ПУБЛИЧНО-ПРАВОВЫЕ ИССЛЕДОВАНИЯ

УДК 34:004
ББК 67.0+32.97

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ: ИНФРАСТРУКТУРНЫЕ, НОРМАТИВНЫЕ И ИНСТИТУЦИОНАЛЬНЫЕ ОСНОВАНИЯ

М. В. Алексеева

Донской государственный технический университет (Ростов-на-Дону, Россия)

Рассматривается цифровая трансформация органов государственной власти и управления как комплексный процесс модернизации, в котором технологические решения и правовое регулирование образуют единую систему оптимизации деятельности. Раскрыто содержание инфраструктурных компонентов цифровой трансформации: государственные информационные системы (ГИС), системы интероперабельности (СМЭВ, ЕСИА), облачные технологии, средства биометрической идентификации. Анализируются ограничивающие факторы: дефицит отечественных решений, ведомственная фрагментация, цифровая неоднородность регионов, кибернетические риски и проблемы защиты персональных данных. Показано, что применение методов искусственного интеллекта (ИИ) в государственном управлении требует четкого разграничения ответственности между техническими системами и органами государственной власти, а также разработки процедур верификации и аудита алгоритмических решений. Обосновывается необходимость комплексного нормативно-правового регулирования, охватывающего федеральное законодательство, указы Президента РФ, ведомственные акты и стандарты, а также системных мер по повышению цифровой компетентности государственных служащих и развитию механизмов общественного контроля над использованием цифровых технологий в управлении.

Ключевые слова: цифровая трансформация государственного управления, государственные информационные системы, искусственный интеллект в публичном секторе, юридическая ответственность и подотчетность, нормативно-правовое регулирование, защита данных, кибербезопасность, компетентность государственных служащих

DIGITAL TRANSFORMATION OF PUBLIC ADMINISTRATION: INFRASTRUCTURAL, REGULATORY, AND INSTITUTIONAL FOUNDATIONS

M. V. Alekseeva

Don State Technical University (Rostov-on-Don, Russia)

The article examines the digital transformation of public authorities and administration as a comprehensive modernization process in which technological solutions and legal regulation form an integrated system for optimizing activities. The content of the infrastructural components of digital transformation is revealed:

government information systems (GIS), interoperability systems (SMEV, ESIA), cloud technologies, and biometric identification tools. The study analyzes limiting factors, such as the shortage of domestic solutions, departmental fragmentation, digital heterogeneity of regions, cyber risks, and issues related to personal data protection. It is shown that the use of artificial intelligence (AI) methods in public administration requires a clear delineation of responsibility between technical systems and government authorities, as well as the development of procedures for verification and auditing of algorithmic decisions. The article justifies the need for comprehensive legal regulation encompassing federal legislation, presidential decrees, departmental acts and standards, as well as systematic measures to enhance the digital competence of civil servants and to develop mechanisms for public oversight over the use of digital technologies in administration.

Keywords: digital transformation of public administration, government information systems, artificial intelligence in the public sector, legal responsibility and accountability, legal regulation, data protection, cybersecurity, competence of civil servants

Doi: https://doi.org/10.14258/ralj(2026)2.4

Цифровая трансформация государственного управления представляет собой системный процесс пересмотра организационных и технологических основ деятельности органов государственной власти всех уровней — федеральных, региональных и муниципальных органов управления, а также учреждений, обеспечивающих реализацию государственных функций. Цель цифровой трансформации состоит в повышении качества, оперативности и доступности государственных услуг, снижении административных издержек, укреплении прозрачности и подотчетности органов управления, а также в оптимизации принятия управленческих решений на основе анализа больших объемов данных [1, с. 33]. Однако результативность этого процесса определяется не только масштабом внедрения информационно-коммуникационных технологий (ИКТ), но и системностью их интеграции в единую управленческую архитектуру с четко определенными правовыми процедурами, механизмами контроля и распределенной ответственностью [2, с. 12].

В условиях четвертой промышленной революции, характеризующейся доминированием данных и интенсивным развитием методов искусственного интеллекта, государство оказывается перед необходимостью адаптации управленческих процессов к новой технологической реальности. При этом внедрение цифровых инструментов невозможно рассматривать изолированно от развития правовой базы, которая должна обеспечивать как эффективность, так и легитимность использования этих инструментов в сфере публичного управления.

Государственные институты в контексте настоящей работы включают: органы государственной власти трех ветвей (законодательную, исполнительную и судебную); органы местного самоуправления, осуществляющие управление на муниципальном уровне; государственные учреждения и казенные предприятия, обеспечивающие реализацию государственных функций; интегрированные государственные информационные системы (ГИС) и системы электронного взаимодействия, выступающие в качестве инфраструктурной основы.

Успешная цифровая трансформация органов государственной власти опирается на развитую и надежную информационно-технологическую инфраструктуру, состоящую из следующих ключевых компонентов:

1. Государственные информационные системы (ГИС) — это комплексные программно-аппаратные комплексы, предназначенные для сбора, обработки, хранения и предоставления информации, необходимой для осуществления государственных функций. ГИС характеризуются многоуровневой архитектурой, основанной на принципе модульности, что позволяет обеспечить гибкость и масштабируемость системы. Компоненты ГИС включают: серверную часть (обработка данных, управление ресурсами); клиентскую часть (веб-приложения, доступные через интернет-браузер); системы хранения данных (базы данных, дата-центры); средства защиты информации (шифрование, системы контроля доступа, антивирусное программное обеспечение, системы обнаружения вторжений); интерфейсы интеграции (API, протоколы обмена данными для взаимодействия с другими системами).

2. Единая система межведомственного электронного взаимодействия (СМЭВ) и Единая система идентификации и аутентификации (ЕСИА), которые выступают в качестве базовой инфраструктуры, обеспечивающей взаимодействие различных органов государственной власти и учреждений. Система интероперабельности позволяет органам управления обмениваться информацией в электронной форме, избегая дублирования данных и сокращая административные процедуры для граждан и организаций.

3. Облачные технологии и центры обработки данных (ЦОД). Развертывание облачной инфраструктуры в государственном секторе обеспечивает гибкое использование ИТ-ресурсов, масштабируемость систем и оптимизацию затрат. Облачные сервисы позволяют государственным органам избежать необходимости в развертывании собственных дорогостоящих технологических мощностей.

4. Средства биометрической идентификации. Внедрение биометрических технологий (отпечатки пальцев, распознавание лица, радужной оболочки глаза) обеспечивает надежную идентификацию граждан и повышает уровень защиты персональных данных благодаря многоуровневой защите и фрагментации данных на разных серверах.

5. Спутниковые системы связи. Развертывание низкоорбитальных спутниковых систем способствует расширению масштабов широкополосного доступа в интернет на удаленных территориях и повышает устойчивость телекоммуникационной инфраструктуры в условиях стихийных бедствий и чрезвычайных ситуаций.

Правовое регулирование цифровой трансформации государственного управления в Российской Федерации строится на многоуровневой системе нормативно-правовых актов, которые можно классифицировать следующим образом:

1. Фундаментальные законы в области информационных технологий, где следует выделить: Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3], который устанавливает общие правовые основы обращения с информацией в Российской Федерации, включая принципы производства, хранения, передачи и защиты информации, определяет права и обязанности обладателей информации, пользователей и операторов информационных систем. Этот закон выступает в качестве фундамента, на котором строится вся система информационно-правового регулирования. Федеральный закон № 152-ФЗ «О персональных данных» регулирует обработку персональных данных и устанавливает требования к их защите, контролю над доступом и трансграничной передаче [4]. Особое значение этот закон приобретает при использовании государственными органами методов искусственного интеллекта, требующих обработки больших объемов персональных данных граждан.

2. Законодательство в области защиты критической инфраструктуры. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» устанавливает обязательные требования к защите объектов критической информационной инфраструктуры (КИИ), включая информационные системы в сфере государственного управления, обороны, энергетики, транспорта и здравоохранения. Закон предусматривает категорирование объектов КИИ в зависимости от масштаба потенциальных негативных последствий при киберинцидентах и устанавливает требования к их защите и мониторингу. Федеральный закон № 63-ФЗ «Об электронной подписи» регулирует применение электронной подписи в электронном документообороте, определяет виды электронной подписи (простая, усиленная, квалифицированная), порядок аккредитации удостоверяющих центров и требования к средствам криптографической защиты [5].

3. Законодательство в области предоставления государственных услуг. Федеральный закон № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» определяет механизмы предоставления государственных услуг в электронной форме, устанавливает требования к их качеству и доступности [6]. Этот закон обеспечивает нормативную базу для развития электронного правительства и трансформации механизмов взаимодействия государства с гражданами.

4. Законодательство в области экспериментального правового регулирования ИИ. Федеральный закон № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве, об особенностях

обработки персональных данных при формировании региональных составов данных и предоставления доступа к региональным составам данных и внесении изменений в статьи 6 и 10 Федерального закона „О персональных данных”» устанавливает специальный режим проведения экспериментов по внедрению технологий искусственного интеллекта в отдельных субъектах Российской Федерации (например, в городе федерального значения Москве) [7]. Федеральный закон № 169-ФЗ «О внесении изменений в Федеральный закон „Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации”» расширяет возможности экспериментального правового регулирования в сфере цифровых инноваций, создавая специальные условия для разработки и тестирования ИИ-решений [8].

Стратегическое направление развития цифровых технологий в государстве определяется президентскими указами. Так, например, Указ Президента РФ № 203 утвердил Стратегию развития информационного общества в Российской Федерации на 2017–2030 гг., определяющую приоритеты в области цифровизации экономики и государственного управления [9], Указ Президента РФ № 490 установил Национальную стратегию развития искусственного интеллекта на период до 2030 г., определяющую основные принципы, цели и задачи развития ИИ в России [10]. Принципиально важным положением Национальной стратегии является закрепление принципа ответственности: не допускается делегирование системам ИИ ответственного морального выбора, а ответственность за все последствия работы систем ИИ всегда несет физическое или юридическое лицо. Указ Президента РФ № 646 утвердил Доктрину информационной безопасности Российской Федерации, определяющую государственную политику в области информационной безопасности и описывающую основные угрозы, цели и направления развития правового регулирования [11].

Практическая реализация требований федеральных законов и указов Президента осуществляется посредством приказов и рекомендаций ведомств, например, Приказ ФСБ РФ и ФСТЭК РФ от 31 августа 2010 г. № 416/489 устанавливает требования к защите информации, содержащейся в информационных системах общего пользования. Эти требования детализируют организационно-технические меры, необходимые для защиты государственных ИС от несанкционированного доступа и иных кибернетических угроз.

Министерство цифрового развития, связи и массовых коммуникаций издает методические рекомендации по внедрению цифровых технологий и принципов цифровой трансформации в деятельность государственных органов. Так, например, ГОСТ Р 57700.37–2021 «Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения» устанавливает стандарты для разработки цифровых двойников объектов и процессов [12], а стандарты ГОСТ Р ИСО/МЭК 27001–2012 и ГОСТ Р ИСО/МЭК 27002–2012 адаптируют международные стандарты ISO/IEC в области управления информационной безопасностью к российским условиям.

Цифровая трансформация государственного управления сталкивается с системными ограничениями, среди которых дефицит отечественных программно-аппаратных решений, что создает зависимость от иностранных поставщиков и ограничивает возможность достижения технологического суверенитета [13, С. 37]; ведомственная фрагментация информационных систем, обусловленная историческим развитием ведомственных ИС в различных органах государственной власти без согласованной архитектуры; отсутствие единых стандартов интероперабельности, что приводит к дублированию функций, снижению качества сервиса и увеличению трансакционных издержек; цифровая неоднородность территорий — неравномерное развитие цифровой инфраструктуры в регионах и сельских местностях, что ограничивает возможность обеспечения единого уровня доступности государственных услуг.

Интенсивное внедрение цифровых инструментов сопровождается ростом уязвимостей перед киберугрозами. Основные риски включают: несанкционированный доступ к государственным информационным системам и персональным данным граждан; компрометацию данных вследствие действий киберпреступников, государственных акторов или внутренних злоумышленников; недостаточную зрелость практик управления рисками в государственных органах; частичную имплементацию политики информационной безопасности.

Применение методов искусственного интеллекта в государственном управлении порождает правовую неопределенность в отношении распределения ответственности за решения, основанные на алгоритмических выводах. Это актуализирует требования к формированию четких нормативных рамок, включая: разработку процедур верификации алгоритмов перед их внедрением в систему государственного управления; установление механизмов независимого аудита алгоритмических систем; документирование методик разработки, обучения и применения ИИ-систем; определение субъектов ответственности — органов государственной власти, разработчиков, операторов систем, должностных лиц; разработку процедур обращения и жалоб граждан на решения, принятые с использованием ИИ.

Методы искусственного интеллекта расширяют аналитический потенциал органов государственной власти благодаря способности обрабатывать большие объемы данных, выявлять скрытые закономерности и строить прогнозы. Качество предоставления государственной услуги определяется не только цифровой формой взаимодействия, но и степенью персонализированности — адаптацией предоставления услуги к индивидуальным потребностям. Показательным примером служит система мониторинга и управления национальными проектами и государственными программами, функционирующая в режиме реального времени. Система сопоставляет массив мероприятий и показателей с целевыми ориентирами, идентифицирует межпроектные связи, включая неочевидные зависимости. Например, при обеспечении доступности жилья система учитывает не только параметры ввода и стоимости, но и платежеспособность населения и конфигурацию мер поддержки; применение методов ИИ позволяет заблаговременно обнаруживать такие взаимосвязи и корректировать траектории достижения целей [14].

Организационно-правовую координацию цифровых инициатив обеспечивает единый план достижения национальных целей с горизонтом до 2030 и 2036 гг. Этот план интегрирует целевые ориентиры, государственные программы и проекты, задает их логико-структурную взаимосвязанность и предусматривает централизованный цифровой мониторинг. К системе подключены федеральные органы исполнительной власти, субъекты Федерации и организации-исполнители; в режиме реального времени отслеживается статус более 2,5 тыс. мероприятий [15]. Применение ИИ в управлении крупномасштабными программами повышает оперативность выявления рисков и создает условия для превентивных мер. При этом принципиально сохраняется ведущая роль человека: алгоритмы выполняют аналитические и вспомогательные функции, а окончательные управленческие решения принимаются уполномоченными органами и ответственными менеджерами. Национальная стратегия развития ИИ закрепляет, что ИИ должен применяться как инструмент повышения эффективности деятельности органов публичной власти, а не как самостоятельный субъект управления. Выявленные алгоритмом связи и предложенные решения направляются на верификацию в профильные органы для экспертной оценки, формируя многоуровневый контур проверки — от алгоритмической генерации гипотез до подтверждения или отклонения корреляций экспертным сообществом.

Цифровая трансформация заметно переопределяет структуру рынка труда в государственном секторе. Автоматизация вытесняет ряд рутинных функций, параллельно формируя спрос на специалистов в области анализа больших данных; разработки и внедрения цифровых решений; сопровождения и контроля качества ИТ-систем; аудита и верификации алгоритмических систем.

Оценка качества нормативно-правового регулирования цифровой трансформации в России по состоянию на 2024–2025 гг. дает следующие результаты: сформирована базовая многоуровневая система нормативного регулирования (федеральные законы, указы Президента РФ, ведомственные акты, стандарты); приняты специальные законы об экспериментальном правовом регулировании ИИ; разработаны технические стандарты и методологические рекомендации; утверждены национальные и региональные стратегии развития цифровых технологий. При этом в исследуемом вопросе выявлены следующие проблемы: недостаточная системность и высокая изменчивость правового поля, затрудняющие долгосрочное планирование и инвестиции; недостаточная проработанность технического регулирования применения ИИ в государственном управлении; наличие нормативных коллизий, создающих препятствия реализации проектов цифровой трансформации; правовые барьеры, ограничивающие возможность цифровой трансформации в регионах; недостаточная правовая защита от ИТ-рисков в государственных структурах; отставание регулирования от технологической дина-

мики. Вместе с тем существуют и более оптимистичные оценки, что усиливает контрастность суждений и повышает неопределенность для делового климата [16, с. 6].

Цифровая трансформация государственного управления предстает не как однонаправленный технологический рывок, а как многоуровневый процесс, в основе которого лежит синергия технических средств, правовых инструментов и человеческого управления. Эффективность перехода к цифровому государству определяется не столько скоростью внедрения отдельных решений, сколько способностью системы интегрировать их в единую управленческую структуру с четко артикулированными правовыми нормами и процедурами распределения ответственности; механизмами независимого аудита и верификации алгоритмических решений; адаптивными стандартами совместимости и интероперабельности; развитыми компетенциями государственных служащих в области управления цифровыми технологиями.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Власов К. С. Информационные технологии в России: вызовы цифровой трансформации. М.: Статут, 2021.

2. Дмитриев А. Н. Цифровизация: вызовы и перспективы. М.: Юрайт, 2020.

3. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

4. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ // СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.

5. Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

6. Об организации предоставления государственных и муниципальных услуг: Федеральный закон от 27.07.2010. № 210-ФЗ // СЗ РФ. 2010. № 31. Ст. 4179.

7. О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве, об особенностях обработки персональных данных при формировании региональных составов данных и предоставления доступа к региональным составам данных и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных»: Федеральный закон от 24.04.2020 № 123-ФЗ // СЗ РФ. 2020. № 17. Ст. 2701.

8. О внесении изменений в Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»: Федеральный закон от 08.07.2024 № 169-ФЗ // СПС «Гарант». URL: https://www.garant.ru/hotlaw/federal/1736326/

9. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 09.05.2017 № 203 // СЗ РФ. 2017. № 20. Ст. 2901.

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

11. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // СЗ РФ. 2016. № 50. Ст. 7074.

12. ГОСТ Р 57700.37–2021 Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения. М.: РСТ, 2021.

13. Бородушко И. В. Тенденции цифровой трансформации в современной России // Путеводитель предпринимателя. 2021. Т. 14, № 1. С. 11–20.

14. Мониторинг национальных целей, проектов и программ. URL: https://ac.gov.ru/activity/monitoring-nacionalnyh-celej-proektov-i-programm-8

15. Мишустин утвердил план по достижению национальных целей развития России. URL: https://minfin.gov.ru/ru/press-center/?id_4=39559

16. Дмитриева М А. Цифровые тренды в стратегическом управлении и существующие ИТ-риски // Управленческие науки. 2023. Т. 13. № 2. С. 6–15.