Северо-Кавказский юридический вестник. 2025. № 2. С. 50–58
North Caucasus Legal Vestnik. 2025;(2):50–58
Проблемы конституционного, административного и гражданского права

Научная статья
УДК 342
EDN CYVJNO

Специфика развития государственного управления в условиях современной цифровой трансформации

Марина Владимировна Алексеева[1], Юлия Игоревна Исакова[2]

[1, 2]Донской государственный технический университет, Ростов-на-Дону, Россия
[1]Ростовский филиал Российской таможенной академии, Ростов-на-Дону, Россия

[1]alekseeva80@yandex.ru, https://orcid.org/0000-0003-1436-6946
[2]isakova.pravo@bk.ru, https://orcid.org/0000-0003-4096-4640

Аннотация

Введение. Современные процессы цифровой трансформации оказывают значительное влияние на все аспекты государственного управления, создавая новые вызовы и возможности для повышения его эффективности и прозрачности. Параллельно с этим цифровизация ставит перед государствами необходимость адаптации правовых механизмов к быстро меняющимся социально-экономическим условиям, диктуемым технологическим прогрессом.

Цель. Исследование особенностей реформирования государственного управления в условиях цифровой эпохи, проведение теоретико-правового анализа зарубежного и отечественного опыта, разработка авторского подхода к адаптации управленческих процессов к вызовам цифровизации.

Материалы и методы. Методологическая основа исследования сочетает теоретические и прикладные подходы, включая системный анализ, сравнительный метод изучения зарубежных практик, а также контент-анализ нормативно-правовой базы, аналитических отчетов и научных публикаций. В контексте правового аспекта применены методы юридической интерпретации с целью выявления проблем и перспектив правового сопровождения цифровизации.

Результаты. Выявлены основные преимущества использования цифровых технологий в государственном управлении: повышение прозрачности, сокращение времени предоставления услуг и улучшение взаимодействия между органами власти и гражданами. Параллельно определено, что развитие цифрового управления требует совершенствования правового регулирования для обеспечения защиты данных, прозрачности процедур и предотвращения злоупотреблений. Для решения данных проблем предложены инструменты адаптации, такие как разработка образовательных программ для госслужащих, создание регуляторных «песочниц» для тестирования инноваций, развитие цифровой экосистемы государственного управления и внедрение механизмов снижения цифрового разрыва. Особое внимание уделено подготовке и обновлению правовых норм, регулирующих аспекты цифровой трансформации, что позволит избежать правовых пробелов и повысить эффективность управления.

Выводы. Подчёркивается важность интеграции современных технологий и комплексного подхода к организации цифровой трансформации государственного аппарата. Анализ правового аспекта выявил необходимость создания универсальной и гибкой нормативной базы, которая способна реагировать на технологические изменения и обеспечивать правовые гарантии защиты интересов всех субъектов управления.

Ключевые слова: государственное управление, государственная политика, цифровизация, информационно-коммуникационные технологии, цифровая трансформация, правовые режимы, современные технологии

Для цитирования: Алексеева М. В., Исакова Ю. И. Специфика развития государственного управления в условиях современной цифровой трансформации // Северо-Кавказский юридический вестник. 2025. № 2. С. 50–58. EDN CYVJNO

Problems of Constitutional, Administrative and Civil Law

Original article

The specifics of public administration development in the context of modern digital transformation

Marina V. Alekseeva[1], Yulia I. Isakova[2]

[1, 2]Don State Technical University, Rostov-on-Don, Russia
[1]Rostov branch of the Russian Customs Academy, Rostov-on-Don, Russia

[1]alekseeva80@yandex.ru, https://orcid.org/0000-0003-1436-6946
[2]isakova.pravo@bk.ru, https://orcid.org/0000-0003-4096-4640

Abstract

Introduction. Modern processes of digital transformation have a significant impact on all aspects of public administration, creating new challenges and opportunities to improve its efficiency and transparency. At the same time, digitalization poses the need for states to adapt legal mechanisms to the rapidly changing socio-economic conditions dictated by technological progress.

Purpose. The authors of the scientific article aim to explore the peculiarities of reforming public administration in the digital age, conduct a theoretical and legal analysis of international and domestic practices, and develop an original approach to adapting management processes to the challenges of digitalization. Special attention is paid to the study of the role of law as a key instrument for regulating digital transformation aimed at balancing innovative development and the protection of public interests.

Materials and methods. The methodological foundation of the study combines theoretical and applied approaches, including systems analysis, a comparative method for studying international practices, and content analysis of legal frameworks, analytical reports, and academic publications. In the context of the legal aspect, methods of legal interpretation were employed to identify the challenges and prospects for the legal accompaniment of digitalization.

Results. The analysis revealed the main advantages of using digital technologies in public administration: increased transparency, reduced service delivery time, and improved interactions between government agencies and citizens. Simultaneously, it was determined that the development of digital governance requires the improvement of legal regulation to ensure data protection, procedural transparency, and the prevention of abuses. To address these issues, adaptation tools have been proposed, such as the development of educational programs for civil servants, the creation of regulatory "sandboxes" for testing innovations, the development of a digital public administration ecosystem, and the implementation of mechanisms to reduce the digital divide. Special attention has been given to the preparation and updating of legal norms regulating the aspects of digital transformation, which will help avoid legal gaps and enhance governance efficiency.

Conclusions. The scientific article emphasizes the importance of integrating modern technologies and taking a comprehensive approach to organizing the digital transformation of the state apparatus. The analysis of the legal aspect revealed the necessity of creating a universal and flexible normative framework capable of responding to technological changes and ensuring legal guarantees for the protection of the interests of all governance participants.

Keywords: public administration, public policy, digitalization, information and communication technologies, digital transformation, legal frameworks, modern technologies

For citation: Alekseeva M. V., Isakova Yu. I. The specifics of public administration development in the context of modern digital transformation. *North Caucasus Legal Vestnik.* 2025;(2):50–58. (In Russ.). EDN CYVJNO

Введение

Современные процессы цифровой трансформации оказывают всё более значительное влияние на все сферы человеческой жизнедеятельности, включая государственное управление. В условиях глобализации, усиления роли информационных технологий и массовой цифровизации возникает необходимость научного анализа особенностей реформирования управленческих процессов на государственном уровне. Цифровые решения превращаются в неотъемлемую часть функциональной структуры органов власти, формируя новый формат их взаимодействия с гражданами, бизнесом и другими социальными субъектами.

Переход к цифровой эпохе оказывает существенное влияние на все аспекты социально-экономического и политического развития государства. Современные информационно-коммуникационные технологии (ИКТ) становятся мощным инструментом трансформации государственного управления, оптимизируя его процессы и открывая новые возможности для взаимодействия между публичной властью и гражданским обществом как на национальном, так и на региональном уровнях [1, с. 141–144]. Это обусловлено способностью ИКТ трансформировать традиционные способы административной деятельности, повышая их эффективность, прозрачность, структурированность и приспосабливая их к изменчивым условиям цифрового общества.

Материалы и методы

В настоящем исследовании для анализа процессов цифровой трансформации в сфере государственного управления применялся комплексный междисциплинарный подход, включающий качественные и количественные методы.

На этапе предварительного анализа был проведен системный анализ существующей литературы по теме цифровизации государственного управления, что позволило выявить основные тенденции, ограничения и проблемы в данной области. Для структурирования собранной информации использовался аналитический метод, который позволил классифицировать данные на основе критериев, таких как уровень цифровизации, доступность цифровых услуг и уровень их использования населением.

Для оценки текущего состояния цифровой трансформации в различных странах был применен сравнительный метод, с использованием конкретных примеров успешного внедрения цифровых технологий в государственном управлении (например, Эстонии, Сингапура, Южной Кореи). Метод анализа позволил оценить возможные результаты применения инновационных технологий (таких как искусственный интеллект, большие данные) в ключевых направлениях государственного управления, включая предоставление государственных услуг, принятие управленческих решений и модернизацию бюрократических процессов.

Эмпирическую базу исследования составили данные об объемах инвестиций в цифровую инфраструктуру, уровень доступа к цифровым услугам граждан, результаты пилотных проектов по внедрению цифровых технологий в управленческую практику, а также примеры использования технологии «регуляторных песочниц» для тестирования новых цифровых решений.

Данное исследование основывается на сочетании теоретического анализа, эмпирических данных и моделирования, что позволило системно подойти к изучению вопросов цифровой трансформации государственного управления и сформулировать научно обоснованные рекомендации для повышения ее эффективности.

Результаты

Государственное управление в контексте цифровой трансформации базируется на системном подходе к созданию и реализации информационной политики, которая действует как основа коммуникационных процессов между публичной властью и различными группами общества. Научные исследования подчеркивают, что формирование таких коммуникаций должно учитывать следующие ключевые факторы: информационные ресурсы, кадровый потенциал, финансовые ресурсы, организационные возможности и уровень социального капитала. Например, успешные модели цифрового управления в таких странах, как Южная Корея, Сингапур, Китай, Япония, эти государства демонстрируют высокую зависимость эффективности управленческой деятельности от наличия профессиональных цифровых кадров и развитой инфраструктуры [2, с. 48]. Внедрение модели электронного правительства потребовало реформирования системы государственного управления для обеспечения открытости и прозрачности деятельности государственных органов. Несмотря на то, что азиатские страны стали несколько позже внедрять модель электронного правительства в своих странах, тем не менее стали мировыми лидерами по использованию цифровых технологий для управления государственным сектором.

ИКТ могут обеспечивать не только оперативное информирование граждан, но также активизировать функции социализации, мобилизации и легитимации государственной политики. При этом механизмы социальной адаптации становятся основными инструментами снижения сопротивления населения изменениям и позволяют свести к минимуму негативные последствия цифровизации как процесса, сопряженного с перераспределением прежних ролей и функций государства.

Для полного раскрытия потенциала цифровизации в государственном управлении необходимо учитывать типологию информационной политики можно выделить следующие типы информационной политики [3, с. 30]:

1. Пассивная информационная политика, которая характеризуется отсутствием стратегического планирования и главным образом сосредотачивается на ситуативных или кризисных реакциях.

2. Реактивная политика, предполагающая мониторинг и планирование, но лишенная стратегической перспективы.

3. Активная информационная политика, сочетающая диагностику и управление информационным пространством в соответствии с динамикой изменений.

4. Рациональная информационная политика, реализуемая в условиях крупных муниципальных образований и обеспечивающая глубокую интеграцию информационных процессов в контексте межведомственного взаимодействия.

Цифровая трансформация государственного управления представляет собой сложный и многоуровневый процесс изменения традиционных управленческих механизмов под воздействием современных информационных систем. В отличие от предыдущих этапов модернизации, современный этап трансформации характеризуется широким внедрением технологий искусственного интеллекта, больших данных (Big Data), интернета вещей (IoT) и блокчейн-систем. Эти технологии не только повышают эффективность процессов внутри государственных структур, но и создают условия для формирования новых моделей взаимодействия между государством и обществом.

Цифровизация генерирует новые вызовы и одновременно открывает возможности для государства. С одной стороны, появляются перспективы повышения прозрачности функционирования государственных институтов, ускорения административных процессов и обеспечения высокого уровня общественного контроля. С другой стороны, возрастают риски информационной безопасности, угрозы кибератак на критическую инфраструктуру, а также выявляются проблемные аспекты монополизации данных и роста цифрового неравенства среди населения.

Цифровая трансформация сопровождается не только техническими инновациями, но и глубокими изменениями в правовой и культурной сфере. Процесс транснационализации культуры играет здесь ключевую роль, формируя новый уровень правосознания, который складывается на пересечении национальных и глобальных парадигм. Это отмечается в исследованиях О.Ю. Рыбакова, где подчеркивается, что «информационная правовая культура – совокупность принципов, ценностей, знаний, компетенций, обеспечивающих участникам информационных отношений достижение модели правомерного/неправомерного поведения, основанного на осознании ценности права и приоритетной ценности человека» [4, с. 64].

Кроме того, внедрение цифровых технологий приводит к значительной уязвимости в аспекте сохранения конфиденциальности персональных данных граждан, что обусловливает рост угроз информационной безопасности. В связи с этим в государственной политике требуется учёт рисков киберугроз и их интеграция в стратегические планы цифровизации.

В России цифровизация государственного управления активно развивается благодаря реализации национальной программы «Цифровая экономика Российской Федерации». Одной из её составляющих является проект «Цифровое государственное управление», который нацелен на повышение качества предоставления государственных услуг в электронном виде. Внутри этой программы особый акцент сделан на совершенствовании Единого портала государственных услуг, системы межведомственного взаимодействия и других инфраструктурных элементов, которые обеспечивают функционирование «электронного правительства».

Научные исследования демонстрируют, что российская модель цифрового управления на современном этапе сосредоточена преимущественно на предоставлении услуг в цифровом формате, но пока не уделяет достаточного внимания более широким аспектам улучшения социального благосостояния граждан. Такой подход создает вызовы для гармоничного включения всех социальных групп в цифровое образование, что является не менее важной задачей для формирования инклюзивной цифровой среды.

Международные практики цифровизации государственного управления, такие как шведская модель открытого правительства или южнокорейская платформа для «умных городов», предоставляют богатый материал для сравнения. «Основные преимущества зарубежных подходов выражаются в более быстром принятии решений за счет анализа данных, повышении государственной прозрачности и предоставлении гражданам доступа к дистанционным услугам. Тем не менее, проблемы

межведомственной координации и совместимости законодательной базы с глобальными технологическими изменениями остаются фундаментальными преградами даже для развитых стран» [5].

Особое внимание уделяется участию граждан в процессах цифрового государственного управления. Это позволяет не только повысить открытость и доверие к государственным институтам, но и создать механизмы обратной связи, которые способствуют быстрому реагированию на возникающие проблемы

Глобальный процесс цифровой трансформации формирует уникальный набор проблем и вызовов для государственного управления. Рассматривая эти проблемы, можно выделить следующие ключевые аспекты:

1. Институциональная инертность и сопротивление изменениям. Государственные структуры, как правило, обладают сложной бюрократической системой, что приводит к задержкам в модернизации процессов принятия управленческих решений. Ключевая проблема заключается в недостаточной гибкости государственной системы по сравнению с динамикой внешней технологической среды.

2. Дефицит квалифицированных кадров – успешная цифровизация государственного управления требует наличия в органах власти высококвалифицированных специалистов, обладающих знаниями в области цифровых технологий. Однако на практике часто наблюдается дефицит таких кадров, что тормозит реализацию стратегий цифровой трансформации.

3. Риски цифрового неравенства – один из главных вызовов цифровизации связан с тем, что доступ к новым информационным услугам и возможностям остаётся неравномерным среди различных групп населения. Это может привести к маргинализации наиболее уязвимых слоёв общества и созданию барьеров в доступе к государственным услугам.

4. Угрозы безопасности информации. С увеличением роли цифровых технологий в управлении растёт опасность кибератак, что требует создания комплексной системы защиты государственных информационных систем и данных граждан.

В эпоху цифровой трансформации масштаб использования информационных технологий и сетей продолжает неуклонно расти, что создает новые вызовы для защиты данных. Согласно Доктрине информационной безопасности Российской Федерации, принятый в 2016 году, обеспечение национальной безопасности во многом связано с предотвращением кибератак, направленных на критическую информационную инфраструктуру и цифровое пространство страны. Действительно, кибератаки на энергетику, транспортные сети, банковский сектор или системы управления обороной могут привести к катастрофическим последствиям для национальной безопасности.

Одной из ключевых проблем становится рост числа киберпреступлений. Это демонстрирует необходимость разработки новых подходов в реагировании на информационные вызовы. В свою очередь, проводимые исследования в этой сфере, фокусируются на автоматизации процессов обнаружения угроз с использованием технологий искусственного интеллекта [6, с. 169–171].

В связи с особыми условиями, связанными с геополитической обстановкой в 2022–2023 годах, роль информационной безопасности возросла и с учетом нового направления агрессивной информационной политики недружественных государств. В частности, использование дезинформации и ряд киберугроз, как показано в работе Небренчина С. М., «ставит под угрозу не только внутреннюю политическую стабильность, но и социальные устои общества» [7, с. 212].

В российской практике данная проблема непосредственно регулируется федеральными законами: Закон №149-ФЗ «Об информации, информационных технологиях и о защите информации» и специализированный Закон №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Однако, как справедливо отмечает Зиновьева Е.С. в своих исследованиях, «в международном праве отсутствует понятийно-категориальный аппарат в области информационной безопасности, который влияет на международные отношения» [8, с. 235].

Обсуждение

Цифровизация государственного управления становится одной из центральных задач современной России. Такие проекты как «Цифровая экономика Российской Федерации» и обновлённая Доктрина информационной безопасности акцентируют внимание на необходимости проактивных мер, направленных на минимизацию информационных угроз за счёт новых технических решений. Введение электронного документооборота, развитие «Госуслуг», а также платформа «ГосТех» позволяют автоматизировать основные процессы управления, но влекут за собой повышенные риски утечки данных, что потребует дальнейшего усиления мер регулирования.

Использование цифровых технологий также наблюдается в сфере выборов. В 2023 г. электронное голосование дало возможность значительно ускорить процесс выборов и повысить их прозрачность,

но одновременно возникли угрозы кибератак и манипуляции голосами, требующие новых методов защиты информационных операций.

Современные исследования указывают на важность инвестирования в развитие технологий искусственного интеллекта (ИИ) как в защитных, так и в наступательных целях. Сегодня ИИ используются как для анализа больших данных, так и для создания самонаводящихся программ кибершпионажа на инфраструктурные объекты. По данным консенсуса, представленного Организацией Объединенных Наций на саммите в Лондоне 2023 года, необходимо глобальное согласование подходов в регулировании ИИ, что касается и вопроса манипуляции данными.

Способность России удерживаться в лидерах цифровизации требует не только технологий, но и инвестиции в человеческий капитал. Работа с утечками данных, оснащение IT-компаний современными средствами защиты и контроль сетевого трафика являются основой обеспечения внутренней стабильности процессов постиндустриального перехода.

Таким образом, этими процессами обусловлена необходимость формирования новой стратегии управления и мониторинга, связанной с дальнейшей цифровизацией. Фокус должен смещаться на активное использование платформенной экономики, атакующих Институтов кибербезопасности Российской Федерации, включая такие институциональные структуры как ОДКБ, и гранты на научные исследования в области ИИ.

Сложным остаётся вопрос противодействия фишинговым атакам, которые, согласно статистическим данным, входят в топ-3 угроз цифрового мира. В частности, кибератаки, использующие социальную инженерию, остаются наиболее сложными для отслеживания. Россия, будучи крупнейшим интернет-рынком Европы, столкнулась с необходимостью значительного увеличения кибертехнологий, таких как системы автоматического оповещения о попытках взлома.

Учитывая вышеизложенное, противодействие киберугрозам на современном этапе требует стратегического совмещения человеческого, технического и правового аспектов. Регулярное обновление законодательной базы, внедрение систем раннего оповещения о кибератаках и анализ повседневных угроз критической инфраструктуры остаются ключевыми аспектами государственной политики. Особо важной задачей становится разработка и внедрение интеграционной концепции к адаптации юридических норм к инновациям, включая передачу данных.

Важным инструментом защиты является также развитие системы патриотического воспитания в киберпространстве, которое формирует устойчивое мировоззрение и защиту граждан от чуждого влияния. Влияние стандартов ИКТ на восприятие угроз должно быть сбалансированным с сохранением национальной идентичности национальной информационной политики.

Концептуальная стратегия обеспечения информационной безопасности должна быть многокомпонентной и учитывать глобальные вызовы, технологические трансформации, присущие цифровой экономике угрозы, а также культурные защитные механизмы, способные реагировать на любые вызовы информационной эпохи. Критическая информационная инфраструктура (КИИ) включает в себя объекты, от функционирования которых зависит стабильность ключевых отраслей экономики, государственного управления, обороны, здравоохранения, финансирования и других систем, обеспечивающих жизнедеятельность государства.

Цифровая трансформация государственных институтов требует не только внедрения новых технологий, но и создания устоявшейся правовой среды, которая обеспечит адекватное и своевременное регулирование возникающих процессов. Одним из ключевых элементов модернизации является разработка комплекса нормативных актов, ориентированных на гармонизацию традиционного законодательства с новыми реалиями цифрового общества. Без такого подхода цифровизация государственного управления может столкнуться с правовыми пробелами, низким уровнем защиты данных и рисками потери доверия граждан к государственным институтам.

Основу правового регулирования цифровизации составляют нормы, направленные на защиту персональных данных, регулирование ответственности за использование цифровых инструментов и обеспечение информационной безопасности. В российской практике внедрение нового Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» стало одним из ключевых шагов для защиты государственных систем информации. Однако в контексте цифровой трансформации государственной политики потребность в разработке новых правовых механизмов возрастает. Например, важной проблемой остаётся недостаточное регулирование использования искусственного интеллекта в управленческих процессах и принятии решений.

Особую значимость приобретает вопрос юридической силы электронных документов. В условиях активного перехода государственных органов на электронный документооборот необходимо

разработать унифицированные стандарты, регулирующие формат, использование и защиту электронных подписей. На текущий момент в мировых практиках наблюдаются различия в подходах к регулированию электронных документов между странами, что затрудняет трансграничное взаимодействие, особенно при реализации международных цифровых проектов или программ.

Другим важным аспектом является организация законодательных баз для работы с большими данными (Big Data). Государственные структуры, активно использующие большие объёмы данных для анализа и прогнозирования социальных процессов, сталкиваются с необходимостью урегулирования вопросов анонимизации данных, их хранения, обработки и передачи. Примером может служить безопасность данных о гражданах, используемых в программах, таких как система электронных медицинских карт или цифровой паспорт гражданина.

Цифровизация государственного управления требует формирования институциональной правовой базы для реализации механизмов так называемых «регуляторных песочниц», которые позволяют проводить тестирование инновационных цифровых технологий в условиях временного освобождения от ряда норм действующего законодательства. В России данные механизмы используются в финансовом секторе, однако их интеграция в сферу государственного управления позволит ускорить внедрение инновационных решений.

На международном уровне также ведутся активные дискуссии по поводу координации правовых подходов к регулированию цифрового управления. Например, в Европейском Союзе с точки зрения регулирования искусственного интеллекта разрабатывается специальный «Акт об ИИ» (AI Act), который станет первой системой нормативного регулирования в этой области. Россия могла бы адаптировать подобные решения на национальном уровне, включая их в программы цифровой трансформации.

При этом информационная безопасность в системе государственного управления в современных условиях является ключевым фактором стабильности, суверенитета и устойчивого социально-экономического развития государства. Эффективное противодействие угрозам и минимизация рисков требуют интеграции усилий государства, бизнеса и общества, направленных на создание безопасной цифровой среды и надежной защиты данных и технологий [9, с. 86].

Цифровизация изменяет не только технические аспекты государственного управления, но и сами принципы организации работы государственных органов. Традиционная концепция государственной службы, основанная на иерархической структуре, всё чаще уступает место сетевым и гибким моделям управления. Госаппарат переходит к концепциям «цифрового государства» и «госуслуг 2.0», где центральное место занимает взаимодействие с гражданами и обеспечение обратной связи.

Авторы таких подходов подчёркивают, что успешная цифровизация государственных структур зависит от интеграции трех основных компонентов: данных, технологий и культуры внутри управления [10, p. 2]. При этом ключевым элементом становится не только внедрение технологий, но и пересмотр традиционных управленческих парадигм.

На основе анализа мирового опыта цифровизации и выявленных вызовов можно предложить несколько авторских решений, которые помогут ускорить процесс адаптации государственного управления к цифровой эпохе:

1. Комплексное развитие компетенций сотрудников органов государственной власти. Необходимо разработать и реализовать образовательные программы для государственных служащих, направленные на обучение основам цифровой грамотности, работе с большими данными, применению технологий искусственного интеллекта. Программы должны предусматривать как базовую подготовку, так и повышение квалификации.

2. Создание цифровой экосистемы управления. Применение концепции единого цифрового пространства позволит интегрировать различные государственные системы, что обеспечит их совместимость и синхронизацию. В рамках такой экосистемы можно внедрять технологии управления на основе данных (Data-driven governance), что даст возможность более точно анализировать социально-экономические процессы и принимать обоснованные управленческие решения.

3. Регуляторные «песочниц». Для облегчения внедрения инновационных цифровых решений в государственном управлении предлагается внедрить механизм регуляторных «песочниц». Это обеспечит испытание и адаптацию новых технологий в условиях реального времени без излишних законодательных ограничений.

4. Инструменты для снижения цифрового неравенства. В качестве одной из ключевых мер необходимо разработать программы по увеличению доступности интернета и цифровых технологий

в удалённых и сельских территориях. Создание «цифровых центров» позволит обеспечить равный доступ граждан к государственным услугам.

5. Обеспечение информационной безопасности. Реализация программы кибербезопасности на уровне государства должна включать внедрение как технических средств защиты, так и обучение госслужащих основам предотвращения атак, связанных с хакерскими угрозами и утечкой данных.

На основе предложенных решений можно дополнительно включить разработку правового механизма, который будет ориентирован на регулирование цифровой трансформации государственного управления. Для этого необходимо создать комплексную законодательную базу, учитывающую специфику внедрения цифровых технологий. Этот механизм должен предусматривать правовые нормы для защиты цифровых данных, создание стандартов работы с искусственным интеллектом и большими данными, а также обеспечение прав граждан в условиях цифровизации. Фундаментом такого механизма может стать принятие рамочного закона о цифровом управлении, который будет определять основные принципы, ориентиры и методы регулирования данной сферы, а также регулировать использование инновационных решений, формируя баланс между развитием технологий, правовой защитой и свободами граждан.

Заключение

Современный этап цифровой трансформации предъявляет уникальные требования к системе государственного управления, которые возникают из-за необходимости реагировать на быстро изменяющуюся технологическую среду. Успешная цифровизация требует комплексного подхода, включающего как модернизацию технической базы, так и развитие человеческого капитала, нормативных и организационных подходов. Несмотря на существующие вызовы, цифровая трансформация предоставляет государству уникальную возможность повысить свою эффективность, сделать управление более прозрачным и ориентированным на потребности общества.

Правовой аспект цифровизации государственного управления предполагает не только устранение пробелов в законотворчестве, но и использование права как инструмента защиты общественных интересов, обеспечения ответственности за нарушения в цифровой среде и создания условий для эффективного взаимодействия граждан и государства. Регулярное обновление законодательства и его адаптация к вызовам цифровой эпохи позволят минимизировать социальные, экономические и правовые риски, сформировав устойчивую правовую среду для цифрового государства.

Предложенные в научной статье решения, включая цифровую экосистему, образовательные инициативы и регуляторные песочницы, могут стать основой для формирования нового поколения государственного управления, адаптированного к реалиям цифрового века. Такой научный подход позволит не только создать новые управленческие парадигмы, но и заложить основу для устойчивого развития государства в условиях стремительных технологических изменений. Переход к цифровой эпохе оказывает существенное влияние на все аспекты социально-экономического и политического развития государства. Современные информационно-коммуникационные технологии (ИКТ) становятся мощным инструментом трансформации государственного управления, оптимизируя его процессы и открывая новые возможности для взаимодействия между публичной властью и гражданским обществом как на национальном, так и на региональном уровнях. Это обусловлено способностью ИКТ трансформировать традиционные способы административной деятельности, повышая их эффективность, прозрачность, структурированность и приспосабливая их к изменчивым условиям цифрового общества.

Список источников

1. Назаренко Т. С., Новикова И. В. Цифровая трансформация государственного управления как стратегическое общественное благо // Стратегирование: теория и практика. 2023. №2. С. 140–157. DOI: 10.21603/2782-2435-2023-3-2-140-157

2. Бурденко Е.В. Модели электронного правительства // January 2023. Russian Journal of Innovation Economics. 13(1):59–76. DOI: 10.18334/vinec.13.1.117234

3. Лихтин А. А., Ковалев А. А. Теоретические аспекты понятия «Информационная политика» и особенности ее реализации в современной российской общественно-политической реальности // Управленческое консультирование. 2017. №1 (97). С. 29–36.

4. Рыбаков О. Ю. Правовая информационная культура в условиях цифровой трансформации общества и государства // Правосудие. 2024. №3. С. 59-74. DOI: 10.37399/2686-9241.2024.3.59-74

5. Титова А. И. Предоставление государственных услуг в электронном виде: зарубежный опыт и российская практика // Инновации и инвестиции. 2018. № 5. С. 169–174.

6. Козаев Н. Ш. Киберпреступность в современном мире: тенденции, вызовы и стратегии противодействия // Гуманитарные, социально-экономические и общественные науки. 2024. № 11. С. 146–153. DOI: 10.24412/2220-2404-2024-11-9

7. Небренчин С. М. Актуальные вопросы укрепления информационной безопасности России в связи со специальной военной операцией на Украине // Россия: тенденции и перспективы развития. 2023. № 18-1. С. 211–216.

8. Зиновьева Е. С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности // Вестник МГИМО. 2016. №4 (49). С. 235-247. DOI: org/10.24833/2071-8160-2016-4-49-235-247

9. Алексеева М. В., Определение категории «Информационная деятельность» в юридической науке // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2012. № 1 (20). С. 86–90.

10.Janowski T., Estevez E., Baguma R. Platform governance for sustainable development: Reshaping citizen-administration relationships in the digital age. – Government Information Quarterly, 2018. – № 35(4). – PP. 1–16. DOI: 10.1016/j.giq.2018.09.002

References

1. Nazarenko T. S., Novikova I. V. Digital Transformation of Public Administration as a Strategic Public Good*. Strategizing: Theory and Practice.* 2023;(2):140–157. (In Russ.)

2. Burdenko E. V. E-government models. *Russian Journal of Innovation Economics*. 2023;13(1):59–76.

3. Likhtin A. A., Kovalev A. A. Theoretical aspects of the concept of "Information Policy" and features of its implementation in modern Russian socio-political reality. *Management Consulting.* 2017;1(97):29–36. (In Russ.)

4. Rybakov O. Yu. Legal information culture in the context of digital transformation of society and state. *Justice.* 2024;(3):59–74. (In Russ.)

5. Titova A. I. Provision of State Services in Electronic Form: Foreign Experience and Russian Practice. *Innovations and Investments.* 2018;(5):169–174. (In Russ.)

6. Kozaev N. Sh. Cybercrime in the Modern World: Trends, Challenges, and Counteraction Strategies. *Humanities, Socio-Economic, and Social Sciences.* 2024;(11):146–153. (In Russ.)

7. Nebrenchin S. M. Current Issues of Strengthening Russia's Information Security in Connection with the Special Military Operation in Ukraine. *Russia: Trends and Development Prospects.* 2023;(18-1):211–216. (In Russ.)

8. Zinovieva E. S. *Perspective Trends in the Formation of an International Regime for Ensuring Information Security. MGIMO Bulletin.* 2016;4(49):235–247. (In Russ.)

9. Alexeeva M.V. Definition of the Category "Information Activity" in Legal Science. *Science and Education: Economy and Industry; Entrepreneurship; Law and Management.* 2012;1(20):86–90. (In Russ.)

10.Janowski T., Estevez E., Baguma R. Platform Governance for Sustainable Development: Reshaping Citizen-Administration Relationships in the Digital Age. *Government Information Quarterly.* 2018;35(4):1–16.

Информация об авторах

М. В. Алексеева – кандидат юридических наук, доцент, зав. кафедрой «Теория и история государства и права» ДГТУ; доцент кафедры государственно-правовых дисциплин Ростовского филиала РТА.
Ю. И. Исакова – доктор социологических наук, кандидат юридических наук, доцент, декан факультета «Юридический» ДГТУ.

Information about the authors

M. V. Alekseeva – Cand. Sci. (Law), Associate Professor, Head of the Department of Theory and History of State and Law of the Don State Technical University; Associate Professor of the Department of State and Legal Disciplines of the Rostov branch of the Russian Customs Academy.
Yu. I. Isakova – Dr. Sci. (Sociology), Cand. Sci. (Law), Associate Professor, Dean of the Faculty of Law at Don State Technical University.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.
Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 12.03.2025; одобрена после рецензирования 25.04.2025; принята к публикации 28.04.2025.
The article was submitted 12.03.2025; approved after reviewing 25.04.2025; accepted for publication 28.04.2025.