и укрепляют доверие потребителей, что, в свою очередь, способст-

вует долгосрочному росту и этичному развитию индустрии ИИ [4].

Одним из таких механизмов является *омбудсмен по искусственному интеллекту*. Так, в Финляндии было принято примечательное решение омбудсмана, успешно восстановившее справедливость путем своевременного информирования потерпевшего лица и предотвращения дальнейшего нарушения его конфиденциальности. В 2020 г. Национальное бюро расследований Финляндии использовало программное обеспечение для распознавания лиц от Clearview AI для выявления потенциальных жертв сексуального насилия над детьми, не применяя надлежащих мер защиты конфиденциальности, таких как ограничения на срок хранения данных или передачу третьим лицам. Национальное управление полиции должно было уведомить о проекте финское Управление омбудсмана по защите данных, что они и сделали в 2021 г. после сообщения об утечке персональных данных. В ответ на это омбудсмен распорядился проинформировать пострадавших о взломе и удалить соответствующие персональные данные [4].

Важную роль в достижении справедливых результатов в случае крупномасштабного вреда, наносимого пользователям ИИ, играют регулирующие органы и службы защиты прав потребителей для получения компенсации. Например, Международная сеть по защите прав потребителей и правоприменению (International Network for Consumer Protection and Law Enforcement, ICPEN) – это международная организация, возглавляемая Федеральной торговой комиссией США (The Federal Trade Commission) (далее – FTC) и состоящая из 70 органов-членов. В США FTC обладает широкими полномочиями по возмещению ущерба, нанесенного ИИ. Раздел 5 Закона о FTC (Federal Trade Commission Act 1914), например, наделяет FTC полномочиями по регулированию недобросовестных и вводящих в заблуждение практик. Федеральная торговая комиссия может подавать в суд на компании и возмещать ущерб пострадавшим пропорционально, издавать судебные запреты, обязывающие компании прекратить вредоносную практику, или заключать долгосрочные соглашения о согласии, предусматривающие дальнейший мониторинг и штрафы. Так, в рамках проверки на предмет спам-звонков FTC в сотрудничестве с генеральными прокурорами штатов обратилась к поставщикам услуг в рамках «Операции по борьбе со спам-звонками» и объявила совместную операцию «Стоп спам-звонкам».

Во многих штатах США также действуют законы об ответственности за введение потребителей в заблуждение, например Закон о недобросовестной конкуренции в Калифорнии (the Unfair Competition Law, UCL), который позволяет отдельным потребителям подавать в суд с требованием о судебном запрете [ibid.].

Еще один шаг – *судебный пересмотр и возмещение ущерба в судебном порядке*. Гражданское право предлагает несколько способов возмещения ущерба в судебном порядке, в том числе в связи с ответственностью за качество продукции и халатностью. Вместе с тем, как отмечают Ю. Пи и М. Проктор, в США до сих пор не было ни одного успешного иска о возмещении ущерба в связи с качеством программного обеспечения. 23 октября 2024 г. Европарламент и Совет утвердили новую Директиву (ЕС) 2024/2853 об ответственности за дефектную продукцию (Directive (EU) on liability for defective products), которая распространяет ответственность за дефектную продукцию на цифровые продукты и программное обеспечение¹. Этот документ значительно снижает барьеры для истцов по всей Европе, которые могут подавать иски об ответственности за вред, причиненный ИИ. Критики утверждают, что это лишь полумера, которая не позволяет в полной мере решить проблему вреда, связанного с ИИ².

Неправомерное использования генеративного ИИ и его ответственность за аудиодипфейки

Учитывая реальные последствия использования ИИ, суды, политики и ученые изучают, как существующие режимы ответственности могут взаимодействовать с ИИ, чтобы стимулировать его безопасное развитие и использование. Однако, как замечают *Бао Кхам Чау* (Корнеллский технологический институт (США)) и *Джордж Хэ* (Лаборатории инноваций Гарвардской библиотеки), эти режимы не учитывают должным образом сложность обучения базовых генеративных моделей ИИ, не принимают во внимание то,

¹ European Council. EU brings product liability rules in line with digital age and circular economy. – 2024. – URL: <https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/eu-brings-product-liability-rules-in-line-with-digital-age-and-circular-economy/>.

² Hacker, P. The European AI liability directives – Critique of a half-hearted approach and lessons for the future, *Computer Law & Security Review*, 51 (2023), 105871. – 2023. – URL: <https://doi.org/10.1016/j.clsr.2023.105871>; <https://ssrn.com/abstract=4279796>

кому принадлежит инфраструктура для обработки данных, обучения моделей и их развертывания. Так, инструменты ИИ, позволяющие генерировать аудио, похожее на настоящее, становятся все более доступными и создают реальную угрозу для моделей, например монетизации существующих игроков музыкальной индустрии. Из-за сложной цепочки поставок данных трудно определить, кто несет ответственность за конкретное нарушение авторских прав. Такой подход к определению ответственного лица может привести к фатальным последствиям при распределении ответственности [1].

Существующие механизмы ответственности

По состоянию на декабрь 2024 г., отмечают Бао Кхам Чау и Дж. Хэ, в мире насчитывалось более 1600 политических инициатив, направленных на регулирование ИИ. В своей статье «Аудиодипфейки и регулирование со стороны “хозяев творчества”» они рассматривают три основные нормативно-правовые базы – американскую, европейскую и китайскую – в целях признать их глобальное влияние на развитие ИИ и управление им. В статье дается обзор этих баз и выявляются недостатки законодательства, особенно в том, что касается распределения ответственности за неправомерное использование генеративного ИИ. Анализ показал, что ни один из этих режимов не учитывает в достаточной мере то, что создатели базовых моделей, как их называют авторы – «хозяева творчества», – должны нести ответственность на разных этапах.

Так, в США разработка генеративного ИИ по большей части не регулируется. Несмотря на то что могут применяться такие механизмы, как судебная практика согласно Первой поправке и разд. 230 Закона о порядочности в сфере коммуникаций (the Communications Decency Act), они не обеспечивают всеобъемлющего нормативного регулирования. Более того, судья Горсач даже поставил под сомнение применимость ст. 230 к контенту, созданному ИИ (Gonzalez vs Google LLC, 2023) [1].

Всеобъемлющей федеральной системы ИИ не существует, утверждают Бао Кхам Чау и Дж. Хэ. Вместо этого несколько штатов, включая Калифорнию, Нью-Йорк и Иллинойс, приняли законы, касающиеся различных аспектов разработки и использования ИИ. Например, Калифорния приняла закон, требующий от своего Технологического департамента провести всестороннюю инвентаризацию всех высокорискованных вычислительных процессов,

полученных на основе машинного обучения, статистического моделирования, анализа данных, используемых в государственных учреждениях. Этот закон содержит перечень мер для снижения рисков или блокирования дискриминационных, предвзятых решений, принимаемых соответствующими вычислительными процессами (Cal. Gov't Code § 11,546.45.5, West). Аналогичным образом в штате Мичиган принят закон, требующий раскрытия информации о том, была ли политическая реклама полностью или по существу сгенерирована искусственным интеллектом (Mich. Comp. Laws Ann. § 169.247, West). В дополнение к этим законам штатов более 40 штатов внесли на рассмотрение более 400 законопроектов, связанных с ИИ [1].

Администрация Дональда Трампа в мае 2025 г. утвердила первый в истории федеральный закон, направленный против пространства «дипфейков» – поддельных изображений и видео, созданных с помощью нейросетей. Документ, получивший название Закона о борьбе с известными случаями эксплуатации путем блокировки технологических дипфейков на веб-сайтах и в сетях, или Закона о блокировке («Take It Down Act») ¹, вводит уголовное наказание за публикацию материалов без согласия человека, включая контент, сгенерированный ИИ ².

В КНР активно разрабатываются нормативные акты в сфере ИИ. Как и в случае с американским и европейским подходами, некоторые китайские нормативные акты не направлены непосредственно на регулирование ИИ, но охватывают смежные области. Три из них имеют непосредственное отношение к генеративному ИИ и дипфейкам:

Положение об управлении алгоритмическими рекомендациями в информационных интернет-сервисах 2021 г. (互联网信息服务算法推荐管理规定) (Положение о китайских алгоритмических рекомендациях), которое в широком смысле распространяется на интернет-сервисы, использующие алгоритмические рекомендации, такие как социальные сети и электронная

¹ Подробнее об этом Законе см.: Take It Down Act. – URL: <https://www.govtrack.us/congress/bills/119/s146/text>; <https://lawforeverything.com/take-it-down-act/>; https://en.wikipedia.org/wiki/TAKE_IT_DOWN_Act?ysclid=mikd5mciqr752029893 (дата обращения: 15.11.2025).

² Дипфейки под запретом: в США начали криминализировать ИИ-подделки. – URL: <https://vgtimes.ru/news/126535-dipfeyki-pod-zapretom-v-ssha-nachali-kriminalizovat-ii-poddelki.html> (дата обращения: 18.10.2025).

коммерция. Оно предоставляет пользователям право отключать алгоритмические рекомендации, удалять теги персонализации и получать разъяснения о влиянии алгоритмов (ст. 17). Кроме того, был введен реестр алгоритмов, согласно которому поставщики должны предоставлять такую информацию, как: название поставщика, тип алгоритма, отчеты о самооценке и отображаемый контент (ст. 24). За нарушения предусмотрены штрафы в размере от 10 тыс. до 100 тыс. юаней (ст. 31);

Положение об управлении интернет-информационными сервисами глубокого синтеза 2021 г. (互联网信息服务深度合成管理规定) (Закон о дипфейках). Этот Закон требует, чтобы дипфейки были помечены соответствующим образом, чтобы их содержание не «вводило общественность в заблуждение» (ст. 17). Хотя в Законе о дипфейках в Китае прямо не указаны меры наказания за его нарушение, в нем говорится, что нарушители «будут наказаны в соответствии с действующими законами и административными постановлениями» (ст. 22);

Временные меры по управлению сервисами генеративного искусственного интеллекта 2023 г. (生成式人工智能服务管理暂行办法) (Китайский регламент о генеративном искусственном интеллекте). Этот Регламент распространяется на использование всех технологий генеративного ИИ, которые применяются для предоставления услуг населению, что, в частности, исключает разработку и применение технологий генеративного ИИ, которые не использовались для предоставления услуг населению (ст. 2). Китайский регламент о генеративном ИИ налагает весьма обременительные обязательства на поставщиков генеративного ИИ, требуя от поставщиков обеспечения того, чтобы права интеллектуальной собственности не нарушались, и чтобы поставщики «применяли эффективные меры для повышения качества обучающих данных и повышения достоверности, точности, объективности и разнообразия обучающих данных» (ст. 7). Если будет установлено, что поставщики генеративного ИИ нарушили китайское законодательство о генеративном ИИ, они могут быть привлечены к ответственности в соответствии с положениями законов КНР о кибербезопасности, о безопасности данных, о защите персональных данных, о научно-техническом прогрессе и других подобных законов и административных постановлений (ст. 21).

В Китае законодательство не предусматривает оптимального распределения ответственности между субъектами, участвующими в создании результатов работы генеративного ИИ. Например, хотя

китайский Закон о дипфейках требует, чтобы «поставщики услуг глубокого синтеза» наносили водяные знаки на результаты работы, это требование может быть возложено также на конечных потребителей базовых моделей (Закон о дипфейках, ст. 17, 23). Согласно китайскому определению, «поставщик услуг глубокого синтеза» – организация, которая дорабатывает (т.е. тонко настраивает) предварительно обученную базовую модель, способную генерировать материалы, нарушающие авторские права, – будет нести ответственность, даже если она не знала о таких материалах. Китайские суды уже возлагали ответственность на конечных потребителей генеративного ИИ в делах о нарушении авторских прав [1]. В связи с этим большое внимание в статье *Бао Кхам Чау и Дж. Хэ* уделяется вопросу ответственности владельцев креативных технологий ИИ, авторы рассматривают, какие стороны должны нести бремя ответственности таким образом, чтобы максимально стимулировать инновации и минимизировать ущерб. Они считают, что возлагать ответственность на арендаторов нецелесообразно, поскольку те не контролируют большие объемы данных для обучения базовой модели и алгоритмы генеративного ИИ. Всё в предварительно обученных базовых моделях контролируется арендодателями [ibid.].

Однако возлагать ответственность на владельцев креативных инструментов тоже проблематично, поскольку их модели могут быть использованы непредсказуемым образом. В самом простом случае владелец, который обучает базовую модель для злонамеренного использования, будет нести полную ответственность за такое использование ИИ. Однако сложность в том, что большинство базовых моделей не предназначены для конкретно злонамеренных действий или использования с высоким риском. Кроме того, если арендаторы (или субарендаторы) перепрофилируют (т.е. дорабатывают) базовые модели для другого законного применения, становится труднее определить, кто несет ответственность, если модели выдают вредоносные результаты.

Предлагаемая авторами система ответственности повышает прозрачность и ускоряет внедрение инноваций, если она (ответственность) по умолчанию возлагается непосредственно на арендодателей и тем самым стимулирует организации, обладающие наибольшим контролем, внедрять надежные меры безопасности и смягчения последствий. В отличие от общей системы ЕС, предусматривающей ответственность разработчиков систем ИИ без каких-либо исключений, китайская система предоставляет арендада-

телям четкие механизмы – такие, как журналы аудита и «красные команды» – для демонстрации ответственного поведения и надлежащего распределения ответственности в случае необходимости, расширяет существующие практики возмещения ущерба. Таким образом, китайский подход использует устоявшиеся правовые принципы для обеспечения более безопасной работы ИИ, не создавая при этом чрезмерных препятствий для инноваций [1].

Заключение

Анализ современных исследований показывает, что интеграция ИИ во все сферы общественной жизни должна быть сопряжена с жесткими и четкими правилами его разработки и использования, соблюдения фундаментальных прав человека и возложения ответственности в случае их нарушения. Труды некоторых участников Кембриджского форума «Искусственный интеллект: право и управление», отраженные в данном обзоре, подтверждают, что:

1) защита основных прав человека лежит в основе глобальных и академических проблем, связанных с технологиями ИИ. Достоинство, свобода, равенство, солидарность и справедливость являются краеугольным камнем человекоориентированного подхода к регулированию ИИ. Закон должен гарантировать индивидуальные меры защиты, предупреждать угрозы и риски, содержать меры предосторожности, направленные на обеспечение справедливого результата применения ИИ [3];

2) расширение возможности управления ИИ с помощью механизмов возмещения ущерба предполагает критически оценивать, в достаточной ли мере нынешнее управление ИИ удовлетворяет потребность в средствах правовой защиты от вреда, причиняемого ИИ, и возмещении ущерба. Обращение в суд, омбудсмену и другие способы правовой защиты позволяют людям, на которых повлияли системы ИИ, отстаивать свои права, особенно в тех случаях, когда нарушаются или подрываются принципы равенства, инклюзивности и справедливости [4];

3) негативные последствия дипфейков становятся все более очевидными по мере того, как расширяется применение генеративного ИИ. Его интеграция в различные приложения сопряжена со значительными рисками для национальной и личной безопасности; соответственно, создает новые проблемы для гражданского регулирования, например, закон об авторском праве. Учитывая реальные последствия, суды, политики и наука изучают, как суще-

ствующие режимы ответственности могут применяться к ИИ, чтобы стимулировать его безопасное развитие и использование. Однако, как показала практика, введенные меры ответственности не учитывают должным образом сложность обучения базовых генеративных моделей ИИ и их текущую экосистему. Поскольку компании-арендодатели владеют всей критически важной инфраструктурой и имеют технические возможности для контроля за ее использованием, предлагается обязать этих «арендодателей креативности» предоставлять технологии ИИ без дефектов и нести ответственность в случае неправильного использования генеративного ИИ [1].

Список литературы

1. Bao Kham Chau, George He. Audio deepfakes and the regulation of the landlords of creativity // Cambridge Forum on AI: Law and Governance. – 2025. – Vol. 1. – e30. – URL: <https://doi.org/10.1017/cfl.2025.10012> (дата обращения: 17.10.2025).
2. Cambridge Forum on AI: Law and Governance. – 2025. – Vol. 1. – URL: <https://www.cambridge.org/core/journals/cambridge-forum-on-ai-law-and-governance/article/individual-safeguards-in-the-era-of-ai-fair-algorithms-fair-regulation-fair-procedures> (дата обращения: 17.10.2025).
3. Grozdanovski L., Cooman J. de. Individual safeguards in the era of AI: Fair algorithms, fair regulation, fair procedures // Cambridge Forum on AI: Law and Governance. – 2025. – Vol. 1. – e18. – URL: <https://doi.org/10.1017/cfl.2025.10> (дата обращения: 17.10.2025).
4. Pi Y., Proctor M. Toward empowering AI governance with redress mechanisms // Cambridge Forum on AI: Law and Governance. – 2025. – Vol. 1. – e24. – URL: <https://doi.org/10.1017/cfl.2025.9>; <https://www.cambridge.org/core/journals/cambridge-forum-on-ai-law-and-governance/article/toward-empowering-ai-governance-with-redress-mechanisms/A1EBCD6CAA146F503C8F6842914F3FB3> (дата обращения: 17.10.2025).

МАДЖУМАЕВ М.М.¹ УГОЛОВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННОГО СУВЕРЕНИТЕТА В ТРАНСГРАНИЧНЫХ МЕТАВСЕЛЕННЫХ²

Аннотация. Статья посвящена проблеме действия уголовного закона в трансграничных метавселенных. Установлено, что традиционные принципы (территориальности, гражданства) и существующие разъяснения Верховного Суда РФ неэффективны в атерриториальной цифровой среде. Это создает юрисдикционный вакуум, угрожает цифровому суверенитету и ведет к доминированию *lex informatica* (частноправового регулирования платформ). В статье критически оцениваются существующие подходы и предлагаются новые решения. Среди них внедрение доктрины эффекта (по месту наступления существенных последствий), механизм «приземления» IT-операторов, юрисдикция дистрибуции (контроль над магазинами приложений) и концепция суверенизации цифровой личности (государственно-верифицированный аватар) для обеспечения уголовно-правовой защиты прав граждан.

Ключевые слова: метавселенная; действие уголовного закона в пространстве; коллизии юрисдикции; цифровой суверенитет; децентрализация; юрисдикция дистрибуции; суверенизация цифровой личности; аватар; цифровой двойник человека; деанонимизация.

MADZHUMAYEV M.M. Criminal legal maintenance of state sovereignty in cross-border metaverse

¹ © Маджумаев Мурад Мамедович, ведущий научный сотрудник, старший преподаватель кафедры уголовного права, уголовного процесса и криминалистики Юридического института Российского университета дружбы народов им. Патриса Лумумбы, кандидат юридических наук.

² Исследование выполнено за счет гранта Российского научного фонда № 25-28-01478, <https://rscf.ru/project/25-28-01478/>

Abstract. The paper addresses the challenge of the application of criminal law in cross-border metaverses. Conventional principles (territoriality, citizenship) and existing interpretations from the Supreme Court of the Russian Federation are found to be ineffective in the territorial digital environment. This creates a jurisdictional vacuum, threatens digital sovereignty, and leads to the dominance of *lex informatica* (private law regulation of platforms). The article critically assesses existing approaches and proposes new solutions. Among them is the introduction of the effect doctrine (based on the place where the essential consequences occur), a grounding mechanism for IT operators, distribution jurisdiction (control over app stores), and the concept of digital persona sovereignty (state-verified avatar) to ensure criminal law protection of citizens' rights.

Keywords: metaverse; spatial application of criminal law; conflicts of jurisdiction; digital sovereignty; decentralization; distribution jurisdiction; digital persona sovereignty; avatar; human digital twin; de-anonymization.

Для цитирования: Маджумаев М.М. Уголовно-правовое обеспечение безопасности государственного суверенитета в трансграничных метавселенных // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4: Государство и право. – 2026. – № 1. – С. 142–157. – DOI: 10.31249/iajpravo/2026.01.09

Введение

Коллизионный потенциал атерриториальных пространств и проблема цифрового суверенитета

Ускоренная цифровизация и внедрение сложных вычислительных систем в ткань общественных отношений требуют от правовой науки переоценки консервативных доктринальных подходов и перехода к проактивному формированию адаптивной нормативной среды. Неспособность существующих юридических институтов адекватно и своевременно реагировать на экспоненциальный рост технологических инноваций создает опасный вакуум регулирования, чреватый не только дестабилизацией социально-экономических процессов, но и эрозией фундаментальных основ правопорядка, включая государственный суверенитет. В таких вопросах право не может занимать позицию дисциплинарного изоляционизма. Аналогичным образом сама траектория развития научно-

технических инноваций требует соответствующего правового регулирования.

Стремительное развитие иммерсивных технологий и формирование глобальных, устойчивых и интерактивных виртуальных сред, объединенных концепцией «метавселенной»¹, знаменует собой не только технологическую, но и фундаментальную правовую революцию. Метавселенная, т.е. иммерсивное, синхронное и интероперабельное цифровое пространство² создает новую сферу для социально значимого взаимодействия. Эти трехмерные пространства параллельной реальности функционируют независимо от присутствия в них конкретных пользователей, которые представлены аватарами (цифровыми двойниками).

Во время как общественные отношения в объективной реальности физического мира (и некоторые цифровые взаимоотношения) регулируются принципами государственного суверенитета и территориальной юрисдикции, метавселенные функционируют как бесшовное, нетерриториальное (или надтерриториальное) пространство. Именно такая трансформация инициирует фундаментальный кризис существующих принципов действия уголовного (и не только) закона в пространстве, которые исторически и концептуально основаны на незыблемости физической географии и государственного суверенитета, проистекающего из контроля над ней.

Правопорядок, являясь главной функцией государства, сталкивается с беспрецедентной сложностью реализации в средах, которые по своей архитектуре атерриториальны, децентрализованы, зачастую анонимизированы и находятся под операционным управлением частных, преимущественно иностранных (транснациональных), корпораций. Классическая вестфальская модель, основанная на жесткой корреляции суверенитета и физической территории³, демонстрирует свою функциональную исчерпанность.

¹ Benaben F., Congès A., Fertier A. A Prospective Vision of the Evolution of Immersive Technologies: Towards a Definition of Metaverse // *Technovation*. – 2025. – Vol. 140. – P. 103–154. – URL: <https://doi.org/10.1016/j.technovation.2024.103154> (дата обращения 24.11.2025).

² Murala D.K., Panda S.K. Metaverse: A Study on Immersive Technologies // *Metaverse and Immersive Technologies: An Introduction to Industrial, Business and Social Applications*. – 2023. – P. 1–41. – URL: <https://doi.org/10.1002/9781394177165.ch1> (дата обращения 24.11.2025).

³ Hu H. Revisiting Territorial Sovereignty: Origins, Legitimacy, and Modern Implications // *San Diego International Law Journal*. – 2024. – Vol. 26. – P. 1. – URL: <https://digital.sandiego.edu/ilj/vol26/iss1/2/> (дата обращения 24.11.2025).

Возникающий де-юре юрисдикционный вакуум де-факто неминуемо заполняется квазиюрисдикцией операторов платформ, устанавливающих собственные правила компьютерным кодом в виде различных компьютерных программ или компьютерных протоколов, в совокупности называемых *lex informatica*.

Пределы применимости территориальной юрисдикции в атерриториальных пространствах метавселенных

Принцип территориальности (ст. 11 УК РФ), являющийся краеугольным камнем российского уголовного права, устанавливает юрисдикцию государства над преступлениями, совершенными на его территории. Однако в метавселенной само понятие *locus delicti* (места совершения преступления) становится неопределенным. Требуется разрешение коллизии относительно территориальной юрисдикции применительно к совершенному деянию в таких средах:

а) по месту нахождения пользователя-субъекта общественно опасного деяния. Для этого требуется его физическая локализация, что крайне затруднительно в условиях анонимности и использования программно-аппаратных средств туннелирования, шифрования и подмены IP-адреса¹ при доступе к информационным ресурсам, информационно-телекоммуникационным сетям (VPN);

б) по месту нахождения пользователя-жертвы. Аналогичная проблема идентификации и локализации;

в) по месту нахождения серверов, на которых размещена метавселенная (его платформы). Серверы могут быть распределены по разным государствам, использовать облачную инфраструктуру, а сама платформа может быть децентрализованной (например, на базе блокчейна), не имея единого центра управления;

г) в самом виртуальном пространстве. Оно не имеет географических координат и не является суверенной территорией какого-либо государства.

¹ A survey on edge computing (EC) security challenges: Classification, threats, and mitigation strategies / A.M. Sheikh, M.R. Islam, M.H. Habaebi, S.A. Zabidi, A.R. Bin Najeeb, A. Kabbani, // *Future Internet*. – 2025. – Vol. 17, N 4. – С. 175. – URL: <https://doi.org/10.3390/fi17040175>; Location privacy-preserving mechanisms in location-based services: A comprehensive survey // *ACM Computing Surveys (CSUR) / Hongo Jiang, Jie Li, Ping Zhao, Fansi Zeng, Zhu Xiao, Arun Iyengar*. – 2021. – Vol. 54, N 1. – С. 1–36. – URL: <https://doi.org/10.1145/3423165> (дата обращения 24.11.2025).

В результате правоприменитель сталкивается с *негативными коллизиями* юрисдикции (когда ни одно государство не может с уверенностью обосновать свою компетенцию, что может породить отвратимость наказания) и *позитивными коллизиями* (когда несколько государств одновременно претендуют на юрисдикцию, например первая страна – по месту нахождения жертвы, вторая страна по месту регистрации корпорации-владельца, третья страна по месту нахождения дата-центра).

Высшая судебная инстанция Российской Федерации предприняла попытку адаптации упомянутого принципа к цифровой среде. В п. 19 постановления Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”», разъясняется, что местом совершения такого преступления является «территория, на которой лицом использовалось компьютерное устройство» для выполнения действий, входящих в объективную сторону деяния. Данный подход, стремящийся найти материальный след в физическом мире, на первый взгляд представляется логичным, однако применительно к метавселенным он демонстрирует свою теоретическую и практическую несостоятельность.

Во-первых, эта позиция основана на опровержимой презумпции возможности установления реального местонахождения устройства. В условиях, когда использование средств анонимизации, делающих определение реального IP-адреса, а значит и «территории, на которой... использовалось... устройство», невозможным без содействия оператора платформы и провайдеров VPN (VPN, Tor, каскадные прокси-серверы), является не исключением, а правилом для любого технически «грамотного» злоумышленника; «территория... устройства» становится юридической фикцией, неустановимым обстоятельством. Правоприменитель, связанный таким разъяснением, как представляется, ставится в процессуальный тупик, поскольку юрисдикция государства становится зависимой не от воли законодателя, а по сути от уровня технической компетенции преступника. По формуле Пленума, юридически юрисдикция имеется (если удастся найти устройство), но фактически она недоказуема, так как для установления местонахождения устройства требуются международные следственные поручения,

которые будут исполняться годами или не исполняться вовсе, особенно с учетом турбулентности международных отношений.

Во-вторых, разъяснение Пленума игнорирует архитектуру современных цифровых (мета)преступлений. Деяние может совершаться не с одного устройства, а распределенно (DDoS), через ботнет, сеть зараженных устройств¹, находящихся в нескольких государствах, либо с использованием арендованных облачных мощностей², физическое расположение которых не совпадает ни с местом нахождения субъекта деяния, ни с местом нахождения жертвы. Более того, в децентрализованных метавселенных, функционирующих на базе технологий распределенного реестра (блокчейн)³, отсутствует единый сервер, а устройство пользователя является лишь одним из тысяч равноправных узлов сети. В такой парадигме попытка локализовать *locus delicti* через одно устройство теряет всякий смысл.

В-третьих, делая неправомерный акцент на месте действия (*locus actus*), Пленум умаляет значение места наступления последствий (*locus consequentiae*). Для материальных составов, таких как мошенничество (ст. 159 УК РФ), в результате которого у российского гражданина списаны денежные средства со счета в российском банке, именно территория наступления вредоносного результата представляет собой гораздо более устойчивый и юридически значимый юрисдикционный базис, нежели эфемерное и зачастую недоказуемое местоположение устройства злоумышленника.

¹ Computer Crimes // *American Criminal Law Review. Annual Survey of White Collar Crime* / S. Bhattar, S. Hilsabeck, F. Sullivan, B. Barry. – 2025. – Vol. 62, N 3. – P. 441. – URL: <https://www.law.georgetown.edu/american-criminal-law-review/aswcc/> (дата обращения 24.11.2025); Singh T. *Understanding Cybercrime and Criminology // Cybersecurity, Psychology and People Hacking. Palgrave Studies in Cyberpsychology*. Palgrave Macmillan. – Cham: Springer Nature Switzerland, 2025. – P. 1–15. – URL: https://doi.org/10.1007/978-3-031-85994-6_1 (дата обращения 24.11.2025).

² Patsakis C., Arroyo D., Casino F. *The Malware as a Service Ecosystem // Malware: Handbook of Prevention and Detection*. – Cham: Springer Nature Switzerland, 2024. – P. 371–394. – URL: https://doi.org/10.1007/978-3-031-66245-4_16 (дата обращения 24.11.2025).

³ Omar M. *Blockchain Technology: Enhancing Security in a Decentralized World // Defense in Depth: Modern Cybersecurity Strategies and Evolving Threats / The Institute of Electrical and Electronics Engineers, Inc.* – Wiley, 2025. – С. 99–125. – URL: <https://doi.org/10.1002/97811394340750.ch5> (дата обращения 24.11.2025).

Иллюзия альтернативных принципов и угроза *lex informatica*

В доктрине нередко высказывается мнение, что описанный кризис территориальности не является нерешимой проблемой, поскольку национальное законодательство (в частности статья 12 УК РФ) содержит альтернативные юрисдикционные основания, принцип активного (субъект преступления – гражданин РФ) и пассивного (жертва преступления – гражданин РФ) подданства¹. Сторонники данной позиции утверждают, что если потерпевшим (еще шире – жертвой) от общественно опасного деяния в цифровой среде (в нашем случае в метавселенной) является гражданин РФ, государство вправе применить принцип пассивного гражданства (ч. 3 ст. 12 УК РФ) и осуществить уголовное преследование, независимо от физического места преступления.

Однако подобная аргументация, будучи формально-юридически верной, смешивает два фундаментально различных аспекта: юрисдикцию устанавливать нормы (*jurisdiction to prescribe*) и юрисдикцию обеспечивать их принудительное исполнение (*jurisdiction to enforce*)². Безусловно, Российская Федерация вправе декларировать свою юрисдикцию на основании гражданства потерпевшего или субъекта преступления (в случаях, когда он находится не в пределах РФ). Но практическая реализация этого права, сбор доказательств, установление личности преступника, получение логов его действий наталкивается на необходимость получения содействия от оператора платформы, находящегося, как правило, в иностранной (иногда и недружественной) юрисдикции. Это инициирует громоздкий и в современных геополитических реалиях практически неработающий механизм международного сотрудничества (запросы о правовой помощи). Сроки исполнения таких запросов, исчисляемые месяцами и годами, не коррелируют со сроками жизни цифровых доказательств (часы или дни). Кроме того, применение ч. 3 ст. 12 УК РФ обусловлено требованием двойной криминализации (деяние должно быть наказуемо и в го-

¹ Payer A. The Territorial Principle as a Basis for State Criminal Jurisdiction: Particularly with Regard to Cross-Border Offences and Attempts, and to Multiple Parties to an Offence Acting in Different Countries // *International Criminal Law Review*. – 2023. – Т. 23, № 2. – С. 175–238. – URL: <https://doi.org/10.1163/15718123-bja10151> (дата обращения 24.11.2025).

² Sinha R., Talmon S. Germany's Position on an 'International Network Law' // *GPIL-German Practice in International Law*. – 2024. – P. 5. – URL: <https://d-nb.info/134687655X/34> (дата обращения 24.11.2025).

сударстве, где оно совершено). Учитывая неопределимость места совершения преступления и правовую неквалифицированность многих виртуальных посягательств (например, хищение аватара) в законодательстве страны хостинга, это условие часто становится невыполнимым.

При этом следует отметить положительным принятие по инициативе Российской Федерации Всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (далее – Конвенция; Конвенция ООН против киберпреступности¹), которая создает новую правовую реальность и предлагает инструменты для решения именно тех проблем, которые обозначены выше. Хотя Конвенция в главе III (ст. 22) во многом содержит существующие юрисдикционные подходы (территориальный, активный и пассивный персональный), ее подлинная ценность заключается не в создании новых юрисдикционных оснований, а в имплементации новых процессуальных механизмов принудительного исполнения, направленных на преодоление процедурного тупика и «разрыва в скорости» между дующими месяцами запросами и исчезающими за часы цифровыми доказательствами.

Ключевой проблемой при расследовании преступлений в метавселенных, как было изложено, является неспособность государства оперативно получить цифровые доказательства (логи, данные о пользователе) от иностранного оператора платформы. Конвенция ООН предлагает для этого конкретные решения. Во-первых, предполагается создание сетей 24/7 (ст. 41). Конвенция обязывает каждое государство-участника назначить «контактный центр, работающий 24 часа в сутки семь дней в неделю для обеспечения предоставления неотложной помощи» по преследованию определенных преступлений. Это создает прямой, высокоскоростной канал связи между правоохранительными органами, минуя медленные дипломатические процедуры, для решения срочных задач. Во-вторых, и самое важное, предполагается создание механизмов оперативного обеспечения сохранности данных (ст. 42). Данная статья позволяет государству-участнику (например Рос-

¹ Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям, принята резолюцией 79/243 Генеральной Ассамблеи от 24 декабря 2024 г.

сии) обратиться через сеть 24/7 к другому государству (где находится оператор метавселенной) с просьбой «оперативно обеспечить... сохранность электронных данных» (ст. 42.1). Самое главное, пунктом 4 ст. 42 Конвенции прямо устанавливается, что «обоюдное признание соответствующего деяния преступлением в качестве условия обеспечения такой сохранности не требуется».

Этим решается две из озвученных ранее проблем, снимаются вопросы быстрого реагирования и двойной криминализации. Запрос на сохранность (preservation) выполняется оперативно, что позволяет «заморозить» цифровые следы до их удаления. Барьер в виде отсутствия аналога преступления (например, «хищение аватара») в законодательстве запрашиваемой страны снимается на первом, самом важном этапе – этапе сохранения доказательств. Конвенция устанавливает, что сохранность данных обеспечивается на срок не менее 60 дней (ст. 42.8), что дает правоохранительным органам время на подготовку и направление уже формального запроса о взаимной правовой помощи (в соответствии со ст. 40 и 44) для получения доступа к этим данным. К моменту подачи формального запроса критически важные доказательства уже будут сохранены и не будут утеряны.

Тем не менее принятие Конвенции ООН против киберпреступности не устраняет полностью проблему своего рода «доминирования» *lex informatica*, но предоставляет государствам действенный многосторонний инструмент для укрепления *jurisdiction to enforce*. Она заменяет архаичные, неработающие механизмы запросов о правовой помощи на двухступенчатую систему:

1) немедленное сохранение данных без оглядки на двойную криминализацию через сеть 24/7;

2) последующее формальное истребование уже сохраненных данных.

Это значительно усиливает позиции национальных правоохранительных органов в борьбе с преступностью в трансграничных цифровых пространствах, включая метавселенные.

Вместе с тем встречается и иная точка зрения, исходящая из либертарианского подхода и поддерживаемая операторами платформ, которая заключается в том, что юрисдикционный вакуум формально не является проблемой, так как на деле он эффективно заполняется частноправовым регулированием транснациональных корпораций¹

¹ Lessig L. Code: and Other Laws of Cyberspace. – 2 nd Revised ed. – New York: Basic Books, 2006. – 432 p.

(операторами метавселенных), пресловутым *lex informatica*. В этой парадигме условия предоставления услуг, пользовательские соглашения как бы заменяют уголовный закон, производством (расследованием) по делу занимается служба модерации, а наказанием – администратор платформы, применяющий бан, удаление аккаунта или конфискацию виртуальных активов.

Сторонники либертарианского подхода и представители цифровой индустрии видят в этом не проблему, а решение. Они указывают на эффективность такого «корпоративного» правосудия, оно транснационально, технически компетентно и, главное, оперативно¹. Администратор платформы может заблокировать мошенника в течение минут, в то время как государственная система будет месяцами решать вопрос о подследственности.

Однако такая «приватизация» правосудия несет в себе экзистенциальную угрозу суверенитету. Во-первых, это прямое делегирование базовой функции государства (защиты граждан и монополии на принуждение) в руки частной, иногда иностранной, коммерческой структуры. Во-вторых, такое правосудие лишено каких-либо процессуальных гарантий, оно не знает презумпции невиновности, права на защиту, состязательности сторон и независимого суда. В-третьих, цели корпорации (прибыль, PR) и государства (правосудие) не совпадают. Корпорация может проигнорировать сложное мошенничество, но заблокирует пользователя за деяние, несущее репутационные риски, даже если оно не является преступным. Принятие *status quo*, как представляется, равносильно отказу государства от уголовно-правовой защиты своих граждан.

Цифровой суверенитет в данном контексте – это не столько контроль над цифровыми границами, сколько функциональная² способность государства обеспечивать верховенство своего права, защиту прав своих граждан и реализацию публичных интересов в цифровой среде. Обстоятельство, когда государство не может применить свой уголовный закон для защиты своего гражданина

¹ Schill S.W., Berger N. *Eroding the Rule of Law through Private-Public Arbitration?* // *The Comparative Constitutional Foundations of Private-Public Arbitration*. – Oxford, UK: Oxford University Press, 2025. – С. 92.

² Shokri A. *Sovereignty in Cyberspace from the Viewpoint of International Law* // *Asian Journal of International Law*. – 2025. – P. 1–31. – URL: <https://www.cambridge.org/core/journals/asian-journal-of-international-law/article/sovereignty-in-cyberspace-from-the-viewpoint-of-international-law/2193733BFBA268E7E211FA345942150> (дата обращения 24.11.2025).

от вымогательства в метавселенной, а единственным «защитником» выступает модератор платформы, зарегистрированной в другой стране, и будет эрозией суверенитета.

Концептуализация расширительного толкования юрисдикции

Необходимо разработать и легитимизировать новые доктринальные подходы к определению юрисдикции, адаптированные к цифровой реальности.

1. Расширительное толкование территориальности (принцип эффекта или наиболее существенно воздействия)

Следует отойти от жесткой привязки к физическому месту. Юрисдикция государства должна распространяться на любое преступление, существенные и предсказуемые вредоносные последствия которого наступают на его территории или направлены против ее граждан (независимо от их физического местонахождения в момент деяния). Этот подход (effects doctrine), давно применяемый в антимонопольном праве США¹, должен быть инкорпорирован в уголовное право. Если мошенничество в метавселенной привело к финансовому ущербу гражданина (списанию средств с его счета в банке) или причинению вреда его здоровью (например, доведение до самоубийства), место преступления должно признаваться находящимся в пределах такого государства. Это требует внесения уточнений в постановление Пленума ВС РФ о применении норм ст. 11–12 УК РФ.

2. Концепция квазитерритории и цифрового присутствия

В качестве доктринальной основы следует рассматривать цифровые аватары и аккаунты российских граждан как их цифровое представительство. Посягательство на аватар (например, неправомерный доступ, его хищение или использование для клеветы) должно приравниваться к посягательству на компьютерную информацию, личность или имущество гражданина, находящегося под юрисдикцией государства.

Интересным представляется введение института «приземления» для операторов метавселенных. Ключевым инструментом

¹ Martyniszyn M. Extraterritoriality in Competition Law: Progressing Narrowing of the Gaps // e-Competitions: National Competition Laws Bulletin. – 2024. – Special Issue on Extraterritoriality. Art. N 120291. – P. 2. – URL: https://pureadmin.qub.ac.uk/ws/portalfiles/portal/608361752/Extraterritoriality_in_Competition_Law_Progressing_Narrowing_of_the_Gaps.pdf (дата обращения 24.11.2025).

восстановления суверенитета является механизм, аналогичный Федеральному закону от 01.07.2021 № 236-ФЗ (в ред. от 01.09.2022) «О деятельности иностранных лиц в информационно-телекоммуникационной сети “Интернет” на территории Российской Федерации» («о приземлении» IT-гигантов). Необходимо законодательно обязать операторов метавселенных, чья аудитория в России превышает установленный порог:

а) открывать полноценные филиалы или представительства в РФ;

б) локализовать данные российских пользователей на территории РФ (это в определенной степени уже реализовано Федеральным законом от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»);

в) создать интерфейс для оперативного взаимодействия с правоохранительными органами (СК РФ, МВД России, ФСБ России и др.).

Наличие юридического лица в Российской Федерации делает корпорацию субъектом российского права и позволяет применять к ней меры процессуального принуждения (запросы о предоставлении данных, обыски в представительстве) и ответственности (оборотных штрафов) за отказ в содействии расследованию. Это переводит проблему из плоскости международного права в плоскость внутригосударственного принуждения.

3. Модернизация уголовно-процессуальных механизмов

Полагаем, что УПК РФ должен быть дополнен нормами, регулирующими следственные действия в виртуальной среде, например:

а) виртуальный осмотр (процессуальная фиксация обстановки в метавселенной, при осмотре аватара, виртуального объекта, запись логов чата);

б) деанонимизация как мера принуждения (четкая процедура получения судебного разрешения на истребование у оператора платформы (ее российского представительства) данных, позволяющих идентифицировать пользователя (IP-адрес, MAC-адрес, платежные данные));

в) обеспечение сохранности цифровых доказательств (механизм быстрого (по судебному решению) «замораживания» цифровых данных (логов, активов) на серверах оператора до их формального истребования).

4. Опосредованное принуждение доктриной юрисдикции дистрибуции

Этот подход предлагает наиболее прагматичный и асимметричный ответ на проблему юрисдикции обеспечивать их принудительное исполнение. Он основан на признании факта, что если государство не может дотянуться до серверов метавселенной в других странах, оно в полной мере контролирует каналы доступа к этому сервису на своей территории. Доступ к метавселенной осуществляется через клиентское программное обеспечение (приложение)¹, которое дистрибутируется через централизованные магазины приложений (App Store, Google Play, RuStore, Steam и т.д.). По своему содержанию такое решение, означает, что государство устанавливает юрисдикцию не над самой метавселенной, а над операторами дистрибуции программного обеспечения, легально действующими на российском рынке.

В законодательство (например, в Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 31.07.2025) «Об информации, информационных технологиях и о защите информации» вводится норма, обязывающая оператора магазина приложений (Apple, Google, VK) незамедлительно приостановить или удалить приложение (клиент метавселенной) по решению российского суда или уполномоченного органа (Роскомнадзор) в случае, если оператор данного приложения (метавселенной) систематически (например, дважды) отказывается исполнять законные требования российских правоохранительных органов (о предоставлении данных, деанонимизации, блокировке преступного контента)). Такое решение обладает высокой вероятностью эффективной реализации. Оно не требует экстерриториальных действий. Оно является классическим примером реализации суверенитета на своей территории в отношении субъектов (Apple, Google, VK), которые здесь физически и юридически присутствуют и получают прибыль. Для оператора метавселенной угроза удаления из App Store или Google Play на многомиллионном российском рынке является гораздо более весомым аргументом, чем символический штраф или трудноисполнимый запрос о правовой помощи. Это, по сути, опосредованное принуждение. Оператор метавселенной ставится перед выбором – сотрудничать с правоохранительными органами или

¹ Понкин И.В. Технологии киберметавселенных в государственном управлении: понятие и возможности применения // Право и государство: теория и практика. – 2024. – № 11 (239). – С. 291–294.

потерять доступ ко всем своим российским пользователям. Этот юрисдикционный рычаг смещает точку давления с неуязвимого разработчика на уязвимый канал его дистрибуции.

5. Концепция суверенизации цифровой личности

Данный подход является наиболее фундаментальным и предлагает изменить сам объект уголовно-правовой охраны. Проблема юрисдикции возникает потому, что аватар в метавселенной рассматривается как анонимный псевдоним. Предлагается ввести в правовое поле доктрину суверенной цифровой личности (далее – СЦЛ)¹.

Государство, по аналогии с выдачей физического паспорта, должно предложить гражданам (а для определенных видов деятельности обязать их) проходить процедуру создания государственно-верифицированной цифровой личности (например на базе усиленной Единой системы идентификации и аутентификации – ЕСИА), которая становится их единственным легальным представителем в метавселенных для совершения юридически значимых действий (экономических транзакций, заключения смарт-контрактов, владения цифровой собственностью).

С момента такой верификации эта суверенная цифровая личность становится юридическим продолжением гражданина РФ в цифровом пространстве. Она становится объектом, находящимся под прямой и безусловной уголовно-правовой защитой Российской Федерации, аналогично физической территории посольства. Любое посягательство на СЦЛ (ее неправомерный доступ, мошенничество с ее использованием, клевета в ее адрес) автоматически квалифицируется как преступление, совершенное против интересов, охраняемых законодательством России (по аналогии с принципом защиты, но в расширенном толковании).

В этом случае полностью снимается вопрос о месте преступления или местонахождении преступника. Сам факт посягательства на верифицированный государством цифровой объект (СЦЛ) является достаточным и неоспоримым юрисдикционным базисом для инициирования уголовного преследования в России. Этот под-

¹ См.: Акутин А.С., Бровка А.В. Реализация алгоритма доказательства с нулевым разглашением в технологии цифровой личности в управлении информационно-технологическими процессами предприятия // Вестник ВГУ. Сер. Системный анализ и информационные технологии. – 2024. – № 2. – С. 113–122; Литвинцева Е.А., Васекин А.С. Формирование цифрового суверенитета личности: коммуникативный аспект // Коммуникология. – 2024. – Т. 12, № 3. – С. 116–127.

ход не запрещает анонимность (можно сохранять анонимные аватары для общения), но он выводит из тени всю экономически и юридически значимую деятельность. Он не ищет юрисдикцию постфактум, а проактивно создает ее до-факта, распространяя суверенитет на новый, созданный государством цифровой объект.

Заключение

Трансграничные метавселенные ставят перед национальным уголовным правом экзистенциальный вызов, обнажая архаичность его территориальных основ. Попытки механической адаптации, подобные разъяснениям Пленума Верховного Суда РФ в постановлении от 15.12.2022 № 37, являются паллиативом, не решающим проблему по существу. Доктринальные апелляции к принципам персональности процессуально несостоятельны (в первую очередь процедурно неисполнимы), а передача правосудия на откуп корпорациям (*lex informatica*) равносильна капитуляции суверенитета. Единственным жизнеспособным ответом является системная реформа, сочетающая введение новой доктрины функциональной юрисдикции, основанной на правовой связи с Российской Федерацией, и создание строгого процедурного механизма цифровых представительств для принудительного исполнения национальных судебных решений.

Независимо от места совершения деяния, уголовная юрисдикция Российской Федерации должна распространяться на преступления, совершенные в электронных или информационно-телекоммуникационных сетях, включая метавселенные, если:

а) основным и непосредственным объектом посяательства являются права, свободы или законные интересы гражданина РФ либо его цифровой идентификатор, верифицированный в установленном порядке (например, через ЕСИА);

б) объектом посяательства является цифровой или виртуальный актив (включая цифровые права), принадлежащий резиденту РФ и (или) учтенный в российских системах реестров или декларированный в Российской Федерации;

в) деяние функционально направлено на причинение вреда охраняемым интересам РФ, включая критическую информационную инфраструктуру, финансовую систему или общественный порядок на территории РФ.

Это дает формально-правовое основание (юрисдикцию) для начала уголовного преследования в России, наложения ареста на

российские счета жертвы (для предотвращения дальнейших списаний), объявления преступника в международный розыск и, главное, направления запроса оператору платформы на основании собственной юрисдикции.

Любая метавселенная (или иная платформа), превышающая порог, например, в 1 млн (количество следует проработать) российских пользователей, обязана не просто открыть юрилицо, а аккредитовать в России (например, при Минцифры или Роскомнадзоре) свое цифровое представительство. Это представительство по доверенности от материнской компании уполномочено принимать и немедленно передавать на исполнение законные требования российских судов и (в установленных законом случаях) следственных органов. И, самое важное, представительство должно обладать техническими ключами доступа (API), достаточными для оперативного исполнения решений. Не отправлять запрос в страну нахождения головной организации, а исполнить здесь и сейчас.

Только такой симбиоз обновленной доктрины и эффективного принуждения позволит государству восстановить монополию на уголовное преследование и обеспечить реальную защиту граждан в новой цифровой реальности.

КРЫСАНОВА Н.В.¹ КИБЕРСТРАХОВАНИЕ В УСЛОВИЯХ РАСШИРЕНИЯ КИБЕРУГРОЗ (Обзор)

Аннотация. В последние несколько лет киберстрахование как альтернативная стратегия управления рисками демонстрирует быстрый рост по сравнению с другими видами страхования. В обзоре рассматриваются позиции ученых по политике киберстрахования и гарантии безопасности юридических и физических лиц от киберрисков и киберпреступлений. Модели киберстрахования – сравнительно новый институт в праве; его динамика позволяет выявить основные тенденции развития комплексных страховых услуг. В разных странах развитие киберстрахования идет разными темпами и в различных формах, что позволяет выявить общие тенденции и оптимальные модели его перспективного развития.

Ключевые слова: страхование; киберстрахование; киберриски; правовой институт; правовая политика.

KRYSANOVA N.V. Cyberinsurance in the context of expanding cyber threats (Review)

Abstract. In the last few years, cyber insurance as an alternative risk management strategy has shown rapid growth compared to other types of insurance. The review examines the positions of scientists on cyber insurance policy and guarantees for the security of legal entities and individuals from cyber risks and cybercrimes. Cyber insurance models are a relatively new institution in law; its dynamics make it possible to identify the main trends in the development of comprehensive insurance services. Cyber insurance is developing at different rates and in different forms in different countries, which makes it possible to identify common trends and optimal models for its future development.

¹Крысанова Нина Владимировна, старший научный сотрудник отдела правоведения ИНИОН РАН, кандидат юридических наук.

Keywords: insurance; cyberinsurance; cyberrisks; legal institute; legal politics.

Для цитирования: Крысанова Н.В. Киберстрахование в условиях расширения киберугроз (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2026. – № 1. – С. 158–171. – DOI: 10.31249/iajpravo/2026.01.10

Введение

Появление и развитие искусственного интеллекта (ИИ), больших данных, облачных вычислений, Интернет вещей и беспилотных автомобилей, цифровизация экономики и общества повышают благосостояние. Однако растущая зависимость от ИТ-сектора и интеграция цифровых технологий практически во все сферы жизни создают значительные киберриски, развиваются подходы по борьбе с киберпреступностью. Наука и практика реагируют на вызовы киберугроз и риски в киберпространстве и ищут пути решения этих проблем, в том числе через развитие институтов страхования. В обзоре представлены история появления института киберстрахования, практика киберстрахования в Российской Федерации и в зарубежных странах.

Появление института киберстрахования

Как указывает Джозефина Вольф (Josephine Wolff), доцент кафедры политики кибербезопасности в Школе Флетчера при Университете Тафтса (США), рост рынка киберстрахования в значительной степени определялся нормативными правовыми актами и регулирующими органами, но само киберстрахование в значительной степени остается нерегулируемым. В отличие от других форм страхования, здесь нет требований, определяющих, какие риски полисы киберстрахования должны охватывать, кто должен их получать или кому они должны быть доступны [7, р. 28–29].

С начала 2000-х годов в ряде штатов США были приняты законы об уведомлении о нарушениях данных, например в штате Калифорния – Билль № 1386 (2002) (California Senate Bill 1386)¹ (далее – S.B. 1386), и Общий регламент ЕС по защите данных

¹ California Senate Bill 1386. – URL: http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html (дата обращения: 23.11.2025).

(General Data Protection Regulation, GDPR) в Европе в 2016 г. (вступил в силу в мае 2018 г.); они способствовали росту спроса на киберстрахование и повлияли на то, какие виды потерь им покрываются, как это было, например, в случае решения Комиссии по ценным бумагам и биржам США (US Securities and Exchange Commission) о том, что компании должны раскрывать киберриски для акционеров в рамках их финансовых заявок.

Однако в США, в отличие от автострахования, киберстрахование не является обязательным. А по сравнению со страхованием от наводнений или терроризма оно не гарантируется правительством, или, в противоположность медицинскому страхованию, фактическое содержание полисов и расходы, которые они должны покрывать, не регулируются никаким законодательством ни на уровне штатов в США, ни на федеральном уровне. Такие подходы, по мнению Д. Вольф, понятны, учитывая небольшой размер и время существования рынка киберстрахования и тот факт, что исторически он охватывал довольно узкий набор относительно специфических угроз, таких, например, как утечка данных розничных продавцов и т.п. [7, р. 29].

Исторически сложилось так, что по мере роста популярности новых страховых продуктов или возникновения проблем, подобных тем, с которыми в настоящее время сталкиваются киберстраховщики, регулирующие органы часто вмешивались, чтобы стабилизировать рынок, защитить потребителей и предоставить необходимую помощь, данные или финансовую поддержку. Поскольку рынок киберстрахования продолжает расти, стоит проанализировать его развитие наряду с развитием других видов страховых продуктов, чтобы лучше понять роль, которую регулирующие органы могут играть на развивающихся страховых рынках, а также влияние, которое государственная политика оказывает на формирование различных форм киберстрахования [ibid.].

В 2025 г. в серии изданий Springer Nature «Международная серия Хюбнера о рисках, страховании и экономической безопасности» под редакцией Жоржа Дионна вышел в свет «Справочник по страхованию». Его авторы, А. Браун и Н. Хейсле, в частности подчеркивают, что в последнее время все больше персональных данных подвергается утечке, а вредоносные атаки и другие события приводят к значительным финансовым потерям [5, р. 251]. Новые технологии и, в частности, цифровые технологии, создали новые риски, которые представляют для страховщиков значительные проблемы. Исследования рисков и возможных стратегий управле-

ния рисками имеют решающее значение как для страховых компаний, так и для общества в целом.

Между тем, еще в 1990 г. Конгресс США выпустил доклад «Несбывшиеся обещания: банкротства страховых компаний», в котором, в частности, был сделан вывод о том, что деятельность страховщиков крайне слабо регулируется, и поэтому они могут регулярно вводить в заблуждение либо отказываться от своих обязательств перед клиентами. По мнению авторов доклада, система регулирования должна предвидеть и эффективно пресекать деятельность недобросовестных лиц, которые неизбежно будут вторгаться в такую привлекательную отрасль, как страхование, где клиенты передают крупные суммы наличных в обмен на обещание будущих выгод [7, р. 40]. Особенно подчеркивалось, что страховая отрасль имеет относительно низкие барьеры для «входа», поскольку новым страховым компаниям и продуктам не требуется вкладывать какой-либо значительный капитал: все, что нужно сделать, – это дать «обещания» потенциальным клиентам о будущей страховке. «Деньги поступают заранее, а выплата страховых возмещений может занять годы», – отмечается в докладе [ibid.].

Как подчеркивает Д. Вольф, ссылаясь на доклад Конгресса США, простота концепции страхования сочетается с чрезвычайной сложностью ее реализации. Правильное ценообразование, управление средствами, распределение рисков посредством перестрахования, создание адекватных резервов и рассмотрение претензий – все это требует должного уровня управления и даже определенного личного таланта; когда этого не хватает из-за недобросовестного отношения или некомпетентности, из страхового бизнеса, в отличие от других видов предпринимательства, можно очень легко уйти [ibid.]. В современных условиях это означает потребность в специальной правовой политике в сфере страхования вообще – и в сфере киберстрахования в особенности. Так, если на ранних этапах становления киберстрахования – с 1990-х годов – выпуск первых полисов страховыми компаниями сопровождался крайне тщательными проверками безопасности, и наличие полиса киберстрахования служило своего рода сигналом, что безопасность фирмы была тщательно проверена, а некоторые первые пользователи киберстрахования приобретали полисы только для того чтобы дать понять своим клиентам и деловым партнерам: они серьезно относятся к безопасности (например компания LockBox) [7, р. 44], в 2000-х годах многие компании – и большинство страховщиков – не имели доступа к специалистам в области

компьютерной безопасности, и страховые компании начали сотрудничать с технологическими фирмами, дабы снизить вероятность убытков своих клиентов, – тенденция, которая сохранялась и в последующие годы, поскольку все больше компаний приобретали киберстрахование, а все больше технологических компаний стали рассматривать страховщиков как потенциальный способ привлечения клиентов [7, р. 46].

Ситуация в сфере киберстрахования, например в США, стала меняться после того, как 5 апреля 2002 г. злоумышленники получили доступ к серверу дата-центра, в котором хранились личные дела, номера социального страхования и информация о заработной плате более 250 тыс. государственных служащих Калифорнии [7, р. 50]. В результате этого инцидента в 2002 г. и был разработан и принят вышеупомянутый Билль об уведомлении о нарушениях данных, который вступил в силу в 2003 г. и обязывал все компании, ведущие бизнес в Калифорнии, уведомлять клиентов о нарушениях в отношении их личной информации (персональных данных). На случаи взлома зашифрованной информации не распространялось требование об уведомлении, но в остальном закон – несмотря на то, что был принят только штатом Калифорния – применялся практически ко всем нарушениям во всех крупных компаниях США. Цель S.B. 1386 состояла в том, чтобы помочь частным лицам, таким как служащие штата Калифорния, чья информация была украдена с офисных компьютеров контролера, защитить себя от кражи личных данных и финансового мошенничества в случае кражи их данных. До принятия S.B. 1386 не существовало требования, согласно которому компании должны были уведомлять клиентов о нарушениях, и поэтому о многих инцидентах не сообщалось [7, р. 51].

Как указывает Дж. Вольф, принятие закона S.B. 1386 (а также других аналогичных ему нормативных правовых актов об уведомлении о нарушениях в сфере персональных данных) не только стимулировало продажи киберстрахования, но и изменило содержание полисов киберстрахования, сделав акцент на страховании от утечки данных [7, р. 54]. Это законодательство США привело к возникновению новых издержек для компаний, таких как расходы на уведомление жертв нарушений в соответствии с требованиями законов и т.п.

По мере распространения законов об уведомлении о нарушениях в различных странах, государства, часто с небольшими вариациями, которые усложняли обременительную задачу соблю-

дения разрозненного набора из десятков различных режимов уведомления, продолжали создавать новые финансовые риски для компаний и новые возможности для киберстрахования и т.д. [7, p. 54].

Вместе с тем, в то время как законы об уведомлении о нарушении данных упростили подачу исков в суд на компании за неспособность защитить личную информацию своих клиентов, режимы ответственности, регулирующие эти инциденты, долгое время оставались далеки от ясности.

Д. Вольф приводит такой пример: в 2011 г., когда у компании Sony произошел взлом данных в системе PlayStation, шло отклонение нескольких коллективных исков о нарушении конфиденциальности данных. Есть и другие примеры. Как пишет Дж. Вольф, практика показала, что тот факт, что частные лица стали получать уведомления о нарушениях, затрагивающих их личную информацию, отнюдь не означало, что компании, допустившие эти нарушения, будут привлечены к ответственности за такие инциденты. Не было четкого набора стандартов или требований безопасности, на которые могли бы указать заявители, чтобы требовать ответственности компании, – другими словами, никто не был уверен, что представляет собой халатность, когда дело касалось кибербезопасности [7, p. 67].

Кроме того, во многих случаях утечка данных и другие виды инцидентов, сопряженных с кибербезопасностью, связаны с множеством различных взаимозависимых организаций. Производители программного и аппаратного обеспечения, дизайн веб-сайтов, операторы связи и хостинги, платежные системы и интернет-провайдеры – все они могут играть определенную роль в совершении взломов, например оставляя уязвимости в коде или будучи не в состоянии обнаружить и заблокировать преступников, действующих в их (цифровой) инфраструктуре. То есть решение о том, кто должен нести ответственность за взломы и утечку данных, во многом зависело от конкретных деталей того или иного инцидента [ibid.].

Тем не менее киберстрахование достаточно долго продолжало развиваться в рамках Страхования коммерческой гражданской ответственности (Commercial General Liability (CGL) Insurance). С появлением киберпреступлений и юридическим признанием их особенностей, полагает Д. Вольф, развитие такой формы, как страхование ответственности от компьютерного мошенничества и киберугроз в качестве разновидности киберстрахования, стал практически неизбежен [7, p. 87].

В разных страховых полисах страховщики предлагали разные определения того, что считается компьютерным мошенничеством, а суды (в США), в свою очередь, придерживались совершенно разных мнений о том, насколько ясны эти формулировки, что они означают и насколько данное преступление должно было совершаться с помощью компьютера, чтобы оно считалось компьютерным мошенничеством. Так, в одном из подходов из формулировок страхового полиса следует, что компьютерное мошенничество – это убытки, непосредственно связанные с использованием любого компьютера для осуществления денежного перевода мошенническим путем, и т.п. [7, р. 90].

Обобщая этапы становления институтов киберстрахования, Дж. Вольф подчеркивает, что если «ранние» полисы киберстрахования были в основном сосредоточены на страховании от утечек персональных данных, а затем в эту сферу добавилось страхование от компьютерного мошенничества, то в настоящее время, по мере расширения спектра онлайн-угроз предприятия, организации и частные лица во всех секторах экономики и повседневной жизни начали сталкиваться с новым набором дорогостоящих и серьезных рисков, начиная от программ-вымогателей и заканчивая перебоями в работе облачных сервисов, экономическим шпионажем и проч. [7, р. 111–112].

Разные государства разрабатывают собственные подходы в развитии киберстрахования – институт киберстрахования бурно развивается.

Далее остановимся подробнее на отдельных примерах его развития.

Опыт Российской Федерации в сфере киберстрахования

Российская компания «Позитивные технологии» приводит такие цифры: мировой показатель среднего совокупного ущерба от утечки данных вырос с 4,45 млн в 2023 г. до 4,88 млн долл. в 2024 г. В России средний ущерб от утечки информации в 2024 г. составил 11,5 млн рублей. Согласно экспертным оценкам, максимальный совокупный ущерб (включая затраты на расследование инцидента) может достигать 140 млн рублей¹.

¹ См.: Утечки конфиденциальных данных из организаций: второе полугодие 2024 года / Positive Technologies. – URL: <https://www.ptsecurity.com/research/analytics/utechki-dannyh-aktualnye-ugrozy-vtorogo-polugodiya-2024-dlya-organizac-zij/#id3> (дата обращения: 18.11.2025).

В России киберстрахование рассматривается как вид страхования, который защищает от финансовых потерь, связанных с кибератаками, кражей личных данных и другими рисками в цифровой среде [3, с. 38].

Киберугрозы признаются крайне актуальными для российских предприятий, а кибератаки рассматриваются как действенный способ нанести финансовый ущерб. В нашей стране, как отмечают Н.Н. Чибинев и Н.В. Ляшенко, исследователи из Южно-Российского государственного политехнического университета (НПИ) им. М.И. Платова (Новочеркасск), кибератаки происходят во всех сферах деятельности человека и направлены в основном на подрыв безопасности объектов экономики и информационных систем государственных учреждений. Здесь они ссылаются на цифры, которые привел вице-премьер РФ Д.Н. Чернышенко 6 февраля 2024 г., выступая на форуме «Цифровая экономика» в рамках выставки «Россия». Он сообщил, что в 2023 г. российские IT-специалисты отразили более 65 тыс. кибератак на критическую информационную инфраструктуру. При этом следует отметить, что в 2021 г. целью атак был финансовый сектор, а в 2022 г. – государственный сектор [6]. В последние два года ИБ-центр ФСБ регистрирует более 170 кибератак каждый день [4].

Кибератаки в настоящее время становятся самыми распространенными причинами возникновения различных видов преступлений, нередко приводящих к чрезвычайным ситуациям. Характерными примерами возможности возникновения техногенных и социальных чрезвычайных ситуаций от кибератак могут служить события в ряде регионов нашей страны. Это подчеркивает опасность киберугроз как потенциальных чрезвычайных ситуаций. Для борьбы с ними авторы предлагают разработать нормативно-правовые акты и использовать современные технологические решения. На государственном уровне в России они предлагают ввести понятие «киберчрезвычайная ситуация», «кибератака» и «кибербезопасность», хотя они установлены в ГОСТ Р 56205–2014 и ГОСТ Р 56498–2015, а в Уголовном кодексе РФ предусмотрены ст. 272–274 за преступления в сфере компьютерной информации [4].

Инициаторами киберпреступления могут выступать как отдельные лица и организованные группировки, так и правительственные структуры недружественных стран. Основные киберинциденты, с которыми сталкиваются представители бизнеса, – это шифрование данных на рабочих станциях, компрометация банковских счетов, кража или модификация данных о клиентах. Также

крайне актуальным является скрытый киберриск, который возникает при неопределенности в полисе киберстрахования, неразвитости рынка киберстрахования с точки зрения предложения или сложности проверки степени ущерба, вызванного киберсобытием [2, с. 13].

Директор по рискам «СберСтрахования», председатель рабочей группы Всероссийского союза страховщиков (ВСС) Владимир Новиков в рамках Уральского форума «Кибербезопасность в финансах» отметил, что в 2023 г. страховщики в сфере киберстрахования получили около 900 млн руб. По его оценке, это составляет меньше 1% от всех страховых премий. Тем не менее, как показывают статистические данные, объем российского рынка киберстрахования быстро растет, приближаясь к 1 млрд рублей в 2025 г. Рост обусловлен увеличением числа кибератак и утечек данных. Несмотря на это, доля компаний с киберстраховкой остается низкой (6% в 2022 г.). Это обусловлено низкой осведомленностью и непониманием киберстрахования со стороны бизнеса, а также сложностей с обеспечением стандартизированного покрытия со стороны страховщиков¹.

В 2023 г. в России был запущен в работу Центр исследования киберугроз Солар (Solar), который аккумулирует базу знаний о кибератаках. Новым инструментом борьбы с потерями от кибератак является страхование посредством иншуртех (InsurTech) [3, с. 33] и децентрализованного финансирования, что позволяет предприятиям и организациям улучшить управление рисками. Российскими учеными предлагается выделение InsurTech в самостоятельное направление страхования и создание для него собственных регулятивных инструментов [3, с. 39].

По мнению Н.Н. Чибинева и Н.В. Ляшенко, для достижения целей защиты от киберугроз необходимо:

1) внести в единые нормативно-законодательные акты по безопасности в системе МЧС России понятие о киберчрезвычайной ситуации и порядок ее установления и классификации. Под *киберчрезвычайной ситуацией* они предлагают понимать обстановку на конкретных объектах жизнедеятельности или определенной территории, сложившуюся в результате разрушения их компьютерно-телекоммуникационной инфосферы и повлекшую за

¹ За 2023 год премии по киберстрахованию в России составили около 900 млн рублей // Коммерсантъ. – URL: <https://www.kommersant.ru/doc/6510671> (дата обращения: 06.09.2025).

собой ущерб здоровью людей или окружающей среде, приостановку производственной деятельности, значительные материальные потери и нарушение условий жизнедеятельности людей;

2) выполнить Указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации», запрещающего использование иностранного программного обеспечения на объектах критической инфраструктуры, принадлежащей госорганам;

3) использовать наиболее эффективный в настоящее время способ обеспечения информационной безопасности – модель Zero Trust, включающую в себя многие слои аутентификации, мониторинг сетевого трафика, криптографию и анализ поведения пользователей. Для реализации концепции Zero Trust используется шлюз кибербезопасности NGFW (NextGeneration Firewall) и применяются классические продукты класса IDM (Identity and Access Management), PAM (Privileged Access Management), EDR (Endpoint Detection and Response) и DLP (Data Loss Prevention);

4) развивать рынок киберстрахования в России как один из видов комплексной защиты от всевозможных киберугроз и др. [4].

Виды киберстрахования в практике зарубежных стран

«*Страхование по требованию*» – инновационная концепция, представленная сектором InsurTech. Этот вид страхования быстро набирает популярность, и некоторые эксперты прогнозируют, что этот развивающийся рынок может вырасти до 190 млрд долл. к 2026 г. Швейцарский исследователь А. Браун определяет страхование по требованию как покрытие эпизодических рисков, предлагающее потребителям индивидуальную защиту в определенные периоды, когда они или их имущество подвергаются риску [4, р. 226].

Страхование по требованию имеет две формы: краткосрочное страхование и страхование на основе универсального базового дохода (Universal Basic Income) (далее – UBI).

Краткосрочное страхование предназначено для защиты от рисков, которые ограничены во времени или повторяются и имеют известный или, по крайней мере, надежно предсказуемый характер воздействия. Распространенными примерами краткосрочных страховых продуктов являются страхование путешествий на одну по-

ездку, временное страхование от несчастных случаев, краткосрочное автострахование и др.

Страхование UBI подходит для ситуаций, когда подверженность потребителей риску меняется во времени. В рамках страхования UBI страховое покрытие активируется полностью автоматически, в зависимости от таких факторов, как местоположение, активность или контекст. По мнению А Брауна, полисы по требованию лучше соответствуют потребностям страховщиков, чем традиционные договоры. Таким образом, действующим страховщикам также следует внедрять инновации в этом направлении [5, p. 228].

Встроенное страхование представляет собой смену парадигмы в предложении и потреблении страховых услуг. Идея заключается в том, чтобы органично интегрировать страховое покрытие в стоимость при продаже нестраховых продуктов и услуг. С ростом популярности цифровых платформ встроенное страхование стало инновационным решением. Оно существенно упрощает процесс покупки страховки для клиентов, создавая единый центр обслуживания для всех их страховых и нестраховых потребностей, устраняя необходимость в многочисленных транзакциях. Хотя в 2020 г. доля встроенного страхования в общем объеме продаж страховых услуг в мире составила всего 6%, его потенциал считается огромным [5, p. 228].

Разновидностями встроенного страхования являются связанное встроенное страхование и пакетное встроенное страхование.

Связанное встроенное страхование подразумевает практику предложения страхования в качестве дополнения к основному продукту или услуге. В этой модели клиенты могут выбрать страховое покрытие, адаптированное к их конкретным потребностям наряду с покупкой основного предложения. Известным примером является покупка онлайн-страховки путешествий на сайтах авиакомпаний или туристических компаний.

Пакетное встроенное страхование подразумевает, что страхование является неотъемлемой частью продукта или услуги. В этом случае клиенты автоматически получают страховое покрытие как часть общего пакета, без необходимости отдельной покупки [5, p. 229].

Рынок киберстрахования в основном представлен коммерческим страхованием, в то время как решения по киберстрахованию на розничном рынке все еще находятся на начальном этапе развития. Так, стандартные полисы страхования имущества и ответст-

венности для коммерческого сектора доступны на большинстве страховых рынков по всему миру. Однако большинство полисов страхования имущества и ответственности покрывают только ущерб физическим активам, таким как производственные мощности, и не включают киберриски. Нередко в договорах страхования не содержится четкого указания о том, будут ли киберсобытия (киберриски) включены или исключены [1, с. 336].

Одной из причин неразвитости киберстрахования, по мнению швейцарского исследователя М. Элинга, может быть то, что как страховщикам, так и страхователям до сих пор неясно, каковы механизмы киберрисковых событий и какую ценность создают полисы киберстрахования [6, р. 215].

Нередки ситуации, когда страхователи полагают, что киберициденты покрываются страховкой, в то время как страховщик предполагает обратное. Это ведет к юридическим спорам, судебной неопределенности, а судебные издержки увеличивают финансовый риск страховщиков. Судебные споры нередко возникают из того, что во многих случаях оказывается невозможным проверить, в какой степени ущерб связан с киберсобытием и кто должен нести ответственность в данных обстоятельствах.

Вследствие обозначенных проблем страховщики стремятся к более четкому изложению условий договоров двумя способами. В первых, страховые компании составляют договоры страхования, явно исключая киберриски из традиционных полисов, и предлагают специальные «отдельные киберполисы». Во вторых, страховые компании могут прямо включать условия киберстрахования в общий страховой полис и соответствующим образом корректировать премии, что приводит к появлению так называемых «позитивных киберполисов» или «пакетных полисов» [6, р. 217].

За последние десять лет, например, в США в сфере страхования сформировался специализированный рынок, предлагающий покрытие киберрисков. Однако, по мнению М. Элинга, за пределами США киберстрахование применяется мало. Так, в Европе многие корпорации даже не знают о существовании этого вида страхования, и лишь единицы им пользуются [6, р. 210].

По состоянию на 2020 г. мировой рынок киберстрахования оценивается в 5 млрд долл. премий. Компании с покрытием в диапазоне от 100 до 199 млн долл. составляют лишь 25% мирового рынка (1,44 млрд долл. премий от примерно 500 компаний), компании с страховым покрытием более 200 млн долл. составляют

20% мирового рынка (1,1 млрд долл. премий от 250 компаний) [6, р. 210]

Рынок США гораздо более развит, чем европейский, отчасти потому, что в США достаточно давно действуют требования к отчетности о кибератаках с относительно высокими штрафами за нарушения. Новые правила отчетности значительно повысили осведомленность о киберрисках и увеличили спрос, особенно на страхование ответственности (третьих лиц) от киберугроз. Таким образом, на рынке США в основном доминирует страхование от третьих лиц, в то время как те немногие полисы, которые уже существуют в Европе, ориентированы на страхование от первой стороны. В 2018 г. в Европейском союзе также были введены обязательства по предоставлению отчетности об утечках данных, что стало важным фактором развития европейского рынка киберстрахования [6, р. 212].

Информации об азиатском рынке страхования у западных исследователей мало, но, по их оценкам, по сравнению с Европой и США многие азиатские страны по-прежнему отстают в политике и стратегиях киберстрахования. С учетом того, что на Азию приходится 25% мировых кибератак, а в Азиатско-Тихоокеанском регионе расположено 40% мировых центров обработки данных, следует ожидать, что со временем азиатские страны обгонят США и Европу в киберстраховании [6, р. 212].

Перестрахование. По оценкам швейцарских исследователей, в настоящее время около половины своих киберпремий страховые компании передают перестраховщикам. Согласно статистическим данным, только четыре компании перестраховщика принимают более 60% премий; более 75% перестраховщиков имеют премии менее 100 млн долл. [ibid.].

Средняя стоимость полиса киберстрахования в США составляет 1485 долл. в год. Страховые премии варьируются от 650 до 2357 долл. для полиса с ответственностью в один млн долл. Прогнозы динамики рынка киберстрахования исследователи дают неоднозначные [6, р. 212].

Заключение

Киберстрахование – перспективный институт страхования, который, однако, по мнению ученых, пока не получил широкого распространения и отчасти не оправдал ожиданий многих экспертов, а также практиков в сфере страхования. Одним из объяснений

этого может быть ошибочное восприятие киберрисков. Повышение осведомленности субъектов правоотношений в вопросах киберстрахования может способствовать повышению спроса на страхование от киберрисков. Невысокая распространенность киберстрахования связана с отсутствием экспертизы для предварительной оценки защищенности страхователей [6, p. 225]

В российской действительности, для того чтобы занять прочную нишу на рынке информационной безопасности, киберстрахованию потребуется время, в течение которого появятся новые и более доступные предложения, включая комплексные услуги в сфере страхования. На фоне роста киберугроз и более осознанного подхода к вопросам обеспечения информационной и кибербезопасности можно ожидать увеличение спроса на услуги киберстрахования. Отметим, что киберстрахование представляет собой комбинированный продукт, включающий в себя не только страхование рисков, но и сервисную составляющую, которая может включать в себя дополнительные услуги с привлечением партнеров. Опыт других стран может быть полезен России при регулировании проблем страхования киберрисков.

Список литературы

1. Жмурова С.С., Джафаров Д.И. Правовое регулирование страхования киберрисков в России: опыт зарубежных стран и перспективы развития // Право и государство: теория и практика. – 2025. – № 4. – С. 334–337.
2. Клишина Ю.Е., Углицких О.Н., Серафимова В.А. Страхование юридических лиц от киберрисков: проблемы и перспективы развития // Финансы и учетная политика. – 2023. – Вып. 2. – С. 11–14
3. Коданева С.И. InsurTech в России и за рубежом: проблемы и перспективы // Право и цифровая экономика. – 2023. – № 4 (22). – С. 33–41.
4. Чибинев Н.Н., Лященко Н.В. Кибератака как новый вид чрезвычайных ситуаций // Инженерный вестник Дона. – 2024. – № 7. – URL: file:///C:/Users/Администратор/Downloads/kiberataka-kak-novyuy-vid-chrezvychaynyh-situatsiy%20(2).pdf (дата обращения: 11.11.2025).
5. Braun A., Haeusle N. Digital Insurance and InsurTech // Handbook of Insurance / ed. by Georges Dionne. – 3 ed. – Cham: Springer Nature: 2025. – Vol. 1. – P. 225–251. – URL: https://link.springer.com/chapter/10.1007/978-3-031-69561-2_8 (дата обращения: 11.11.2025).
6. Eling M. Cyber Risk and Cyber Insurance // Handbook of Insurance / ed. by Georges Dionne. – 3 ed. – Cham: Springer Nature, 2025. – Vol. 1. – P. 199–225. – URL: https://link.springer.com/chapter/10.1007/978-3-031-69561-2_7 (дата обращения: 11.11.2025).
7. Wolff J. Cyberinsurance policy: Rethinking risk in an age of ransomware, computer fraud, data breaches, and cyberattacks. – Cambridge: MIT Press, 2022. – 291 p.

ЗАХАРОВ Т.В.¹ К ВОПРОСУ О СИСТЕМЕ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ УСТАВА ООН (Обзор)

Аннотация. В обзоре представлены взгляды российских теоретиков международного права на современное состояние системы международной безопасности и направления ее развития. Рассматривается право ООН как основа международной безопасности, в частности, в ее юридическом аспекте, а также добросовестность государств как базовое условие ее эффективности.

В обзоре представлен особый взгляд зарубежных ученых на роль государства в системе международной безопасности, на использование международных органов по разрешению споров.

Ключевые слова: международное право; поддержание международного мира и безопасности; система международной безопасности; национальная безопасность; изменение климата.

ZAKHAROV T.V. On the issue of the international security system based on the UN Charter (Review)

Abstract. The review presents the positions of Russian international law theorists on the current state of the international security system and the directions of its development. The UN law is considered as the basis of international security, in particular, in its legal aspect, as well as the good faith of states as a basic condition for its effectiveness.

The review presents a special view of foreign scientists on the role of the state in the international security system, on the use of international dispute resolution bodies.

Keywords: international law; maintenance of international peace and security; international security system; national security; climate change

¹ Захаров Тимофей Владимирович, научный сотрудник отдела правопедия ИНИОН РАН.

Для цитирования: Захаров Т.В. К вопросу о системе международной безопасности на основе Устава ООН (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2026. – № 1. – С. 172–181. – DOI:10.31249/iajpravo/2026.11.

Введение

Современные проблемы международной безопасности остро сопряжены и взаимосвязаны с проблемами мира и обеспеченности правомерных действий государств – участников международной системы – нормами международного права¹.

Журнал «Вестник экономической безопасности» издательства Московского университета МВД России им. В.Я. Кикотя опубликовал две статьи: в 2024 г. (статья Р.А. Каламкаряна и Е.В. Мигачевой) и 2025 г. (статья С.А. Лобанова и Я.Д. Сурхаевой), объединенные сложной темой обеспечения международного мира и безопасности.

Авторы данных статей последовательно рассматривают построение (теоретической) модели системы международной безопасности на основе современного международного права и направления ее развития. Терминология, используемая авторами, отражает сложный подход к определению угроз международному миру и безопасности. Внесение изменений в эту терминологию влечет неминуемое изменение в толковании теоретической конструкции, так как предполагаемое условие международно-правового дискурса требует восприятия применяемых авторами терминологических конструкций в авторском варианте.

Роль международного права в формировании современного миропорядка

Р.А. Каламкарян, доктор юридических наук, профессор Московского университета МВД России имени В.Я. Кикотя, и Е.В. Мигачева, доцент кафедры международного права Московского государственного лингвистического университета, рассматривают в своей статье целостность системы права ООН как основы обеспечения международного мира и безопасности. Они отмечают

¹ См.: п. 6 Стратегии национальной безопасности Российской Федерации, утв. Указом Президента Российской Федерации от 02.06.2021 № 400.

связь состояний международной системы и системы международного права. «Международно-правовое строительство современного миропорядка в режиме верховенства права по обстоятельствам объективной констатации сопряжено, считают авторы, с поддержанием целостности системы международного права» [1, с. 89]

Р.А. Каламкарян и Е.В. Мигачева обращают внимание на *позитив права в миропорядке*, выражающийся в его потенциале в решении целой последовательности стоящих перед мировым обществом задач. «Показательный позитив права по факту международно-правового строительства современного миропорядка обозначен глобальным партнерством в целях развития; борьбой с транснациональной преступностью; системой применения силы на основании Устава ООН; укреплением Международного суда с целью обеспечения правосудия и верховенства права в международных делах; уважением прав человека и основных свобод для всех без каких-либо различий по признаку расы, цвета кожи, пола, языка, религии, политических или иных воззрений, национального или социального происхождения, имущественного положения, рождения или другого статуса; поддержанием международного мира и безопасности в рамках ООН; соблюдением принципа верховенства права как в международных, так и во внутренних делах; обеспечением воплощения государствами – членами ООН решений Международного суда по любым делам, сторонами которых они являются; повышением эффективности ООН в деле поддержания международного мира и безопасности; укреплением сотрудничества между ООН и региональными организациями в соответствии с предписаниями главы VIII Устава ООН; содействием мирному разрешению споров; проведением последовательной борьбы с терроризмом; осуществлением скоординированного, последовательного, комплексного подхода к постконфликтному миростроительству и примирению в целях достижения устойчивого мира» [1, с. 89–90].

Система права ООН как основа международного мира и безопасности

Основой миропорядка выступает система права ООН. В том случае, если государства признают международные обязательства в соответствии с Уставом ООН, нормы устава становятся нормами прямого действия в отношении членов ООН. Это относится и к целям, закрепленным в Уставе ООН, отмечают Р.А. Каламкарян и

Е.В. Мигачева. Таким образом обеспечивается целостность системы и потенциал в ее адаптации в решении ставящихся задач.

Устав ООН закладывает в том числе систему международной безопасности – также в «режиме востребованности» ее прямого (юридического) действия. Система представляется не только в категориях «международный мир», «безопасность», «дружественные отношения», но и в принципах ее организации – «суверенное равенство государств», «равноправие и самоопределение народов», «добросовестное выполнение международных обязательств», «невмешательство во внутренние дела», в свою очередь также являющихся юридическими категориями системы прямого действия. *Позитив* Устава ООН в том, что он закладывает «юридические параметры» применения силы в международной системе, считают Р.А. Каламкарян и Е.В. Мигачева. Они также выделяют такие документы, как Декларация тысячелетия ООН 2000 г. и Итоговый документ Всемирного саммита 2005 г. [1, с. 90–91].

Доктор юридических наук, заведующий кафедрой правового регулирования ТЭК МГИМО (университет) МИД России С.А. Лобанов и соискатель той же кафедры Я.Д. Сурхаева считают, что система права ООН «предметно позиционирована на поддержание международного мира и безопасности» [2, с. 96–97]. Они рассматривают систему международной безопасности на основе Устава ООН и цели внешней политики Российской Федерации.

Система ООН представлена авторами в (юридических) категориях «мир и безопасность», «развитие и права человека», также имеющих прямое (юридическое) действие. Реализация в системе международной безопасности права, основанного на таких категориях «согласно целям и принципам Устава ООН», обеспечивает решение всего комплекса задач, стоящих перед международным сообществом [там же]. Р.А. Каламкарян и Е.В. Мигачева также полагают, что «в конечном, результативном, итоге весь потенциал международно-правового строительства современного миропорядка показательно направлен на всестороннее соблюдение всего корпуса предписаний прямого юридического действия согласно Уставу Организации Объединенных Наций» [1, с. 91–92].

Роль государства в системе международной безопасности

Особую теоретическую модель развития системы международной безопасности представляет бывший директор отдела управления и инклюзивных институтов и бывший заместитель Ге-

нерального юрисконсульта Всемирного банка Х. Сиссе, в статье, опубликованной Гарвардском журнале международного права (Harvard International Law Journal) в 2025 г. Современный контекст глобального управления автор видит в растущей взаимозависимости и общей уязвимости [4, р. 407]. Право вето постоянных членов Совета Безопасности ООН неоднократно использовалось для приостановления действий по важнейшим вопросам, имеющим глобальные последствия [4, р. 408]. Сбоем в этой системе является фрагментарность глобального управления здравоохранением, которая стала очевидной во время пандемии COVID-19. Выход США из Всемирной организации здравоохранения поставит вопрос о том, будет ли система глобального управления здравоохранением опираться на страны-спонсоры [4, р. 412].

Почти невероятные разрушения, вызванные двумя тотальными войнами, создали глобальные системы, которые помогают определять нынешний мировой порядок. Однако ждать, пока еще одно крупное глобальное потрясение приведет к необходимым радикальным изменениям, нецелесообразно. Время ограничено, и не только потому что надвигающиеся климатические катастрофы могут быть настолько масштабными, что принимать ответные меры станет слишком поздно. Кризисы, связанные с конфликтами, ухудшением состояния окружающей среды и пандемиями, уже наступили. Зачем ждать новых войн, которые еще больше изменят геополитический ландшафт, или очередного крупного глобального кризиса в области здравоохранения, которые кажутся неизбежными, учитывая неослабевающее давление человечества на другие формы жизни и природные ресурсы? – задается вопросом Х. Сиссе [4, р. 422].

Наиболее фундаментальным стимулом для системной трансформации нынешнего мирового порядка Х. Сиссе называет эволюцию американского участия в этом порядке. Данную эволюцию он рассматривает как последовательный отход США от лидерства в международной системе и, в дальнейшем, выход из этой системы и противопоставление ей собственной национальной политики [4, р. 423].

Переосмысленная система глобального управления должна быть легко адаптируемой и самообучающейся системой, основанной на общих ценностях, принципах и нормах, которые отражают как чаяния, так и реалии большинства людей во всем мире. Общими ценностями и принципами должны быть следующие: равноправие и справедливая представленность; устойчивость и управле-

ние; инклюзивность и солидарность; справедливость и подотчетность; инновационность и адаптивность. Такие принципы, которые в значительной степени отражены в Целях устойчивого развития ООН, теперь также должны быть закреплены в новой архитектуре глобального управления, причем не как пустые слова, а как структурная реальность. Инновации и адаптивность означают, что в быстро развивающемся мире системы глобального управления должны быть способны быстро приспосабливаться к новым реалиям, что включает в себя внесение гибкости в уставы международных организаций [4, p. 424–425].

Желательные компоненты для новой архитектуры глобального управления, по мнению Х. Сиссе, следующие: 1) мир должен перейти к системе наднационального управления, разделенной по темам и / или регионам; 2) переосмысленная система глобального управления также должна развивать системы принятия решений, основанные на многополярности и распределении полномочий; 3) внести существенные изменения в уставы существующих международных организаций, таких как Организация Объединенных Наций, МВФ, Всемирный банк и ВТО (или создать новые организации вместо них), чтобы лучше отражать сегодняшние политические и экономические устремления и реалии, а также обеспечить у этих институтов мандат, средства и полномочия для решения проблем XXI в.; 4) встроенные механизмы участия негосударственных субъектов, включая организации гражданского общества (которые могут быть организованы на глобальном и региональном уровнях), частный сектор и группы коренного населения. Архитектура глобального управления также должна иметь механизмы принуждения, которые не зависели бы исключительно от интересов нескольких влиятельных субъектов в ущерб интересам многих; 5) парадигма экономического развития, основанная на европейском и североамериканском экономическом мышлении и модели роста, должна быть заменена моделями, отражающими ценности, потребности и опыт других стран и континентов [4, p. 426–427].

Юридический аспект в системе международной безопасности

Одним из проявлений системы международной безопасности называется «юридическая безопасность», которая рассматривается как совокупность прав и законных интересов государств. С.А. Лобанов и Я.Д. Сурхаева отмечают *позитив* в правомерном «юридически значимом» поведении государства (когда оно не на-

рушает права и законные интересы других государств). «При обстоятельствах, когда нарушение права, равно как злоупотребление правом представляются неприемлемыми с точки зрения добросовестного выполнения государствами своих международных обязательств, юридически значимое правомерное поведение государств образует собой юридическую основу системы коллективной безопасности на пространстве всего мирового сообщества в целом», – говорят авторы [2, с. 96].

Такое качество, как «целостность» системы международной безопасности, обеспечивается общим пониманием государствами стоящих перед ней задач. С.А. Лобанов и Я.Д. Сухарева говорят о «консенсусе» в отношении угроз международному сообществу как юридической основе устранения их причин. Практическая реализация такого консенсуса – устранение угрозы, рассматривается ими как «конечный юридический результат правомерного юридически значимого поведения государств» [2, с. 96–97; см. также: 1, с. 91]. В условиях, когда государства взаимно реализуют общую (позитивную) ответственность поддержания международной безопасности, проявляется основа развития системы безопасности в «режиме равнозначной юридической безопасности всего субъектного состава системы международных правоотношений» [2, с. 96–97]. В этом же, как представляется, проявляется юридическая основа юстиции в международной системе.

Добросовестное участие государства в системе международной безопасности

Система международной безопасности рассматривается как «коллективная». Ее эффективность прямо зависит от вклада государств в ее реализацию. Р.А. Каламкарян и Е.В. Мигачева говорят о «слаженности» в действиях государств как части их должного поведения. Требование действовать слаженно они рассматривают как «предписание прямого юридического воздействия». Приверженность целям Устава ООН показательно реализуется во вкладе государства в обеспечение мира и безопасности, в разрешение международных споров [1, с. 91]. Показательны также нарушения государствами международного права, нарушения ими прав и законных интересов других государств.

По мнению С.А. Лобанова и Я.Д. Сухаревой, сама логика потребности в целостной системе международного права, взаимозависимости современного мира диктует значимость выполнения

государствами международных обязательств на основе принципа добросовестности *bona fides* [2, с. 96]. Система международной безопасности, опирающаяся на эффективное сотрудничество государств, дает позитивный (созидательный) импульс взаимосвязанности мирового сообщества. Юридический интерес государства сопряжен с юридическим интересом мирового сообщества. Система такого рода позволяет приблизиться к пониманию акта юстиции в международной системе – разрешения споров между государствами не просто мирными средствами, но посредством вынесения судебным органом ООН обязательного для сторон решения (*res judicata*) [2, с. 97].

С иной стороны на международное правосудие смотрят Д. Голдензиел, профессор Национального университета обороны – Колледжа информации и киберпространства (США), Ш. Блочбергер и Т. Грэнхолм, исследователи Юридического факультета Виргинского университета (University of Virginia School of Law) (США) в статье «Оружие слабых: законность и государственная власть в Международном суде ООН» [5]. С их точки зрения, правовые средства, используемые государствами, следует рассматривать как целенаправленное использование закона для достижения стратегической, оперативной или тактической цели против конкретного противника, или для укрепления легитимности собственных стратегических, оперативных или тактических целей, или для подрыва легитимности действий противника [5, р. 573].

Авторы предполагают, что государства будут передавать споры в Международный суд ООН для достижения целей, которых они не могут достичь иным военным путем. Судебные иски в Международный суд могут быть своего рода инструментальным средством правовой защиты, использующим закон для достижения военной цели, которая в противном случае могла бы быть достигнута с помощью насилия [5, р. 573]. Если Международный суд является нейтральным арбитром, государства, имеющие асимметричное преимущество на поле боя или в стратегической конкуренции, скорее всего будут вести споры в зале суда [5, р. 573].

Д. Голдензиел, Ш. Блочбергер и Т. Грэнхолм анализируют политологические исследования условий, при которых государства выбирают международные механизмы разрешения споров, которые показывают, что государства, равные с юридической, военной или экономической точек зрения, с наибольшей вероятностью окажутся в зале суда. Так, демократические страны, лидеры которых стремятся использовать орган по разрешению споров в каче-

стве внутривластного прикрытия того, что может привести к неблагоприятному исходу урегулирования спора, с наибольшей вероятностью будут представлять споры на рассмотрение [5, р. 573]. Государства с большей вероятностью будут передавать споры в международные суды, когда юридическая сила их аргументов ненамного превосходит аргументы их оппонентов [5, р. 573–574].

Обращение к правовому урегулированию территориальных споров наиболее вероятно в тех случаях, когда две стороны относительно равны по военной мощи. Лидеры государств с меньшей вероятностью прибегнут к международным органам по разрешению споров для урегулирования территориальных споров, когда одна из сторон имеет явное военное преимущество [5, р. 574].

Заключение

Определение направлений развития системы международной безопасности зависит от понимания международной системы. Разность в подходах, представленных в обзоре российских и зарубежных («западных») авторов к положению в международной системе государства и его влиянию на международные механизмы, отражается в акцентах их внимания. Так, в пределах конструкции права ООН Р.А. Каламкарян и Е.В. Мигачева выделяют потребности миротворческих операций ООН, наращивание их потенциала. Применение санкций в международной системе «вне включенности факторы силы» требует осмысления с позиции их влияния на государство и их население, а также предметной направленности [1, с. 91–92].

Примечателен в этом отношении тезис С.А. Лобанова и Я.Д. Сурхаева об ответственности за развитие системы международной безопасности. Система, в основе которой лежит международное право, показательна юридической ответственностью государств содействовать безопасности [2, с. 97].

Х. Сиссе высказал в своей статье тезис, что неспособность действовать решительно, основываясь на международном праве и коллективных интересах, в отличие от предполагаемых краткосрочных интересов отдельных стран, подрывает легитимность и эффективность Организации Объединенных Наций в целом [4, р. 408]. Тем не менее в качестве контраргумента можно выделить гипотезу, данную в статье Р.А. Каламкаряна и Е.В. Мигачевой о том, что «Современный миропорядок как воплощение целостности

системы международного права позиционирован в параметрах отсутствия пробельности, способностью судебных органов международного правосудия осуществлять урегулирование международных споров через суд на основе права и справедливости, обеспечения неотвратимости наказания в части процесса международного уголовного правосудия в отношении всего круга международных преступлений, поддержания универсальной международной безопасности на основе Устава ООН» [1, с. 89]. Многосторонний подход в решении общих задач международного сообщества напрямую зависит от наличия у государств общих ценностей и общей ответственности за состояние международной системы.

Список литературы

1. Каламкарян Р.А., Мигачева Е.В. Целостность системы права ООН как основа последовательного внешнеполитического курса Российской Федерации на обеспечение международного мира и безопасности // Вестник экономической безопасности. – 2024. – № 5. – С. 89–93.
2. Лобанов С.А., Сурхаева Я.Д. Универсальная международная безопасность на основе Устава ООН как реализация установочных целей внешней политики Российской Федерации // Вестник экономической безопасности. – 2025. – № 1. – С. 95–100.
3. Шинкарецкая Г.Г. Повышение уровня мирового океана и защита населения уязвимых районов // Труды Института государства и права РАН. – 2024. – Т. 19, № 1. – С. 109–136.
4. Cisse H. Global Governance at a Crossroads: Incremental Reform or Fundamental Transformation? // Harvard International Law Journal. – 2025. – Vol. 66. – P. 401–429.
5. Goldenziel J., Blochberger S., Granholm T. Weapon of the Weak: Lawfare and State Power in the International Court of Justice // Harvard International Law Journal. – 2025. – Vol. 66. – P. 563–631.

ГЛОТОВ С.А.¹ «ЦИФРОВОЙ КИТАЙ»: ОБЗОР ЗАКОНОДАТЕЛЬНЫХ АКТОВ КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКИ, РЕГУЛИРУЮЩИХ ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. В обзоре рассматриваются три ключевых акта Китайской Народной Республики, регулирующих отношения в области цифровизации, больших данных, цифровой экономики. Это Закон о кибербезопасности КНР; Закон о безопасности данных КНР; Закон о защите персональных данных КНР.

Ключевые слова: Китай; цифровизация; цифровое право; кибербезопасность; защита данных; утечка данных; безопасность данных; персональные данные; объекты критической инфраструктуры; мониторинг безопасности данных; юридическая ответственность.

GLOTOV S.A. “Digital China”: review of legislative acts of the people's republic of china regulating cybersecurity and personal data protection

Abstract. The review examines three key acts of the People's Republic of China regulating relations in the field of digitalization, big data, and the digital economy. These are the Cybersecurity Law of the People's Republic of China; the Data Security Law of the People's Republic of China; the Law on the Protection of Personal Data of the People's Republic of China.

Keywords: China; digitalization; digital law; cybersecurity; data protection; data leakage; data security; personal data; critical infrastructure facilities; data security monitoring; legal responsibility.

¹ Глотов Сергей Александрович, ведущий научный сотрудник отдела правоведения ИНИОН РАН, доктор юридических наук, профессор.

Для цитирования: Глотов С.А. «Цифровой Китай»: Обзор законодательных актов КНР, регулирующих вопросы кибербезопасности и защиты персональных данных // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4: Государство и право. – 2026. – № 1. – С. 182–198. – DOI: 10.31249/iajpravo/2026.01.12

Введение

В 2025 г. в издательстве «Проспект» вышла книга «Избранные нормативно-правовые акты Китайской Народной Республики в области цифровизации»¹, которая содержит тексты законов КНР, регулирующие отношения в сферах кибербезопасности и защиты данных, в том числе персональных. Данный сборник избранных нормативных правовых актов КНР для российского читателя, прежде всего юристов, перевела Ли Яо, доктор юридических наук из Института верховенства права за рубежом при Восточно-Китайском университете политических наук и права.

В предисловии к этому сборнику Ли Яо замечает, что «искусственный интеллект создает много удобного и эффективного для жизни общества, однако и порождает потенциальные сокрушительные риски, которые в основном отражаются в ряде вопросов, таких как защита конфиденциальности, дискриминация данных, трансграничные данные, безопасность данных и др. (...) Юристам всего мира необходимо активно реагировать на них и добиваться баланса между безопасностью данных и экономическим развитием, выстраивая правовую систему, обеспечивающую национальную безопасность, общественные интересы, защиту законных прав граждан и юридических лиц и других организаций в киберпространстве» (с. 3).

КНР стала одной из ведущих стран мира в развитии цифровой экономики, больших данных и искусственного интеллекта, машинного обучения, мобильных платежей блокчейна, умного правосудия и т.д. Ли Яо приводит такие данные: в 2023 г. объем цифровой экономики Китая достиг 53,9 трлн юаней, доля цифровой экономики в ВВП КНР составляет 42,8% (там же). Это подтверждается и показателями, уже 2024–2025 гг., а также тем, что Китай является сегодня общепризнанной мировой фабрикой това-

¹ См.: Избранные нормативно-правовые акты Китайской Народной Республики в области цифровизации / пер. с кит. Ли Яо. – Москва: Проспект, 2025. – 136 с.

ров, да и во многом услуг. С помощью «цифры» и других инструментов ведения бизнеса и администрирования ему удалось стать второй экономикой мира.

Достигнуть подобного рода результатов невозможно без качественного эффективного правового обеспечения, и в этой связи китайский опыт правового регулирования в области цифровизации, кибербезопасности, защиты данных интересен и для российской научной общественности.

В сборник законов КНР в рассматриваемой области включены не только законы КНР в сфере цифровизации, принятые Всекитайским собранием народных представителей (ВСНП), но и различные положения, утвержденные постановлениями Государственного совета КНР с указанием их срока вступления в силу (например постановление Госсовета КНР № 745 «О защите безопасности критической информационной инфраструктуры» от 27.04.2021 г., вступившее в силу с 01.09.2021 г.).

В данном обзоре кратко анализируются основные положения следующих законов КНР в области цифровизации.

№ п/п.	Наименование законов, включенных в сборник, и количество статей в них	Время принятия Постоянным комитетом ВСНП и вступления их в силу
1	Закон о кибербезопасности КНР, содержит 79 статей	Принят 07.11.2016 г. Вступил в силу 01.01.2017 г.
2.	Закон о безопасности данных КНР – 55 статей	Принят 10.06.2021 г. Вступил в силу 01.09.2021 г.
3	Закон о защите персональных данных КНР – 74 статьи	Принят 20.08.2021 г. Вступил в силу 01.11.2021 г.

Закон КНР о кибербезопасности

Закон о кибербезопасности принят в целях «поддержания суверенного киберпространства и национальной безопасности, социальных общественных интересов, защиты законных прав и интересов граждан, юридических лиц и других организаций, а также содействия здоровому развитию информатизации экономики и общества» (ст. 1).

Следует отметить, что понятие «кибербезопасность» определяется в ст. 76 Закона гл. 7 «Дополнительные положения». В ней *Кибербезопасность* понимается как «способность предотвращать атаки, вторжение, вмешательство, разрушение и незаконное использование сети, а также аварии, путем принятия необходимых мер для поддержания сети в стабильном и надежном состоянии, а

также для обеспечения целостности, конфиденциальности и доступной сети».

Указанная статья определяет: «*сеть* – это система, состоящая из компонентов или других информационных терминалов и соответствующего оборудования, которая собирает, хранит, передает, обменивается и обрабатывает информацию, согласно с определенными правилами и процедурами»; «*операторы сетей* – владельцы и администраторы сетей и поставщики сетевых услуг; сетевые данные – все виды электронных данных, собираемых, хранимых, передаваемых, обрабатываемых и создаваемых в сети»; «*персональные данные* – все виды информации, записанные в электронном или ином виде, которая может идентифицировать личность физического лица, отдельно или в сочетании с другой информацией, включая, но не ограничиваясь ФИО физического лица, дату рождения, номер документа, удостоверяющего личность, личную биометрическую информацию, адрес проживания, номер телефона и т.д.».

Структура Закона КНР о кибербезопасности: общие положения (гл. 1); вопросы поддержания кибербезопасности и продвижения ее на государственном уровне (гл. 2); правовой режим безопасности сетевых операций (гл. 3); безопасность самих сетей (гл. 4); а также создание системы мониторинга и раннего предупреждения кибербезопасности (гл. 5) и юридической ответственности (гл. 6), дополнительные положения (гл. 7).

Закон устанавливает:

1. *Права и обязанности государства в сфере кибербезопасности*. Государство формирует и постоянно совершенствует стратегию кибербезопасности, определяет основные требования и главные цели по обеспечению кибербезопасности, предлагает политику, задачи и меры по обеспечению кибербезопасности в ключевых отраслях (ст. 4). Государство: выявляет угрозы кибербезопасности, определяет и реализует меры по поддержанию безопасности и порядка в киберпространстве (ст. 5), «пропагандирует честное добросовестное полезное и цивилизованное поведение в интернете» (ст. 6); активно участвует в международных обменах и сотрудничестве в области управления киберпространством (ст. 7).

Государственный департамент сетевой информации, отвечающий за координацию работы по обеспечению кибербезопасности (ст. 8), участвует в создании и эксплуатации сетей Интернет, улучшает уровень веб-сервисов, обеспечивает их безопасность (ст. 10, 12); защищает права граждан и юридических лиц, органи-

заций, работающих в сети (ст. 12); поддерживает исследования и разработку сетевых продуктов, способствующих здоровому развитию несовершеннолетних, и наказывает тех, кто использует Интернет, угрожая физическому и психологическому здоровью несовершеннолетних (ст. 13).

За защиту, надзор и управление кибербезопасностью в рамках своих обязанностей отвечает Департамент телекоммуникаций при Государственном совете КНР, Департамент общественной безопасности и другие компетентные органы (ст. 8). В приведенных выше положениях Закона есть важное указание законодателя на конкретные государственные органы, отвечающие за выполнение конкретных норм Закона.

2. Права и обязанности лиц и организаций в сети Интернет. Они обязаны: соблюдать Конституцию КНР и законы, общественный порядок и общественную мораль в данной сфере, не должны ставить под угрозу кибербезопасность (ст. 12).

Лица и организации имеют право: сообщать в департамент сетевой информации, телекоммуникации и общественной безопасности о любых действиях, которые ставят под угрозу кибербезопасность (ст. 14); в свою очередь, соответствующие ведомства должны сохранять конфиденциальную информацию, поступившую от осведомителей, и защищать законные права и интересы осведомителей (ст. 14).

3. Продвижение Концепции и конкретных требований кибербезопасности государством и обществом (ст. 15–20). Государство создает стандарты кибербезопасности, в том числе отраслевые, связанные как с управлением процессами в данной области, так и с обеспечением безопасности сетевых продуктов и услуг. Эта функция возложена на Административный департамент по стандартизации при Государственном совете, а также госсоветы и народные правительства провинций, автономных районов, городов и т.д. Эта деятельность осуществляется на плановой основе, путем роста инвестиций, поддержки научных исследований и защищает при этом интеллектуальную собственность на сетевые технологии.

Активными проводниками государственной политики кибербезопасности являются предприятия и организации, различные НИИ, вузы и профтехучилища. «Средства массовой информации

проводят массовую пропаганду и просвещение общества по вопросам кибербезопасности» (ст. 19)¹.

4. *Обязанности операторов сетей и безопасность закреплены в ст. 21–50.* Операторы сетей «обязаны защитить сеть от вмешательства, разрушения или несанкционированного доступа, также предотвращать утечку, кражу сетевых данных или фальсификацию (ст. 21). Для этого сетевые операторы предпринимают организационные и технические меры, обеспечивают сохранение соответствующих сетевых данных в течение не менее шести месяцев, их классификацию, разрешение копирования и шифрование наиболее важных данных.

Закон КНР о кибербезопасности также определяет, что *операторы крупнейших инфраструктур* обязаны проверять свои сети не реже одного раза в год в режиме тестирования и оценки, информируя об этом власти, в том числе Государственный департамент сетевой информации. Обращается внимание на то, что операторы сети «должны сохранять строгую конфиденциальность сообщений или информацию о пользователях и создавать надежную систему защиты информации о пользователях (ст. 40), не должны раскрывать, подделывать или уничтожать собранные или персональные данные, не должны предоставлять персональные данные другим лицам без согласия лица, у которого они собраны» (ст. 42), а если «физическое лицо ощущает, что операторы сетей собирают или используют его персональные данные в нарушение положений законов ... то операторы сетей обязаны принять меры по удалению или неиспользованию» (ст. 42).

Поставщики сетевых продуктов и услуг не должны устанавливать вредоносные программы; наоборот, обязаны обеспечивать обслуживание безопасности своих продуктов и услуг на постоянной основе, сообщать пользователю и получать согласие на сбор персональных данных, осуществлять сертификацию своих процессов и оборудования, проверять подлинность идентификационной информации, регистрировать доменные имена, своевременно устранять риски безопасности, такие как компьютерные вирусы, сетевые атаки и вторжение в сеть и т.д. (ст. 22–26).

¹ Подробнее об этом см.: Галяшина Е.И., Анонян Е.А., Богатырёв Е.Н. Защита от злоупотребления искусственным интеллектом и нейротехнологиями в аспекте медиабезопасности: монография / отв. ред. Е.И. Галяшина. – Москва: Проспект, 2025. – 272 с.

Закон КНР о кибербезопасности предусматривает, что «ни одно физическое лицо или организация не должны заниматься деятельностью, угрожающей кибербезопасности путем незаконного вторжения в чужие сети, нарушения нормального функционирования чужих сетей, кражи сетевых данных и т.д. (ст. 27)¹. Важно и то, что «любое лицо или организация несут ответственность за использование сети и не должны создавать веб-сайты или коммуникационные группы с целью совершения мошенничества, обучения преступным методам, изготовления или продажи запрещенных или контролируемых предметов» (ст. 46 Закона) что сегодня становится особенно актуальным.

5. *Мониторинг и раннее предупреждение кибербезопасности, а также вопросы юридической ответственности* (ст. 51–75). Мониторингом раннего предупреждения занимаются отраслевые департаменты, ответственные за защиту безопасности критической инфраструктуры при руководящей (контролирующей) роли государственного департамента сетевой информации.

Закон КНР о кибербезопасности в гл. 6 устанавливает юридическую ответственность операторов, не выполняющих обязательства по защите кибербезопасности: значительные штрафы накладываются как на саму компанию, так и на ее контролирующий и непосредственно отвечающий за работу операторов лиц; возможно приостановление соответствующей деятельности, закрытие веб-сайта, отзыв лицензии и др.(ст. 62).

Согласно ст. 64, к оператору сетей, посягающему на право персональных данных, наряду с уже указанными мерами воздействия могут быть применены и такие, как «конфискация незаконных доходов или штраф в размере не менее двойной и не более десятикратной суммы незаконных доходов», а если незаконных доходов нет, то накладывается штраф в размере не более 1 млн юаней.

Если сетевые операторы хранят информацию из разряда критической информационной инфраструктуры (о чем подробно говорится в ст. 31–39 Закона) за пределами страны или предоставляют данные за пределы страны, в нарушение ст. 37 Закона², то их

¹ Об этико-правовой проблематике по данному вопросу см., напр.: Бахтев Д.В. Искусственный интеллект: этико-правовые основы: монография. – Москва: Проспект, 2025.–176 с.

² В ст. 37 Закона КНР о кибербезопасности устанавливается, что персональные данные и важные данные, собранные и созданные операторами, должны храниться на территории страны. Если возникает деловая потребность в передаче

также ожидает предписание об исправлении и предупреждение; конфискация незаконного дохода, штраф в размере не менее 50 тыс. и не более 500 тыс. юаней; приостановка деятельности; закрытие веб-сайта; отзыв лицензии, а также штраф на контролирующий персонал и персонал, непосредственно отвечающий за работу, в размере не менее 10 тыс. и не более 100 тыс. юаней (ст. 66).

Закон КНР о кибербезопасности в ст. 31 содержит перечень критических отраслей критической инфраструктуры, нуждающейся (защищаемой) кибербезопасностью. Это: государственные коммуникации и информационные услуги; энергетика, транспорт, водоснабжение; финансы, государственные услуги; электронное правительство и др.

Критерием важности защиты подобного рода инфраструктуры является факт «повреждения, потери функции или утечки данных», которые «могут серьезно угрожать национальной безопасности, жизнеобеспечению населения и общественным интересам» (ст. 31).

Конкретные рамки «критических информационных структур и мер их защит» определяет Государственный совет КНР.

Указанный Закон в ст. 67 предусматривает возможность карать и тех, кто «создает веб-сайты или коммуникационные группы с целью совершения незаконной деятельности или использует интернет для публикации информации, связанной с совершением незаконной или преступной деятельности».

Если это преступление не влечет уголовной ответственности, то лицам, вставшим на этот путь, грозит: арест на срок не более пяти суток и штраф в размере не менее 10 тыс. и не более 100 тыс. юаней, при отягчающих обстоятельствах арест на срок не менее пяти, но не более 15 суток и штраф в размере не менее 50 тыс. и не более 500 тыс. юаней, а также закрытие веб-сайта и коммуникативной группы.

Приговор по таким делам выносит орган общественной безопасности. Если это касается деятельности не лица, а организации в аналогичных случаях, то на организацию, ее руководящий и контролирующий состав накладывается штраф в размере не менее 100 тыс. и не более 500 тыс. юаней. Приговор также выносит орган общественной безопасности.

этих данных за рубеж, оценки их безопасности и возможности передачи производятся государственным департаментом сетевой информации совместно с соответствующим департаментом Государственного совета КНР.

В ст. 69 Закона КНР о кибербезопасности содержится исчерпывающий перечень действий, за которые операторы несут ответственность, если они не вносят исправления, предписанные соответствующим государственным органом, действующим в сфере обеспечения кибербезопасности: 1) невыполнение требований по уничтожению или удалению запрещенной к публикации, распространению информации; 2) отказ или воспрепятствование осуществлению компетентным департаментом законного надзора и проверок; 3) неоказание технической поддержки и помощи органам общественной и государственной безопасности.

Анализируемый Закон в ст. 73 предусматривает ответственность государственных структур, действующих в сфере безопасности, за пренебрежение их сотрудников своими обязанностями; злоупотребление своими полномочиями; недобросовестную деятельность в целях личной выгоды, если это не является преступлением¹. Если же в их действиях содержится состав преступления, виновные несут уголовную ответственность в соответствии с законом (ст. 74).

Следует заметить, что некоторые важные положения Закона КНР о кибербезопасности регулируются Гражданским кодексом КНР, принятым в 2020 г., вступившим в силу с 1 января 2021 г. Глава 6 «Право на неприкосновенность частной жизни и защиты персональных данных» ГК КНР (ст. 1032–1039) определяет понятия и содержание права на неприкосновенность частной жизни и персональных данных, условия обработки и ответственности операторов персональных данных, сохранение тайны сведений о личности и ее персональных данных. Статья 1039 ГК КНР устанавливает обязанность органов государственной власти, организаций, наделенных административными функциями, а также их сотрудников сохранять в тайне сведения, относящиеся к личной жизни граждан и их персональным данным, которые становятся им известны в связи с исполнением обязанностей, не вправе распространять указанные сведения и персональные данные или осуществлять их передачу в нарушение закона.

¹ Об уголовной ответственности в Китае см. подробнее: Гео Минсюань. Зарождение, становление и развитие современного уголовного законодательства в Китайской Народной Республике: монография / под науч. ред. Н.А. Сидоровой, И.В. Васильева. – Москва: Проспект, 2025. – 568 с.

Китай: безопасность больших данных

Закон КНР о безопасности данных принят Постоянным комитетом ВСНП спустя пять лет после вступления в силу Закона КНР о кибербезопасности, т.е. в 2021 г. Он содержит семь глав, 55 статей и имеет целью регулировать деятельность информационных властей КНР по отношению безопасности данных, воздействию, развитию и использованию данных законных прав и интересов физических лиц и организаций. Речь идет также о защите национального суверенитета, безопасности и интересов развития Китая и его граждан (ст. 1 Закона о безопасности данных).

Этот Закон регулирует обработку данных как на территории КНР, так и за его пределами. Если это угрожает национальной безопасности Китая, общественным интересам или законным интересам граждан, то речь идет в первую очередь о защите правительственных данных, а также содержит следующие определения понятий, важных для реализации этого Закона.

Данные – любая запись информации с помощью электронных или иных средств обработка данных, включая сбор, хранение, использование, обработку, передачу, предоставление, распространение данных и т.д. (ст. 3).

Безопасность данных – способность гарантировать, что данные находятся в состоянии эффективной защиты и законного использования, а также способность гарантировать постоянное состояние безопасности принимаемых необходимых мер (ст. 3).

Система обеспечения безопасности данных в КНР включает Центральное агентство по руководству национальной безопасностью, отвечающее за безопасность данных национального характера, их изучение, формулирование, выработку «национальной стратегии безопасности данных и соответствующих основных политик, координацию основных вопросов и важных работ по обеспечению национальной безопасности данных» (ст. 5).

Народные правительства на уровне провинций и выше, – согласно ст. 14 Закона, – должны включать развитие цифровой экономики в национальный план экономического и социального развития на местном уровне и разработать план развития цифровой экономики в соответствии с потребностями.

Государство берет на себя целый ряд обязанностей: защиту прав и интересов физических лиц¹ и организаций, связанных с данными; разумное и эффективное использование данных в соответствии с законом, гарантии свободного потока данных в упорядоченном порядке; развитие цифровой экономики, ключевым элементом которой являются данные (ст. 7); пропаганду и распространение знаний о безопасности данных, повышение осведомленности среди населения и уровня защиты данных в обществе, отраслевых организациях, НИИ, на предприятиях и у частных лиц (ст. 9); осуществление международного обмена и сотрудничество в области управления безопасностью данных эксплуатации и использования данных, развитие международных правил и стандартов, связанных с безопасностью данных; обеспечение безопасного и свободного трансграничного потока данных (ст. 12); координацию развития и безопасности, продвижение безопасности данных в промышленном развитии (ст. 13); развитие использования данных для повышения интеллектуального уровня государственных услуг (ст. 15); поддержку исследований в обществе технологий эксплуатации и использование данных и безопасности данных, продвижение технологий и коммерческих инноваций в области данных, в том числе в промышленных разработках и системах (ст. 17); поддержку развития тестирования, оценки, сертификации и других услуг в области безопасности данных (ст. 18); совершенствование системы управления операциями с данными, развитие рынка операций с данными (ст. 19); поддержку образовательных учреждений, НИИ, предприятий в проведении обучения и подготовки кадров, связанных с технологией эксплуатации и использования данных безопасности данных (ст. 20).

Закон КНР о безопасности данных в гл. 3 закрепляет права и обязанности государства в сфере защиты данных. Государство берет на себя следующие обязанности: создание системы классификации и иерархии по защите данных для предотвращения их фальсификации, уничтожения, утечки, незаконного приобретения и использования в области национальной безопасности, жизнеобеспечения национальной экономики, значимых национальных интересов и нужд народа (ст. 21); формирование национального координационного механизма по безопасности данных (ст. 21); совершенствование централизованного единого эффективного и

¹ См., напр.: Ван Лимин. Личные права: учебник. – Москва: Проспект, 2023. – гл. 14: Право на персональные данные. – С. 283–296.

авторитетного механизма оценки рисков безопасности данных отчетности, обмена информацией, мониторинга и раннего предупреждения (ст. 22); создание механизма реагирования на чрезвычайные ситуации, связанные с безопасностью данных, предотвращением расширения ущерба, устранением потенциальных рисков безопасности и своевременного распространения информации о предупреждении общественности, отвечает за это соответствующий компетентный департамент (ст. 23); установление системы проверки безопасности данных; осуществление экспертного контроля в отношении данных, которые также затрагивают национальную безопасность (ст. 24, 25).

И еще один важный аспект из общих правил поведения в информационном пространстве в процессе оборота цифровых данных предусмотрен ст. 10 рассматриваемого Закона: все участники делового, хозяйственного и т.д. оборота, отраслевые организации в соответствии со своими уставами должны разрабатывать свои «кодексы поведения и групповые стандарты безопасности данных, на основе закона укреплять самодисциплину в отрасли, направлять своих членов на совершенствование защиты безопасности данных, повышать уровень защиты безопасности данных, способствовать здоровому развитию отрасли».

Китайское государство в сфере безопасности и открытости правительственных данных, согласно ст. 39–43, вправе и обязано: создавать и совершенствовать систему управления безопасностью данных; получать другим лицам создавать и поддерживать систему электронного правительства, хранить и обрабатывать правительственные данные (ст. 44), но при этом контроль за этими лицами оставляет за собой; следовать в своей работе принципам справедливости, честности и удобства и раскрывать правительственные данные своевременно и точно, за исключением тех, которые не разглашаются в соответствии с Законом (ст. 41); разрабатывать открытый канал правительственных данных, создавать единую стандартизированную взаимосвязанную безопасную и контролируруемую платформу для открытия правительственных данных (ст. 42).

Закон КНР о безопасности данных в гл. 6 уточняет, за что и в каких размерах накладываются штрафы на физические лица и организации за допущенные нарушения при обработке данных (максимально это не более 10 млн юаней). При этом соответствующий компетентный департамент может принимать и такие меры воздействия, как предписание исправить ситуацию; вынести

предупреждение; вынести постановление о приостановке соответствующей деятельности; отозвать соответствующее разрешение или лицензию на ведение предпринимательской деятельности и даже провести собеседование с соответствующими организациями и лицами и потребовать от них принятия мер по исправлению и устранению скрытых опасностей (ст. 44).

Закон КНР о безопасности данных предусматривает и другие штрафные санкции за нарушения в области безопасности и открытости правительственных данных (ст. 47–48). Дисциплинарные взыскания могут быть наложены на контролирующий и другой отвечающий непосредственно за работу персонал, если государственный орган не выполняет свои обязанности по защите безопасности данных.

Уголовной, административной ответственности должны быть подвергнуты те, кто «крадет или приобретает данные другими незаконными способами, осуществляет деятельность по обработке данных с целью исключения или наносит ущерб законным правам и интересам частных лиц или организаций» (ст. 51).

Не исключается гражданско-правовая ответственность за нарушения Закона о безопасности данных (ст. 52), а тех, кто нарушает управление общественной безопасностью ожидает административная ответственность.

Как и в Законе КНР о кибербезопасности, Закон КНР о безопасности данных содержит положение о том, что меры по защите безопасности военных данных должны быть отдельно сформулированы Центральной военной комиссией (ст. 54).

КНР: право на защиту персональных данных

Закон КНР о защите персональных данных принят Постоянным комитетом ВСНП 13го созыва 20.08.2021 г. и вступил в силу с 01.01.2022 г., т.е. всего на два месяца позже Закона КНР о безопасности данных. Этот Закон был принят на основе Конституции КНР в целях защиты прав и интересов в отношении персональных данных, стандартизации деятельности по их обработке и рациональному использованию (ст. 1).

«Персональные данные», согласно ст. 4 Закона, – «это все виды информации, записанные электронным или иным способом, относящиеся к идентификационному или идентифицируемому физическому лицу, за исключением информации, обработанной после анонимизации» (ст. 4).

Данный Закон содержит восемь глав, 74 статьи и декларирует: «персональные данные физических лиц охраняются законом, и никакая организация или частное лицо не могут нарушать права и интересы в отношении персональных данных физических лиц» (ст. 2); «персональные данные должны обрабатываться в соответствии с принципами законности, обоснованности, необходимости и честности» (ст. 5), а также «ни одна организация или частное лицо не должны незаконно собирать, использовать, обрабатывать или раскрывать персональные данные другого лица» (ст. 10).

Рассматриваемый Закон распространяет свое действие на обработку персональных данных китайских граждан за границей (ст. 10). Закон применяется в трех случаях: 1) в целях предоставления продуктов или услуг физическим лицам, находящимся на территории КНР; 2) при анализе и оценке поведения физических лиц, находящихся на территории КНР; 3) в других обстоятельствах, предусмотренных в законах или административных нормах Китая.

В гл. 1 «Общие положения» Закона КНР о защите персональных данных предусматривается: 1) «государство не только создает надежную систему защиты персональных данных и строго наказывает тех, кто это нарушает, но и усиливает пропаганду и просвещение в области защиты персональных данных, способствует формированию благоприятной среды, в которой правительство, предприятия, соответствующие общественные организации и население участвуют в защите персональных данных» (ст. 11); 2) готовность КНР активно участвовать на международном уровне: в разработке международных правил по защите персональных данных; их обмене и сотрудничестве; взаимном признании правил и стандартов, действующих в других странах и регионах; взаимодействии с международными организациями (ст. 12).

В гл. 2 (ст. 28–37) Закона устанавливаются правила обработки персональных данных¹. Обработка персональных данных может работать с данными несовершеннолетнего в возрасте до 14 лет только получая согласие родителей или опекуна несовершеннолетнего (ст. 31).

Закон КНР о защите персональных данных в ст. 13 определяет семь обстоятельств, в связи с которыми обработчик может

¹ Под *обработкой персональных данных* ст. 73 данного Закона понимает «организацию или физическое лицо, которые самостоятельно принимают решение о цели и способах обработки персональных данных».

заниматься обработкой данных. Это получение согласия физического лица, когда оно необходимо для выполнения установленного законом полномочий или обязанностей, когда необходимо для заключения или исключения договора и в других случаях. Среди них есть такой: частичная обработка данных «в целях мониторинга общественного мнения и других действий в общественных интересах» (п. 5 ст. 13).

Чтобы приступить к обработке персональных данных (ст. 17), обработчик должен выполнить четыре условия, в том числе: «на видном месте и на ясном и понятном языке, правдиво, точно и полно информировать о своем наименовании и контактных данных, цели и порядке обработки персональных данных, сроки их хранения, правах и обязанностях физического лица, чьи данные обрабатываются». Обработчик персональных данных «не должен раскрывать обрабатываемые им персональные данные, кроме как с отдельного согласия физического лица» (ст. 25).

Анализируемый Закон в гл. 3 определяет условия и порядок передачи персональных данных за границу «в связи с деловыми или иными потребностями» (ст. 38). В связи с этим обработчик должен проходить оценку безопасности передаваемых данных (чем занимается Государственный департамент сетевой информации) либо иметь сертификат по защите персональных данных. При этом получатель данных за пределами КНР должен соответствовать стандартам защиты персональных данных, определяемых Законом КНР о защите персональных данных (ст. 38 Закона). Данные «критических инфраструктур» передаются обработчиком за пределы КНР только с разрешения Государственного департамента сетевой информации после проведения «оценки безопасности» (ст. 40).

Довольно подробно права физически лиц в процессе обработки и передачи персональных данных определены в гл. 4 Закона КНР о защите персональных данных (ст. 44–50). Главное состоит в том, что физическое лицо имеет право: знать и принимать решение об обработке персональных данных или отказаться от этого; проверять и копировать свои данные. Потребовать исправить или заменить собранные данные; отозвать свое согласие на сбор и обработку данных и т.д. Всё это, конечно, реализуется в рамках действующего в КНР законодательства.

Обязанности обработчиков персональных данных и госорганов, занимающихся их защитой, регулируются ст. 51–65 гл. 5 Закона КНР о защите персональных данных. Так, ст. 51 содержит

перечень требований к обработчику персональных данных, выполнение которых позволяет предотвратить незаконный доступ, а также утечку, фальсификацию и потерю данных. Среди них: разработка компанией-разработчиком данных внутренних систем управления и операционных процедур, внедрение классификационного управления персональными данными, принятия соответствующих технических мер безопасности и т.д. При этом устанавливается персональная ответственность лица, занимающегося непосредственно обработкой данных. Сведения о нем передаются в департамент, выполняющий обязанности по защите персональных данных (ст. 52).

Закон КНР о защите персональных данных требует от обработчика данных: провести предварительную оценку воздействия на защиту персональных данных и определить порядок, в том числе определить, являются ли принятые меры защиты законными, эффективными и соответствующими степени риска (ст. 56); немедленного принятия мер по исправлению ситуации при утечке, фальсификации и потере персональных данных (ст. 57).

Обязанности отраслевых департаментов, выполняющих работу по защите персональных данных (а они, как указывалось выше, действуют под руководством Государственного департамента сетевой информации), определены в ст. 61 Закона КНР о защите персональных данных: расследование и рассмотрение незаконных действий обработчиков данных; рассмотрение поступивших жалоб; проведение пропаганды и обучение по вопросам защиты персональных данных и др.

Данный Закон также предусматривает обязанности Государственного департамента сетевой информации, как то: разработка конкретных правил и стандартов для защиты персональных данных, поддержка исследований в данной области деятельности, содействие созданию системы специализированных услуг по защите персональных данных и др.

Права департаментов, выполняющих обязанности по защите персональных данных, включая право на проведение проверки бухгалтерских книг, опроса заинтересованных сторон, проведение проверок на местах и расследований проверки оборудования и т.д., определены в ст. 63 Закона.

Любая организация или частное лицо «имеют право подать жалобу или заявление о незаконной деятельности по обработке персональных данных в департаменты» (ст. 65), которые обязаны дать заявителю ответ. Сами же департаменты, выполняющие обя-

занности по защите персональных данных, «должны обнародовать конкретную информацию для получения жалоб и заявлений» (ст. 65).

Закон КНР о защите персональных данных в гл. 7 «Юридическая ответственность» (ст. 66–71) предусматривает ряд санкций, которые могут быть наложены на лицо, обрабатывающее персональные данные и нарушающее требования Закона: предупреждение; конфискация незаконных доходов; штраф в размере не более 1 млн юаней (на организацию); штраф не менее 10 тыс. юаней и не более 100 тыс. юаней (на контролирующий персонал и непосредственных исполнителей); приостановление деятельности; отзыв лицензии или разрешения на работу и др. (ст. 66).

При этом не исключается уголовная ответственность и занесение в кредитный рейтинг в соответствии с нормами административного права, а также предание гласности о случившейся ситуации (ст. 67).

На страже исполнения Закона КНР о защите персональных данных стоят не только сам обработчик данных, Государственный департамент сетевой информации и отраслевые департаменты, но и народная прокуратура, организации, определенные Государственным департаментом сетевой информации, которые имеют право в соответствии с законом обращаться в народные суды (ст. 71).

Заключение

В данном обзоре изложены основные положения трех законов Китайской Народной Республики – о кибербезопасности, о безопасности данных, о защите персональных данных, которые составляют правовой каркас «цифрового права» Китая. Его дополняют различного рода положения и временные меры, регулирующие деятельность сферы информационно-коммуникационных технологий, оборота персональных (и не только) данных, деятельность сетевых операторов, обработчиков данных, госорганов и т.д., утвержденных постановлениями Государственного совета КНР. Среди них ранее указанные: Положение о защите безопасности критической инфраструктуры 2021 г.; Временные меры по регулированию сервисов генеративного искусственного интеллекта 2023 г.; Положение об управлении рекомендациями для информационных интернет-услуг 2022 г.; Правила проверки кибербезопасности 2021 г. и др.

ГРОГОЛЬ А.Г.¹ ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В МЕДИЦИНЕ: ВОПРОСЫ ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ НАДЕЖНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И БЕЗОПАСНОСТИ МЕДИЦИНСКИХ ДАННЫХ В ЕВРОПЕЙСКОМ СОЮЗЕ (Обзор)

Аннотация. Использование искусственного интеллекта (ИИ) в сферах медицины и здравоохранения открывает как новые возможности, так и влечет новые риски, связанные с нарушением прав пациентов и созданием угрозы безопасности медицинских данных. В обзоре анализируется правовой опыт Европейского союза в сфере оказания медицинских услуг, защиты персональных данных пациентов, получение компетентного клинического решения, принятого ИИ-системой. Особое внимание акцентируется на правовых вопросах перехода на алгоритмические решения, принимаемые ИИ в сфере медицины, и необходимости пересмотра существующих механизмов обеспечения прав пациентов и их безопасности при использовании технологий искусственного интеллекта.

Ключевые слова: Европейский союз; правовое регулирование; Регламент ЕС о защите персональных данных; права пациентов; искусственный интеллект; медицинские данные; персональные данные; автоматизированные решения; право на «человеческий надзор».

GROGOL A.G. Legal regulation of the use of AI technologies in medicine: issues of ensuring the functional of reliable AI and security of medical data based on EU countries (Review)

¹Гроголь Анастасия Георгиевна, младший научный сотрудник отдела правоведения ИНИОН РАН.

Abstract. The use of artificial intelligence (AI) in the fields of medicine and healthcare opens up both new opportunities and entails new risks related to the violation of patients' rights and the creation of threats to the security of medical data. The review analyzes the legal experience of the European Union in the field of providing medical services, protecting patients' personal data, and obtaining a competent clinical decision made by an AI system. Particular attention is paid to the legal issues of the transition to algorithmic decisions made by AI in the field of medicine, and the need to review existing mechanisms for ensuring patients' rights and safety when using artificial intelligence technologies.

Keywords: European Union; legal regulation; EU Regulation on Personal Data Protection; patients' rights; artificial intelligence; medical data; personal data; automated solutions; the right to «human supervision».

Для цитирования: Гроголь А.Г. Правовое регулирование использования технологий искусственного интеллекта в медицине: вопросы обеспечения функционирования надежного искусственного интеллекта и безопасности медицинских данных в Европейском союзе (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2026. – № 1. – С. 199–212. – DOI: 10.31249/iajpravo/2026.01.13

Введение

Стремительное развитие технологий искусственного интеллекта (ИИ) претерпевает множество изменений и оказывает все большее влияние на основные сферы жизни общества, в том числе здравоохранение и медицину. Современные способы оказания медицинских услуг постепенно модернизируются, внедряя алгоритмы ИИ в диагностику, лечение и принятие клинических решений. Одновременно возрастает количество угроз, связанных с сохранением и обеспечением фундаментальных прав пациентов в условиях цифровизации медицины. Использование алгоритмических систем вполне может осложнять реализацию таких основополагающих прав, как осознанное и добровольное изъявление согласия граждан на выбор альтернативных путей диагностики и лечения. Кроме того, переход на автоматизированные клинические процессы ставит под угрозу автономность пациента, так как прозрачность принятия клинического решения ИИ не всегда поддается отслеживанию ввиду несовершенства механизмов правового и регулятивного

характера. В связи с этим возникает необходимость вводить новые гарантии защиты персональных медицинских данных (конфиденциальности информации о состоянии здоровья пациента).

В обзоре рассматриваются особые направления цифровой трансформации в различных сферах медицины и здравоохранения в условиях применения технологий ИИ в Европейском союзе: институт защиты персональных медицинских данных, дача информированного согласия на обработку данных ИИ-системами, право на отказ от участия в автоматизированных процессах, непосредственное участие пациента в принятии клинических решений, обеспечение доступа к цифровым медицинским данным и свобода выбора альтернативных способов лечения.

Правовое регулирование искусственного интеллекта в медицинской сфере в Европейском союзе

Общий регламент о защите персональных данных

Искусственный интеллект в медицине, по мнению Софии Палмиери, научного сотрудника Университета в Генте (Бельгия), является одной из наиболее обсуждаемых повесток в рамках правового поля ЕС; это подтверждает активное расширение нормативно-правовой базы и научных исследований. основополагающим правовым актом признается Общий регламент ЕС по защите данных 2016 г.¹ (далее – Регламент, GDPR). Данный Регламент С. Палмиери характеризует как многоаспектный, комплексный документ, образующий правовую основу в виде правил сбора, обработки, хранения и распространения персональных данных, принципов, подлежащих применению независимо от контекста, в котором обрабатываются персональные данные. По мнению автора, GDPR вполне применим в регулировании медицинского ИИ в случаях, когда данные системы участвуют в обработке персональных данных [3, р. 1–6].

На изучении положений GDPR также сосредоточивают свое внимание Леандро Пеккья, профессор-ассистент в области биомедицинской инженерии Уоринского университета (Великобритания), и Алессия Маккаро, доктор в области биоэтики, научный со-

¹ The Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data. – URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (дата обращения: 15.10.2025).

трудник этого же Университета, и другие исследователи. Среди наиболее важных положений Регламента авторы выделяют регулируемые этим актом права физических лиц в эпоху цифровых технологий, обязанности лиц, участвующих в обработке данных (сбор, хранение, анализ), способы и методы обеспечения соблюдения медицинскими работниками и пациентами законодательства, а также меры ответственности за нарушение установленных правовых норм. Ученые отмечают, что GDPR напрямую не регулирует применение медицинского ИИ, но содержит общие положения, указывающие на необходимость руководствоваться принципом справедливости в управлении данными при принятии доступного и понятного решения, принятого ИИ (ст. 22 GDPR) [1, р. 665–667].

Регламент о медицинском оборудовании

Анализируемый автором Регламент о медицинском оборудовании, принятый Европейским парламентом и Советом ЕС в 2017 г. (далее – MDR)¹, является специализированным правовым актом, регулирующим порядок реализации устройств медицинского назначения на территории ЕС, размещения таких товаров на рынке и процесс проведения медицинских исследований, учитывая отдельные вопросы применения ИИ в медицинском секторе. Данный правовой акт характеризует медицинский ИИ в качестве специализированного программного обеспечения, а также устанавливает строгие требования соблюдения безопасности и сохранения эффективности оказания медицинских услуг для медицинских учреждений, которые применяют технологии ИИ в своей деятельности; обеспечивает надежность данных, которые получаются в результате клинических исследований, сохраняя при этом безопасность участников исследовательских программ. MDR также предусматривает необходимость установления ответственного лица, удовлетворяющего минимальным квалификационным требованиям, которое выступает гарантом качества и безопасности медицинского оборудования на всех этапах его реализации – от производства до послепродажного контроля и мониторинга (ст. 34 Регламент о медицинском оборудовании).

¹ The Regulation on Medical Devices: сайт. – URL: <https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng> (дата обращения: 11.08.25).

**Регламент об установлении гармонизированных правил
в области искусственного интеллекта**

В своем исследовании С. Палмиери сосредоточивает особое внимание на Законе ЕС об установлении гармонизированных правил в области ИИ 2024 г.¹ (далее – Закон ЕС об ИИ). Этот Закон является ключевым в вопросах применения ИИ в различных сферах жизнедеятельности (кроме военной), в том числе в здравоохранении и медицине, состоит из 13 глав и содержит положения о безопасности и прозрачности медицинских ИИ-систем, запрещенных практиках использования ИИ-моделей, категорирование рисков, связанных с применением различных технологий ИИ, в том числе в медицинской сфере. По мнению С. Палмиери, только во взаимодействии всех трех актов – Регламент о защите персональных данных, Регламент о медицинском оборудовании и Закона ЕС об ИИ – можно говорить о создании в Евросоюзе сильной правовой основы регулирования применения ИИ в рассматриваемой области.

**Риск-ориентированный подход применительно
к медицинскому искусственному интеллекту**

Один из вопросов, рассматриваемый С. Палмиери, – применение риск-ориентированного подхода при классификации ИИ. Такой подход позволяет расширить или ограничить применение технологий ИИ, воспринимать эти технологии как определенный продукт, категорировать его в зависимости от риска, снизить сомнения пользователей, связанные с развитием, функционированием и использованием ИИ путем соблюдения требований безопасности, установленных в Законе ЕС об ИИ [3, р. 3–8].

Исходя из положений Закона ЕС об ИИ, автор выделяет три класса риска:

- 1-й класс – неприемлемые риски (unacceptable risks), ставящие под угрозу фундаментальные основы безопасности, здоровья, благополучия и основные права человека. Виды и типы ИИ-систем, попадающие под данную категорию, подробным образом изложены в разделе II ст. 5 рассматриваемого Закона.

¹ Regulation Laying down Harmonized Rules on Artificial Intelligence (the EU Artificial Intelligence Act). – URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (дата обращения: 19.10.2025).

• 2-й класс – высокая степень рисков (high risk considered). Для данной категории установлен институт двойного соотношения (double ratio). С одной стороны, данные системы и соответствующие продукты должны отвечать требованиям безопасности, которые в законе подробно не описаны; достаточно лишь указать, что конечная цель использования таких технологий – соблюдение безопасности. С другой стороны, ИИ-системы с высокой степенью риска помимо вышеуказанного требования должны предусматривать определенные меры предосторожности, которые уже регламентированы и перечислены в ст. 6.2 указанного Закона.

• 3-й класс – ограниченные и минимальные риски (limited and minimal risks) применяются для поддержания баланса между безопасностью и инновациями. Ограниченными, согласно рассматриваемого Закона, считаются ИИ-системы, генерирующие ложные сведения (deep fakes) через аудио- или видеоконтент, а минимальными рисками принято считать ИИ-системы вышеупомянутых категорий, которые не имеют повышенную степень опасности [4, p. 9].

Углубленный анализ Закона ЕС об ИИ, регулирующего вопросы проведения оценок рисков и уязвимостей ИИ-систем, постмаркетингового надзора, внедрения принципов обеспечения безопасности, а также создания надежных и прозрачных ИИ-систем предприняли также авторы статьи «Нормативная экосистема ЕС для этичного искусственного интеллекта» [2] – Вайос Болгурос, доктор в области кибербезопасности из Пирейского университета (Италия), Апостолис Заррас, профессор кафедры цифровых систем этого же университета, Кристиан Лека, профессор факультета науки Университета Лучиана Благи в Сибиу (Румыния). С их точки зрения, именно критерий прозрачности выполняет главную роль, так как обязывает ИИ-разработчиков детально прописывать системные ограничения и возможные риски, предоставлять их в общедоступном формате, чтобы пользователи могли самостоятельно прийти к решению о согласии применения технологий ИИ в личных медицинских целях. Однако, несмотря на широкую сферу действия Закона ЕС об ИИ, авторы сходятся во мнении, что данный правовой акт не уделяет существенного внимания функциональным требованиям к операционным особенностям ИИ-систем [2, p. 5067–5068].

Право пациента на информированное согласие и отказ в использовании медицинских и персональных данных при работе с технологиями искусственного интеллекта

В своем исследовании ученые из Туринского университета (Италия) – Маринелла Кваранта, профессор факультета компьютерных наук, Марко Гроссо, доктор наук в области общественного здравоохранения и Илария Анжела Амантеа, отмечая сложность в объяснении работы ИИ-систем пациентам, ставят под вопрос осознанность получения согласия на анализ медицинских данных с использованием ИИ-систем. По их мнению, в настоящее время большинство технологий ИИ не отвечают критерию прозрачности, доступности, понятности, так как алгоритмы вычисления и обработки информации многих ИИ-систем крайне трудно отследить и тем более объяснить лицам (пользователям), не владеющим специализированным набором знаний. Такая проблема ставит под угрозу индивидуальные и коллективные права пользователей, и если результаты ИИ-операций недоступны для понимания простым гражданам, то риск возникновения более сложных и серьезных юридических претензий будет возрастать. Именно поэтому в работе с медицинскими данными пациентов с применением ИИ-технологий обработки информации крайне важно предоставить пользователям понятную и доступную информацию о функционально-операционных деталях используемой ИИ-технологии, чтобы дать пациенту возможность самостоятельно принять решение об информированном согласии или отказе от ИИ-услуги. Авторы подчеркивают, что в современном правовом поле отсутствует прямо выраженное и закрепленное право на отказ от применения ИИ-технологии, в том числе в сфере медицины и здравоохранения. Именно поэтому необходима правовая конкретизация применения медицинского ИИ на уровне национального законодательства [4, р. 275–276].

На ограниченные условия участия пациента в выборе и отказе от применения технологий ИИ также указывает С. Палмиери. Она считает, что институт раскрытия информации об использовании той или иной технологии особенно со все большим переходом на автоматизированные решения является преимуществом для пациентов, которым не была предоставлена возможность выбрать соответствующую ИИ-систему в обработке медицинских данных или принятии клинических решений, также как и отказаться от данной технологии. Содержание ст. 13–15 GDPR позволяет

С. Палмиери утверждать о существовании косвенного правового механизма, содержащего требование раскрытия информации о существовании автоматизированного процесса принятия решений. Несмотря на споры в научной литературе, автор убеждена, что применение института раскрытия информации в юридической практике оказало бы значительное влияние на регулирование медицинского ИИ без необходимости применения положений специального Закона ЕС об ИИ [3, р. 4–9].

Право на «человеческий надзор» (right to human oversight) при принятии решений на основе ИИ-систем

В ходе изучения требований безопасности по использованию и эксплуатации ИИ-систем В. Болгурос, А. Заррас и К. Лека обратили внимание на многоуровневый, комплексный подход в их регулировании. По мнению ученых, рассматриваемые ИИ-платформы могут быть эффективными лишь в некоторых областях. При коллективном применении таких платформ, как правило, создается полноценная целостная система безопасности, учитывающая технические, этические и ориентированные на пользователя нюансы. Так, устранение выявленных пробелов в данной цепочке через повышение их функциональной совместимости, систематическое внедрение принципов «человеческого надзора» и справедливости способствуют этическому и безопасному процессу применения медицинских систем на основе технологий ИИ. По мнению авторов, такой комплексный механизм обеспечит защиту медицинских пользователей, повысит доверие и впоследствии станет новой стратегией-ориентиром для других стран [2, р. 5069–5070].

Внедрение механизма «человеческого надзора» за развитием технологий ИИ в медицинском секторе имеет, по мнению названных авторов, множество преимуществ, так как сохраняется приоритетная роль человеческого суждения в программах с применением ИИ, особенно в ситуациях, связанных с принятием наиболее важных медицинских решений (постановка диагноза, обработка медицинских анализов, выбор способа лечения и т.д.). Такой инструмент позволяет снизить риск как ошибочного автоматизированного решения, так и человеческого фактора (врачебной ошибки) [2, р. 5067–5068].

Тема сохранения ключевой роли человека в автоматизированном процессе в медицинской деятельности рассматривается в статье «Европейская ответственность за качеством продукции для

систем поддержки клинических решений на основе искусственно-го интеллекта» [5] Яна Штальдуинена, исследователя вопросов медицинской ответственности в сфере применения технологий ИИ в Институте частного права Лейденского университета (Нидерланды). Автор полагает, что врач является своего рода «переводчиком» автоматизированных медицинских решений ИИ, и именно поэтому он должен нести юридическую ответственность независимо от объема применения ИИ-технологии в данном решении. Такая позиция позволяет ему сделать вывод о высокой доли человеческого фактора в эпоху автоматизированных решений.

Я. Штальдуинен подробно анализирует концепцию внедрения систем поддержки принятия клинических решений (Clinic Decision Support System) (далее – CDSS), разработанную Робертом Хейвордом, сотрудником Центра доказательной медицины при Оксфордском университете и являющуюся передовым достижением в области машинного обучения. В таких системах программируются правила и механизмы вывода наиболее точных решений для клинической диагностики на основе ранее встроенных кейсов, опыта и т.п. Это позволяет более гибко решать проблему возможной врачебной ошибки. По мнению автора, вспомогательная роль алгоритмов и технологий ИИ делает CDSS наиболее подходящей автоматизированной системой в медицинской сфере. В то же время нельзя отрицать недостаток критерия прозрачности в CDSS-системах на базе ИИ. В случаях сбоя или какой-либо непредвиденной ошибки в виде некорректной рекомендации о клиническом решении, препарата, ошибка ИИ-системы может отразиться на ответственности доктора. В отношении CDSS указанные риски являются наиболее серьезными, так как реализуются через посредника (медицинского работника) и могут охватывать более широкий спектр негативного воздействия в системе здравоохранения. На данном основании Я. Штальдуинен предлагает учитывать такие ошибки, как халатность медицинского работника, который, получив сомнительный результат или рекомендацию CDSS, не принял во внимание и не учел негативные последствия такого клинического решения. Однако для этой новой формы ответственности, возникающей на основании некорректного функционирования CDSS, по мнению автора, необходимо принять специализированный правовой акт. На данный момент реальность такова, что клиницисты далеко не всегда несут полную юридическую ответственность за используемые ими технологии и алгоритмические устройства [5, p. 15–18].

По мере того, как CDSS находит все большее распространение на европейском пространстве, стандарты халатности в правовом регулировании будут также расширяться. Несмотря на первоначальную выгоду в использовании CDSS, Я. Штальдуинен приходит к выводу о том, что внедрение данных систем на основе ИИ может лишить потенциально пострадавшую сторону (пациента) средств правовой защиты [5, p. 15–18].

М. Кваранта, Марко Гроссо и Илария Анжела Амантеа в дополнении позиции Я. Штальдуинена резюмируют, что автоматизация медицинских решений на базе ИИ неминуемо приведет к двум крайне опасным последствиям: потенциальной потере врачебного контроля и снижению качества персонализированного подхода. В связи с этим, подчеркивают исследователи, важно сохранять баланс между машинным и человеческим вмешательством в медицинские операции [4, p. 276–278].

Механизмы обеспечения конфиденциальности и защиты медицинских (персональных) данных в европейском законодательстве

Европейский союз и страны – члены ЕС в парадигме своего развития продвинулись далеко от «индустриальной экономики» (industrial economy) к «экономике знаний» (knowledge economy), что, по мнению Л. Пеккья и А. Маккаро, было вызвано процессами цифровизации и массовым распространением технологий ИИ. Данные в современных реалиях стали новой главной ценностью в медицине. Однако, чтобы необработанные данные (raw data) приобрели набор ценностных характеристик, необходимо создание определенных механизмов, дабы эти данные превратились в интеллектуальный капитал, инновации, информацию и стали стимулом разработки новых технологий. В связи с этим авторы справедливо утверждают, что в Общем регламенте (GDPR) недостаточно принципов, установленных для полноценного эффективного обеспечения защиты данных, особенно персонализированных данных, касающихся отдельных пользователей, в том числе и в медицинском секторе. Исходя из этих положений, Л. Пеккья и А. Маккаро приводят подробный анализ системы европейских данных о состоянии здоровья (European Health Data Space, EHDS). Пандемия COVID-19 позволила повысить осведомленность государств во взаимосвязи и взаимовлиянии между поддержанием устойчивых механизмов обмена медицинскими данными и конкурентоспособ-

ностью, о лидерстве в сфере медицинского сектора (проведения медицинских исследований, производства лекарственных препаратов и др.). В 2020 г. распространившаяся эпидемия с точки зрения прогрессивного роста послужила позитивным стимулом к активному внедрению цифровых технологий в рамках создания единой платформы-пространства медицинских данных (EHDS). Данная экосистема для управления медицинскими данными и их обмена оказала благоприятный эффект на качество результатов медицинского обслуживания, стимулирование медицинских исследований, способствовала выработке стандартизированного и безопасного подхода в обмене медицинскими данными среди государств – участников ЕС. Л. Пеккья и А. Маккаро уточняют, что основным элементом системы EHDS является различие между первичным использованием (primary use), заключающемся в непосредственном предоставлении клинической помощи (clinical care), и вторичным использованием (secondary use), в форме различных исследований, разработки политики и т.д. [1, p. 665–668].

В рамках первичного использования была специально создана добровольная платформа-инфраструктура «MyHealth@EU», которая функционирует на наднациональном уровне и представляет собой эффективный банк медицинских данных, позволяющий упростить доступ среди всех стран ЕС. Данная система также позволяет обеспечить требование GDPR о безопасном обмене информацией для целей первичного использования.

В рамках вторичного использования были установлены общие правила и стандарты в отношении порядка предоставления разрешений и гарантий для исследовательских и политических целей. По мнению авторов, такой дуальный подход раскрывает потенциал экономики данных (data economy protection) в медицинском секторе и сфере здравоохранения, преимущественно посредством разработки политики и нормотворческой деятельности, реализации политики, основанной на фактических данных [ibid.].

Таким образом, авторы сходятся во мнении и убеждены, что платформа EHDS является основным фундаментом в продвижении Европейской стратегии здравоохранения, принятой Еврокомиссией 30 ноября 2022 г. (The EU Global Health Strategy to improve global health security and delivery better health for all)¹, целью кото-

¹ The EU Global Health Strategy to Improve Global Health Security and Delivery Better Health for All. – URL: <https://ec.europa.eu/commission/presscorner/detail/en/ip22153> (дата обращения: 19.08.2025).

рой является преодоление существующей фрагментации правовых норм и создание эффективной многоуровневой системы управления оборотом медицинских и персонализированных медицинских данных. Авторы подчеркивают, что стабилизация и стимуляция использования данной платформы увеличивают быстроту реагирования в случае форс-мажора или чрезвычайной ситуации, как это произошло в период пандемии COVID-19. Однако следует учитывать, что даже EHDS имеет ряд свойственных ограничений, в частности в отношении трансграничной защиты конфиденциальности данных в форме информации, функциональной совместимости и стандартизации данных (data interoperability and standardization). Например, ограничения могут возникнуть в различных системах и практиках лиц, предоставляющих медицинские услуги. Сложности заключаются в беспрепятственном обмене и использовании медицинских данных ввиду различий национального законодательства [1, p. 669].

Функциональные требования законодательства Европейского союза к эффективному обращению с медицинскими данными при использовании технологий искусственного интеллекта и иных алгоритмических технологий

Рассмотренные ранее регуляционные требования, а также нормы в отношении безопасности данных не могут в полной мере обеспечить оборот медицинских данных. С точки зрения греческих ученых – В. Болгуроса, А. Зарраса и К. Леки, занимающихся изучением вопросов этического использования технологий ИИ, такую дуальную систему регулирования следовало бы дополнить функциональными требованиями, так как значительные институциональные различия препятствуют нормальному использованию систем обработки медицинских данных на базе ИИ.

В. Болгурос и А. Заррас и К. Лека предлагают выявить и дополнить набор существующих функциональных требований к ИИ-системам, содержащих этические принципы и операционную надежность. Основопологающим критерием-требованием здесь может выступать оценка соответствия (conformity assessment requirement, CAR) этическим и функциональным параметрам. Согласно ст. 43–51 разд. 5 гл. III Закона ЕС об ИИ, поставщики технологий с использованием ИИ обязаны соблюдать CAR для систем ИИ с высоким уровнем риска и получить сертификат соответствия, выданный уполномоченным органом на срок не более пяти

лет. При несоответствии требованиям, установленным в разд. 2 Закона об ИИ, ранее полученный сертификат соответствия может быть приостановлен до устранения нарушений. Раздел 2 Закона об ИИ предусматривает, что ИИ-системы с высокой степенью риска должны проходить обязательную проверку на соответствие требованиям, установленным в технической документации, процедурам управления качеством (quality management procedures), стратегиям послепродажного маркетинга (post-market monitoring strategies), при этом данная процедура проходит как на этапе внедрения ИИ-технологии, так и в рамках ее последующего эксплуатации. Такой подход позволяет свести к минимуму потенциальные ошибки в функционировании ИИ-систем и моделей, что повышает эффективность предоставляемых медицинских услуг. Регламент GDPR дополняет положения Закона ЕС об ИИ и в ст. 32 содержит положения о безопасности и устойчивости ИИ, о необходимости интеграции таких механизмов на протяжении всего жизненного цикла ИИ-системы. По мнению авторов, симбиоз данных требований способствует выработке упреждающих мер против киберугроз, гарантирует надежность и эффективность ИИ-системы при принятии клинических решений [2, р. 5069–580].

Заключение

Представленный обзор показывает, что развитие и внедрение технологий ИИ в медицинской сфере позволяет открыть качественно новые подходы в диагностике заболеваний, принятии клинических решений, разграничении юридической ответственности за медицинские ошибки, сохранении конфиденциальности медицинских и персональных данных. Именно поэтому крайне важно, чтобы трансформация традиционной модели оказания медицинских услуг, основанная на ИИ-системах и алгоритмических технологиях, подлежала детальной правовой оценке, так как обеспечение баланса между инновациями и этическими нормами позволит грамотно и качественно внедрить такие достижения без потерь и угроз. Европейские регламенты – GDPR, MDR, Закон об ИИ – демонстрируют комплексный подход в регулировании ИИ-систем и медицинских данных, обеспечивая прозрачность, безопасность и соблюдение общепринятых норм. Ключевыми приоритетами развития правового регулирования в ЕС сегодня стали вопросы обеспечения информированного согласия пациента на применение ИИ-систем при предоставлении медицинских ус-

луг, института «человеческого надзора», защиты персональных медицинских данных и расширения требований к медицинским ИИ-системам.

Список литературы

1. Artificial Intelligence, Data Protection and Medical Device Regulations: Squaring the Circle with a Historical Perspective in Europe / L. Pecchia, A. Macarro, M.A.G. Marrese, F. Folkvord, G. Fico // *Health and Technology*. – 2024. – Vol. 14. – P. 663–670. – URL: <https://link.springer.com/article/10.1007/s12553-024-00789-9> (дата обращения: 22.10.2025).
2. EU Regulatory Ecosystem for Ethical AI / V. Bolgouras, A. Zarra, C. Leka, I. Stylianou, A. Farao, C. Xenakis // *AI and Ethics*. – 2025. – Vol. 5. – P. 5063–5080. – URL: <https://link.springer.com/article/10.1007/s43681-025-00370-6> (дата обращения: 22.10.2025).
3. Palmieri S. The Renewed EU Legal Framework for Medical AI // *European Journal of Law and Technology*. – 2024. – Vol. 15, N 3. – P. 1–23. – URL: <https://ejlt.org/index.php/ejlt/article/view/957> (дата обращения: 24.10.2025).
4. Quaranta M., Amantea I.A., Grosso M. Obligation for AI Systems in Healthcare: Prepare for Trouble and Make it Double? // *The Review of Socionetwork Strategies*. – 2023. – Vol. 17. – P. 1–20. – URL: <https://link.springer.com/article/10.1007/s12626-023-00145-z> (дата обращения: 24.10.2025).
5. Staalduin J.H. van (Jan) European Product Liability for AI Based Clinical Decision Support Systems // *Digital Governance*. – 2025. – Vol. 39. – P. 15–40. – URL: https://link.springer.com/chapter/10.1007/978-3-031-47834-2_8 (дата обращения: 24.10.2025).

СКУРКО Е.В.¹ РЕЦЕНЗИЯ НА КНИГУ: ЗАКОНОДАТЕЛЬСТВО О БЕДСТВИЯХ: ПОДХОДЫ К УПРАВЛЕНИЮ И ИМПЛЕМЕНТАЦИЯ / РЕД. ЯНЬ ЦУЙ и РАДЖИБ ШОУ
SKURKO E.V. Book review: Disaster Law: Implications to Governance and Implementation / ed. Yan Cui, Rajib Shaw. – Singapore: Springer, 2025. – 331 p.

Ключевые слова: законодательство о бедствиях; право катастроф; сравнительное правоведение; управление рисками.

Keywords: disaster law; comparative law; risk management.

Для цитирования: Скурко Е.В. [Рецензия] // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2026. – № 1. – С. 213–222. – Рец. на кн.: Disaster Law: Implications to Governance and Implementation / ed. Yan Cui, Rajib Shaw. – Singapore: Springer, 2025. – 331 p. – DOI: 10.31249/iajpravo/2026.01.14

В 2025 г. в издательстве Шпрингер (Springer) вышла коллективная монография «Законодательство о бедствиях: подходы к управлению и имплементация». Авторы исследования – ученые-политологи и праведы из Бангладеш, Великобритании, Индии, Индонезии, Китая, Малайзии, Пакистана, Сингапура, Таиланда, Турции, Шри-Ланки, Японии.

В предисловии к работе ее редакторы – Янь Цуй, доцент юридического факультета Университета политических наук и права в Ганьсу (Китай) (Gansu University of Political Science and Law), и Раджиб Шоу, профессор Высшей школы медиа и управления Университета Кейо в Фудзисаве, Канагава (Япония) (Graduate

¹ Скурко Елена Вячеславовна, старший научный сотрудник отдела правоведения ИНИОН РАН, кандидат юридических наук.

School of Media and Governance Keio University Fujisawa, Kanagawa, Japan), отмечают главную особенность этой коллективной монографии – «погружение читателя в сложную сеть законов, нормативных правовых актов и правовой политики, лежащих в основе борьбы со стихийными и антропогенными бедствиями в различных странах мира».

Описание многогранной природы «права катастроф», законодательства о стихийных и антропогенных бедствиях, а также его глубокого влияния на национальное и международное право и управление рассматривается как задача авторского коллектива. Изучая данные и исследования со всего мира, авторы выявляют лучшие практики, а также пробелы, предлагают инновационные решения для усиления правового и институционального реагирования в ситуациях катастроф различной природы и происхождения (р. V).

Законодательство о стихийных и антропогенных бедствиях, определяемое как *право катастроф*, по сути образует правовую основу управления рисками в условиях чрезвычайных, природных и техногенных катастроф в каждой стране. Оно предоставляет правительству инструментарий для принятия мер до, во время и после стихийного бедствия или техногенных катастроф, обеспечивает определенный уровень руководства, полномочий и компетенций для всех вовлеченных сторон – национальных правительств, местных органов власти, гражданского общества и, что более важно, граждан; предусматривает определенные обязательства и ответственность за их действия до и во время стихийных или техногенных бедствий.

В последние годы, подчеркивают авторы, во многих странах были разработаны новые законодательные и иные нормативные правовые акты о стихийных бедствиях и катастрофах, чрезвычайных ситуациях, а также внесены изменения и дополнения в действующие законы в целях их более эффективного применения. Данная книга представляет комплексное междисциплинарное исследование не только законодательства об управлении и правореализации в условиях катастроф, но и предлагает конкретные политико-правовые и практические шаги и меры по совершенствованию применения законодательства о ликвидации последствий стихийных бедствий и чрезвычайных ситуаций, в том числе на основании «лучших практик» (р. VII).

В этой книге, как отмечается во введении, рассматриваются различные аспекты развития законодательства о стихийных бедствиях и применения, представлены обзоры и новые данные, осно-

ванные на тематических исследованиях по всему миру, в том числе и на междисциплинарных. Кроме того, ее авторы предлагают конкретные стратегии и меры для повышения эффективности реализации законодательства о стихийных бедствиях в целях обеспечения устойчивости населения и местных органов власти.

Законодательство о стихийных бедствиях лежит в основе управления их рисками. Правовая база не только предоставляет правительству инструменты для принятия мер до, во время и после стихийных бедствий, но и помогает в процессе восстановления. Законодательные меры, описанные в монографии, содержат определенные рекомендации для различных заинтересованных сторон, таких как национальные правительства, местные органы власти, гражданское общество и рядовые граждане.

Первую главу работы авторы позиционируют как обзорную. В ней раскрываются основные понятия, используемые этой новой «отраслью» права, дается общая характеристика «права катастроф» и его сложившемуся международно-правовому массиву: история, потенциал и вызовы, которые оно призвано нейтрализовать.

Катастрофы, вызванные природными или иными опасностями, представляют серьезную угрозу для жизни людей, имущества и окружающей среды. Сложность управления такими чрезвычайными ситуациями, как утверждают авторы, требует наличия надежной правовой базы для обеспечения готовности, реагирования, восстановления и смягчения последствий.

Необходимо еще раз подчеркнуть, что «право катастроф», помимо законов о стихийных и антропогенных бедствиях, включает в себя широкий спектр нормативных правовых актов, актов правовой политики и др., направленных на минимизацию последствий стихийных бедствий и содействие эффективному управлению в случае их возникновения. То есть, *право катастроф* – это специализированная область юридической практики и научных знаний, которая занимается подготовкой к стихийным и иным бедствиям, реагированием на них, восстановлением и смягчением их последствий.

Следует согласиться с авторами в том, что формирование правовых рамок, связанных с ликвидацией последствий стихийных и иных бедствий, важно для обеспечения эффективных и скоординированных действий до, в период и после таких событий. Эволюция «права катастроф» была обусловлена растущим признанием необходимости в структурированных и всеобъемлющих подходах к борьбе со стихийными и иными бедствиями. Исторически

сложилось, что меры реагирования на стихийные и иного рода бедствия и катастрофы были в основном реактивными, т.е. специальные меры принимались уже после катастрофы. Со временем стало ясно, что для смягчения последствий стихийных бедствий и техногенных катастроф, иных чрезвычайных ситуаций, содействия эффективному реагированию и обеспечения устойчивого восстановления необходимы активные правовые и политические меры (р. 2).

Особое внимание в работе уделяется *роли ООН в обеспечении устойчивого развития и устойчивости к стихийным бедствиям и иным катастрофам*. В дополнение к национальным законам и политике, международные структуры играют важную роль в формировании законодательства о бедствиях. Такой акт, как Сендайская рамочная программа по снижению риска катастроф 2015 г. (Sendai Framework for Disaster Risk Reduction), а также принципы международного гуманитарного права обеспечивают руководящие начала и стандарты для эффективной борьбы с бедствиями и преодоления катастроф. Этот и другие акты, программы и принципы подчеркивают важность обеспечения готовности, участия обществ и необходимость комплексного подхода к снижению риска бедствий, учитывающего все факторы риска (ibid.).

Согласно международным документам Управления ООН по снижению риска бедствий (UN Office for Disaster Risk Reduction (UNDRR)), законодательство о бедствиях – это совокупность норм и принципов, регулирующих подготовку к бедствиям, реагирование на них и восстановление после них. Оно охватывает широкий спектр правовых рамок, включая национальное законодательство, международные договоры, нормативные акты и акты государственной политики, направленные на управление рисками бедствий и повышение устойчивости к ним. «Право катастроф» призвано обеспечить структурированный и систематический подход к решению правовых вопросов управления в борьбе с бедствиями, обеспечивая эффективную координацию, защиту прав человека и оказание гуманитарной помощи.

Хиогская рамочная программа действий (далее – ХРПД) на 2005–2015 гг. стала ключевой международной инициативой, направленной на существенное сокращение потерь от стихийных бедствий к 2015 г. Будучи принята на Всемирной конференции по уменьшению опасности бедствий в Кобе, Хиого, Япония, ХРПД представила всеобъемлющий план действий по снижению риска бедствий во всем мире. В ХРПД были определены пять приоритетов для государств в условиях бедствий: 1) обеспечение снижения

риска бедствий как национальный и местный приоритет с прочной институциональной основой для реализации; 2) выявление, оценка и отслеживание рисков бедствий и повышение эффективности раннего предупреждения; 3) использование знаний, инноваций и образования для создания культуры безопасности и жизнестойкости на всех уровнях; 4) снижение основных факторов риска; 5) повышение готовности к стихийным бедствиям для эффективного реагирования на всех уровнях.

Исходя из подходов ХРПД, во многих странах мира принято законодательство об учреждении национальных агентств или органов по борьбе с катастрофами, поставлена задача координировать усилия по снижению риска бедствий в различных секторах и на различных уровнях государственного управления. В рамках ХРПД были предложены подходы и модели систем оценки рисков и раннего предупреждения, на основании которых – на национальном уровне во многих странах мира – были разработаны законы и иные нормативные акты, предписывающие проводить регулярные оценки рисков и уязвимости, объединяющие научные и местные знания для разработки стратегий снижения риска бедствий на государственном и местном уровнях.

Учитывая, кроме того, что системы раннего оповещения имеют решающее значение для своевременного и эффективного реагирования на стихийные бедствия и техногенные катастрофы, в национальном законодательстве были закреплены соответствующие правовые положения, гарантирующие их разработку и поддержание функционирования. По общему правилу, государства обязуются, что такие системы должны быть доступны для всех, обеспечивая то, чтобы предупреждения доходили и до наиболее уязвимых граждан и сообществ в стране.

Этот приоритет был воплощен в национальном законодательстве, в части, обязывающей проводить кампании по информированию общественности о готовности к стихийным бедствиям и снижению риска. В ряде стран информация о снижении риска бедствий была включена в школьные программы и учебные планы, а программы обучения местных жителей получили юридическую поддержку для повышения осведомленности общественности и готовности к стихийным бедствиям. Существенное внимание в международно-правовом регулировании, в том числе в рамках ХРПД, уделяется проблеме устранения факторов риска, лежащих в основе появления ситуаций бедствий, таких как неэффективное

планирование землепользования, ухудшение состояния окружающей среды и др. (р. 4).

На основе ХРПД была принята Сендайская рамочная программа по снижению риска бедствий на 2015–2030 гг., предусматривающая следующие руководящие принципы: 1) понимание риска бедствий; 2) усиление средств управления рисками бедствий; 3) инвестирование в снижение риска бедствий; 4) повышение готовности к бедствиям для эффективного реагирования.

В своей монографии Янь Цуй и Раджиб Шоу выделяют и рассматривают, исходя из преобладающих основных характерных признаков, нормативные правовые акты, содержащие положения, предусматривающие: механизмы межведомственной координации и координации между различными правительственными и неправительственными учреждениями для обеспечения единого реагирования; распределение ресурсов; юридические полномочия и ответственность в условиях чрезвычайной ситуации; оценку рисков и планирование; строительные нормы и правила, планирование землепользования; информирование и просвещение общественности; планы и стратегии восстановления после бедствий; финансовую помощь и компенсацию жертвам и пострадавшим в бедствиях; психосоциальную поддержку; международное сотрудничество: заключение межгосударственных соглашений о взаимопомощи; гуманитарную помощь и мероприятия по оказанию чрезвычайной помощи.

В монографии также раскрывается опыт правового реагирования в ситуациях бедствий, действие права катастроф в различных регионах и странах мира, в том числе: законодательство по управлению в условиях катастроф ЕС (гл. 2); соглашения по управлению в условиях катастроф АСЕАН (гл. 3); особенности законодательства в области стихийных бедствий и чрезвычайных ситуаций в ЕС, США, Китае, Японии, Индии, Пакистане, Турции, Индонезии, Филиппинах, Австралии и др. (гл. 4–19).

Европейский союз. Анализируя правовые документы ЕС, Чжиин Чжао (Zhiying Zhao) и Раджиб Шоу отмечают, что в ЕС принимались различные меры по борьбе со стихийными и антропогенными бедствиями, которые позволяли скоординировать эту деятельность и снизить риски катастроф, смягчить их последствия, провести восстановительные мероприятия. Особенное внимание законодательство ЕС уделяет стратегиям сокращения и предотвращения катастроф, поскольку эти действия помогают умень-

шить последствия, связанные с неблагоприятными природными и техногенными катастрофами (р. 16).

Подходы ЕС в сфере борьбы с бедствиями основаны на обязательстве ЕС предоставлять помощь, защиту и чрезвычайную помощь государствам-членам, что подкрепляется правовыми положениями, содержащимися в Лиссабонском договоре, Сендайской рамочной программе по снижению риска бедствий, а также национальным законодательством стран – членов ЕС. Законодательство ЕС о борьбе с бедствиями направлено на повышение устойчивости существующих экосистем, инфраструктуры, экономики и общества в целом для смягчения их последствий – неблагоприятных событий для жизни человека и окружающей среды (р. 16).

Соединенные Штаты Америки. США, как пишут Яфан Вэнь (Yafang Wen) и Раджиб Шоу, являются одной из наиболее подверженных стихийным бедствиям стран в мире из-за своей обширной территории и сложной и разнообразной окружающей среды. По сравнению с другими странами мира, законодательство о бедствиях в США имеет ряд отличительных особенностей, в том числе длинную историю, быстрый процесс разработки и обновления нормативных актов и разнообразие аспектов их содержания. Еще в 1803 г. Конгресс принял первый отдельный закон о ликвидации последствий бедствий. С 1950-х по 1970-е годы законодательство о бедствиях в США достигло пика своего развития, и Закон Стаффорда 1988 г. охватывает множество федеральных мер по ликвидации последствий бедствий; за прогнозирование и восстановление после стихийных бедствий в США отвечает специальное ведомство и т.п. С этой точки зрения, по мнению авторов, США можно признать в ряду лидеров в области развития «права катастроф» (р. 69).

Китайская Народная Республика. Опыт КНР, как указывают Янь Цуй, Яфан Вэнь, Инань Гао (Yinan Gao) и Раджиб Шоу, свидетельствует о том, что законодательство о ликвидации последствий стихийных и антропогенных бедствий содержит государственные гарантии борьбы с катастрофами и имеет огромное значение для поддержания социальной стабильности и защиты жизни и имущества людей.

Китай, страна с обширной территорией и разнообразным климатом, традиционно сталкивается с угрозой многочисленных бедствий. Вместе с тем, как указывают авторы, в КНР в правовых вопросах борьбы с бедствиями сохраняются некоторые проблемы, в том числе отсутствие фундаментального закона о бедствиях, не-

достаточные капиталовложения, отсутствие подробных правовых норм для общественных организаций и несовершенная система страхования от стихийных бедствий (р. 89).

Особенный интерес представляет опыт законодательства Гонконга и Макао о стихийных и антропогенных бедствиях, который, по мнению исследователей, демонстрирует хорошую нормативную структурированность, высокий уровень межведомственного сотрудничества и координации, вовлечение общественности и технологической интеграции. Эти регионы, по мнению специалистов, дают ценные уроки для совершенствования практики борьбы со стихийными бедствиями – для многих стран мира.

Япония. Как указывают Руйян Чжао (Ruiyan Zhao), Томо Каване (Томо Kawane) и Раджиб Шоу, из Высшей школы медиа и управления Университета Кейо (Graduate School of Media and Governance, Keio University), в Японии в 1961 г. был принят Закон о бедствиях (Основной закон о борьбе с бедствиями) (Disaster Law (Basic Act on Disaster Management)) – как реакция ее законодательных органов на тайфун «Исеван» (р. 55).

С этих пор развитие законодательства о бедствиях в Японии и его имплементация протекали под влиянием трех известных стихийных бедствий – уже упомянутого тайфуна «Исеван», землетрясения Ханшин-Авадзи и масштабного землетрясения в Восточной Японии. Особенно после Восточно-Японского землетрясения 2011 г. в стране постоянно совершенствовалась государственная политика и законодательство в отношении стихийных бедствий.

Авторы подчеркивают динамичную взаимосвязь между стратегиями реагирования Японии на стихийные бедствия и реальными вызовами, порожденными неистовством природы страны, что получало отражение в многолетних усилиях по повышению устойчивости и адаптации политики государства при противодействии этому (*ibid.*).

Ключевые компоненты японского законодательства о бедствиях связаны с финансированием, разграничением полномочий и юрисдикции, а также координацией между различными уровнями государственного управления – учреждениями и структурами, действующими в сфере борьбы с бедствиями (р. 58).

Современные практические проблемы развития и реализации законодательства о катастрофах в стране связаны с местными особенностями, сложностями с распределением ресурсов и необходимостью эффективного участия общественности. Решение этих проблем требует сочетания политики, ресурсов и усилий по вовле-

чению общественности для обеспечения того, чтобы все регионы и граждане были надлежащим образом подготовлены к стихийным бедствиям и могли эффективно реагировать на них (р. 65).

Турция, как пишет Бурджак Басбуг (Burscak Basbug), неоднократно переживавшая землетрясения, начиная с землетрясения в Эрзинджане в 1939 и в 1992 гг., в Мраморном море в августе 1999 г. и в Кахраманмараше 6 февраля 2023 г., извлекая уроки из крупных стихийных бедствий, постоянно совершенствовала свое законодательство. После каждого случая в него вносились дополнения и изменения, в соответствии с потребностями общества и политикой правительства. Например, обязательное страхование от землетрясений, которое было введено после разрушительного землетрясения в Мраморном море 1999 г., что оценено как одно из важнейших событий в нормативно-правовом развитии страхования в стране. Как отмечает Б. Басбуг, в Турции принимаются очень значимые меры в нормативном регулировании вопросов, связанных с разработкой строительных норм, совершенствованием муниципального управления и финансовых механизмов в этой области (р. 121).

Автор подчеркивает, что для всех без исключения стран важно увязывать правовую политику со стратегиями и действиями по снижению риска бедствий и противодействию им. Создание мощного правового потенциала в сфере борьбы с катастрофами, помимо прочего, способствует достижению целей устойчивого развития, провозглашенными ООН, решению задач Сендайской рамочной программы по снижению риска бедствий 2015–2030 (SFDRR) на местном, национальном и глобальном уровнях.

К сожалению, в большинстве случаев усилий по обеспечению готовности, предотвращению и смягчению последствий катастроф оказывается недостаточно, и справиться с последствиями бедствий сложно. Турция часто подвергается природным и техногенным опасностям. Основной геоопасностью для Турции является землетрясение, которое, хотя и происходит относительно редко, приводит к высокой степени тяжести своих последствий для населения и страны в целом. В последние годы в Турции также фиксировались гидрологические и метеорологические опасности, такие как внезапные наводнения и сильные штормы с тяжелыми последствиями. Это требует различных планов по смягчению последствий катастроф, в том числе на нормативном правовом уровне. Поскольку количество событий, виды опасностей и размер ущерба варьируются от года к году, от места к месту, возникает необхо-

димось в надежной комплексной правовой защите, которая могла бы предотвратить хаотические последствия для выживших в результате стихийных бедствий, а также для местных и национальных органов власти. Надежное законодательство, как пишет Б. Басбуг, должно охватывать потребности общества и способности государства отвечать им. Регулирование землепользования, строительства зданий, инвестиции в сельское хозяйство, инфраструктуру, страхование, связь, образование, транспорт, снабжение и логистику, социальную поддержку и многие другие секторы, которые прямо или косвенно затрагиваются, если происходят стихийные бедствия и техногенные катастрофы, находятся в центре внимания законодателей страны (р. 131).

Таким образом, монография «Законодательство о бедствиях: подходы к управлению и имплементация» – актуальная работа как для правоведов, так и для специалистов-практиков в сфере стихийных бедствий и катастроф, чрезвычайных ситуаций.

В целом эта книга представляет собой ценный справочный материал, где каждая глава написана учеными с экспертными знаниями права катастроф, которые делятся с читателем своим профессиональным опытом. В работе в основном дается анализ стран Азиатско-Тихоокеанского региона.

Книга предназначена для широкого круга читателей, включая политиков, практикующих юристов, ученых и студентов правоведов, а также специалистов в сфере государственного управления, экологии, чрезвычайных ситуаций.

Социальные и гуманитарные науки
Отечественная и зарубежная литература
Информационно-аналитический журнал

Серия 4

**ГОСУДАРСТВО
И
ПРАВО**

2026 – № 1

Техническое редактирование
и компьютерная верстка В.Б. Сумерова
Корректор Д.Г. Валикова

Подписано к печати 14.12.2025

Формат 60×84/16
Усл. печ. л. 14,0
Тираж 300 экз.

Цена свободная
Уч.-изд. л. 12,0
Заказ №

**Институт научной информации по общественным наукам
Российской академии наук**
Нахимовский проспект, д. 51/21,
Москва, 117418
<http://inion.ru>

Отдел печати и распространения изданий
Тел. : 8(499) 124-32-15
e-mail: izdat@inion.ru

Отпечатано в типографии
АО «Т8 Издательские Технологии»
109316, Москва, Волгоградский проспект, д. 42, корп. 5, к. 6

