***Алексеева Кристина Александровна***
магистрант
*Научный руководитель*
***Фастова Марина Андреевна***
канд. юрид. наук, доцент
ФГБОУ ВО «Российский государственный социальный университет»
г. Москва

# РАЗВИТИЕ ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ В СВЕТЕ ТЕХНОЛОГИЧЕСКИХ ИННОВАЦИЙ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ

***Аннотация:*** *стремительное развитие цифровых технологий радикально меняет экономические и социальные отношения, ставя перед правом новые задачи по обеспечению баланса между интересами личности, бизнеса и государства. Российское законодательство о персональных данных переживает этап глубокой трансформации под влиянием биометрии, искусственного интеллекта, больших данных, интернета вещей, блокчейна и облачных сервисов. В статье анализируется эволюция регулирования персональных данных в Российской Федерации в сравнительно-правовом контексте, выявляются ключевые технологические вызовы и пробелы правоприменения, рассматриваются механизмы комплаенса и безопасности, а также формулируются перспективные направления модернизации. Предложены конкретные меры по гармонизации российских подходов со стандартами Совета Европы и лучшими зарубежными практиками при сохранении национальных приоритетов цифрового суверенитета. Особое внимание уделяется вопросам защиты прав субъектов персональных данных в условиях цифровизации, а также необходимости создания эффективных механизмов контроля за обработкой персональной информации. Материал опирается на нормативные акты РФ и международные документы, судебную и ведомственную практику, а также широкий круг отечественных и зарубежных научных источников. В заключение подчеркивается важность интеграции*

*новых технологий в правовую систему с учетом этических аспектов и социальной ответственности, что позволит создать безопасное и справедливое цифровое пространство для всех участников экономических и социальных отношений.*

***Ключевые слова:*** *персональные данные, биометрические данные, искусственный интеллект, большие данные, локализация данных, кибербезопасность, трансграничная передача.*

Цифровизация экономики и государственного управления приводит к экспоненциальному росту объема и разнообразия обрабатываемых персональных данных (далее – ПДн) [4], усложнению цепочек обработки и расширению круга участников экосистем данных. Параллельно растет регуляторная нагрузка на организации, а также ожидания общества в части приватности и безопасности [5]. Базовый каркас российского права о ПДн сформирован Федеральным законом №152-ФЗ «О персональных данных» [1] (далее – 152-ФЗ) и сопутствующими актами по безопасности и локализации. Цель статьи – выявить, как инновации трансформируют правовое регулирование персональных данных в РФ, какие вызовы стоят перед правоприменением и какие реформы представляются перспективными в свете международных стандартов. Методологически работа опирается на сравнительно-правовой, формально-юридический и риск-ориентированный подход, анализ правоприменительной практики и научного дискурса.

Российская модель защиты ПДн опирается на конституционные гарантии частной жизни, тайны переписки и информации о частной жизни, развиваемые в 152-ФЗ и подзаконном массиве: постановления Правительства о защите ПДн, уровнях защищенности и особенностях неавтоматизированной обработки, приказы ФСТЭК и ФСБ о требованиях защиты и моделировании угроз, а также нормы о локализации первичного сбора ПДн граждан РФ. С 2014–2015 годов акцент сместился к цифровому суверенитету (локализация, усиление надзора РКН), а также к интеграции безопасности ПДн в более широкий контур критической информационной инфраструктуры. Новейшие изменения касаются биометрических данных, обработки в целях госуслуг и цифрового профиля,

регулирования инцидентов и уведомления субъектов. Международные стандарты формируют ориентиры: Конвенция Совета Европы 108 продвигает риск-ориентированность, подотчетность и оценку воздействия, GDPR закрепляет детализированные принципы обработки, права субъектов, DPIA, DPO и трансграничные механизмы. ЕС дополняет экосистему данными публичного сектора, промышленными данными и доступом к IoT, а также актом об ИИ с режимом риска и ограничений «высокого риска».

Технологические инновации радикально усложнили ландшафт обработки персональных данных. Искусственный интеллект и машинное обучение опираются на масштабные датасеты, нередко собранные для иных целей, что ставит вопрос о совместимости целей первоначальной и последующей обработки, допустимости вторичного использования и достаточности мер деидентификации [7]. Российское право традиционно исходит из приоритета согласия субъекта и ограниченного набора альтернативных оснований, тогда как зарубежные модели шире используют «легитимный интерес» и тест баланса, подкрепляя его механизмами подотчетности. Биометрические технологии усиливают напряженность между эффективностью идентификации и правами личности [8]. Специальное регулирование биометрических ПДн закрепило повышенные требования к согласию, безопасности, хранению и инфраструктуре, однако встает проблема массового видеонаблюдения и удаленной идентификации в общественных пространствах, где тест пропорциональности и наличие реальных альтернатив приобретают ключевое значение [11]. В правоприменении это требует четких методик DPIA для биометрии, документирования оценок риска и ограничений, а также режимов изъятия и уничтожения шаблонов. Большие данные и профилирование поднимают вопросы предсказуемости целей и границ «обоснованных ожиданий» субъектов, особенно при вторичной аналитике и таргетинге. Российская доктрина деидентификации развивается в сторону риск-ориентированной оценки, но сохраняется опасность реидентификации при объединении наборов, что влияет на выбор правовых и технических мер защиты. На особом месте находится блокчейн с присущей ему неизменяемостью записей, что вступает в

очевидное противоречие с принципами актуальности и удаления данных. Юридико-технические компромиссы включают хранение ПДн вне цепочки при использовании хешей для верификации, применение криптографических техник псевдонимизации и управляемой анонимизации, а также формулирование оговорок, разъясняющих пределы исполнения требований на распределенных реестрах. В совокупности эти вызовы демонстрируют необходимость перехода к подотчетности и системной оценке риска для прав и свобод как ключевого контура регулирования.

Современный комплаенс в сфере персональных данных в России складывается на пересечении требований 152-ФЗ, подзаконных актов к защите информации и практик риск-менеджмента. Хотя институт оценки воздействия на права и свободы прямо не закреплен, его функциональные аналоги вытекают из обязанности оператора обеспечивать соответствующие угрозам меры защиты и минимизацию обработки, что обосновывает внедрение процедур DPIA для высокорисковых сценариев, включая биометрию, профилирование и массовое наблюдение. Требования к безопасности ПДн устанавливают уровни защищенности информационных систем [6], структуру организационных и технических мер, порядок моделирования угроз, криптографическую защиту и аттестацию, причем все чаще эти требования интегрируются с режимом безопасности критической информационной инфраструктуры и отраслевыми стандартами киберустойчивости. Это предполагает комплексный подход: сегментацию и управление доступом, шифрование и управление ключами, журналирование и мониторинг событий, обучение персонала, регулярные тесты на проникновение и аудит поставщиков. Режим локализации первичного сбора ПДн граждан РФ и трансграничная передача данных образуют еще один контур комплаенса, требующий оценки юрисдикционных рисков, договорных гарантий и технических мер (сквозное шифрование, хранение ключей у резидентов, распределение ролей и ответственности в цепочке обработки). В условиях фрагментации глобальных стандартов и ограничений международного обмена особую роль приобретает развитие методик оценки «адекватности» и модельных договорных условий. Правоприменение

усиливается за счет роста штрафов, расширения полномочий Роскомнадзора и развития судебной практики по компенсации нематериального вреда и оценке достаточности мер защиты. Эффективное реагирование на инциденты предполагает готовность к оперативному уведомлению регулятора и субъектов, проведение форензики, реализацию корректирующих мер и ретестов, а также постоянное улучшение процессов на основе извлеченных уроков.

Перспективная траектория развития российского законодательства о персональных данных задается переходом от формально-процедурного к риск-ориентированному регулированию, в центре которого – подотчетность оператора. Обоснованным выглядит закрепление в законе обязательности DPIA для обработок повышенного риска, введение требований к назначению ответственного по защите данных в крупных организациях и при высокорисковых операциях, установление обязанности вести и актуализировать реестры операций, а также проводить периодические пересмотры мер защиты [3]. Режим биометрии нуждается в дальнейшей дифференциации по уровню риска и условиям использования. Должны быть обеспечены запреты или моратории на наиболее инвазивные практики, такие как удаленная биометрическая идентификация в публичных пространствах без достаточных гарантий, а также гарантированы полноценные альтернативы для отказавшихся от биометрии, усиление независимого надзора и прозрачности технологий. В сфере трансграничной передачи целесообразно развивать критерии «адекватности» и признанные договорные механизмы, поддерживать двусторонние рамки с ключевыми экономическими партнерами и стимулировать технические решения, снижающие трансграничные риски, включая распределение ключей шифрования и локализованные сегменты обработки. Важным направлением являются регуляторные песочницы и экспериментальные правовые режимы, позволяющие тестировать инновационные модели обработки при усиленных гарантиях для субъектов данных и контролируемых рисках, с прозрачной методологией оценки и механизмами масштабирования успешных практик [9]. Институционально требуется развитие методических материалов регулятора по деидентификации и псевдонимизации, модельных договоров и

стандартов взаимодействия операторов и порученных лиц, а также просветительские инициативы, повышающие цифровую грамотность и осведомленность граждан о правах и способах их реализации. Наконец, согласование режима ПДн с развитием цифрового государства предполагает четкие рамки объединения государственных и коммерческих массивов, независимые аудиты алгоритмов, механизмы алгоритмической транспарентности и регулярную оценку воздействия на права при запуске значимых госцифровых сервисов.

Технологические инновации усиливают ценность и уязвимость персональных данных, делая их центральным ресурсом цифровой экономики. Российское право в целом обеспечивает базовые гарантии защиты ПДн, но нуждается в системной адаптации к высоким рискам ИИ, биометрии, больших данных и трансграничных экосистем. Перенос в национальный контекст ключевых инструментов международных стандартов [2] – риск-ориентированного подхода, подотчетности, DPIA, усиленных прав субъектов и прозрачности алгоритмов – позволит укрепить доверие и повысить глобальную интероперабельность без утраты национальной специфики и приоритета безопасности.

***Список литературы***

1. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» // Собрание законодательства РФ. – 2006. – №31 (ч. I). – Ст. 3451.

2. Баронов В.И. Международное право в схемах и таблицах: учебное пособие / В.И. Баронов, В.А. Батырь, В.И. Липунов; Московская академия экономики и права. – М.: Альфа-Пресс, 2011. – ISBN 978-5-94280-529-6. – EDN QSCFZX.

3. Бембеева Б.С. Право на защиту персональных данных и различные категории персональных данных / Б.С. Бембеева // Право в сфере Интернета: сборник статей / отв. ред. М.А. Рожкова. – М.: Статут, 2018. – С. 48–61. – EDN VNLNWS.

4. Бондаренко Н.Л. Правовая и организационная природа процессов цифровизации и регуляторная функция государства в данной сфере / Н.Л. Бондаренко, Ю.Г. Конаневич // Ex Jure. – 2021. – № 1. – С. 56–67. – EDN OZFAFE. DOI 10.17072/2619-0648-2021-1-56-67

5. Землин А.И. Обеспечение информационной безопасности в условиях специальной военной операции / А.И. Землин, Д.А. Колоколова // Военное право. – 2025. – №3 (91). – С. 13–17. – EDN DARBAZ.

6. Правовое обеспечение профессиональной деятельности для специальности «Информационные системы и программирование»: учебник / А.И. Землин, Д.Ю. Левшиц, Е.С. Митячкина, М.В. Мамонова. – М.: КноРус, 2024. – 128 с. – EDN DLIPYY.

7. Липунов В.И. Искусственный интеллект и тренды цифровизации: техногенный прорыв как вызов праву / В.И. Липунов // Искусственный интеллект и тренды цифровизации: техногенный прорыв как вызов праву: материалы Третьего Международного транспортно-правового форума (Москва, 10–11 февраля 2021 г.). – М.: Российский университет транспорта, 2021. – С. 241–249. – EDN PBDDMP.

8. Мамыкина Е.В. Правовой статус субъектов, участвующих в обработке персональных данных: субъект персональных данных; оператор персональных данных / Е.В. Мамыкина // Моя профессиональная карьера. – 2020. – Т. 3. №11. – С. 117–122. – EDN XYOPDW.

9. Раханов К.Я. Обеспечение конфиденциальности информации в сети Интернет: учебное пособие / К.Я. Раханов, Н.А. Раханова. – Новополоцк: ПГУ им. Евфросинии Полоцкой, 2021. – 192 с. – ISBN 978-985-531-723-5. – URL: https://e.lanbook.com/book/366821 (дата обращения: 21.10.2025).

10. Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) / А.И. Савельев // Право. Журнал Высшей школы экономики. – 2015. – №1. – URL: https://cyberleninka.ru/article/n/problemy-primeneniya-zakonodatelstva-o-personalnyh-dannyh-v-epohu-bolshih-dannyh-big-data (дата обращения: 19.10.2025). EDN WYYJPP

11. Терещенко И.А. Биометрические персональные данные: проблемы и перспективы определения понятия / И.А. Терещенко // Закон и право. – 2024. –

№2. – URL: https://cyberleninka.ru/article/n/biometricheskie-personalnye-dannye-problemy-i-perspektivy-opredeleniya-ponyatiya (дата обращения: 19.10.2025). DOI 10.24412/2073-3313-2024-2-186-192. EDN KLMANL