УДК 004.056

Астахова А.С.,
Магистрант
2 курс, ИГСУ РАНХиГС
Россия, г. Москва

ГОСУДАРСТВЕННОЕ УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ СФЕРОЙ И ЦИФРОВЫМИ ТЕХНОЛОГИЯМИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: *В статье проанализированы правовые и институциональные основы госуправления информационной сферой в России. Исследована цифровизация госаппарата, регионов, муниципалитетов и социальной сферы, включая образование. Среди главных проблем: фрагментация права, нехватка ИТ-кадров, киберугрозы и зависимость от импорта. Для их решения предложено развивать отечественное ПО, улучшать координацию и повышать цифровые навыки служащих.*

Ключевые слова: *информационная сфера, цифровые технологии, государственное управление, цифровой суверенитет, региональная исполнительная власть, кибербезопасность.*

Abstract: *The article analyzes the legal and institutional foundations of IT state management in Russia. It explores the digitalization of the government, regions, municipalities, and the social sphere. Major challenges include legal fragmentation, IT staff shortages, cyber threats, and import reliance. Proposed solutions include developing domestic software, improving coordination, and enhancing digital skills.*

Keywords: *information sphere, digital technologies, public administration, digital sovereignty, regional executive power, cybersecurity.*

Современный этап социально-экономического развития Российской Федерации неразрывно связан с форсированным переходом к цифровой экономике и информационному обществу. В новой парадигме информация и данные выступают не просто как вспомогательный ресурс, но как ключевой стратегический актив, напрямую определяющий уровень национальной безопасности и конкурентоспособность государства на глобальной арене. Информационная сфера, охватывающая сложную совокупность процессов генерации, обработки, систематизации, хранения, распространения и использования массивов данных, становится важнейшим объектом целенаправленного государственного регулирования.

Актуальность темы исследования обусловлена синергией внутренних и внешних факторов. С одной стороны, существует острая внутренняя потребность в глубокой модернизации механизмов государственного управления, повышении доступности и прозрачности публичных услуг, а также в преодолении цифрового неравенства между различными территориями страны. С другой стороны, нарастающее геополитическое давление, технологические санкции и беспрецедентная глобальная конкуренция требуют от государства немедленных действий по обеспечению технологического и цифрового суверенитета. Цель настоящей статьи — провести системный, многоуровневый анализ правовых, организационных и практических основ государственного управления информационной сферой в РФ, выявить барьеры цифровизации и разработать научно обоснованные рекомендации по их преодолению.

1. Теоретико-правовые основы государственного управления информационной сферой.

В современной российской правовой доктрине под информационной сферой понимается «совокупность информационных ресурсов, сложной информационной инфраструктуры, а также субъектов (организаций и граждан), осуществляющих сбор, обработку, накопление, хранение, поиск,

распространение и предоставление информации» [1, с. 18]. Государственное управление данной сферой представляет собой системную, целенаправленную и властную деятельность органов публичного администрирования по формированию благоприятных условий для её устойчивого развития. Эта деятельность направлена на защиту национальных интересов, обеспечение кибербезопасности и безусловную реализацию конституционных прав граждан на свободный поиск и получение информации.

Фундаментальную правовую базу цифрового развития составляют положения Конституции Российской Федерации (в частности, ст. 29 и 30), закрепляющие базовые информационные права. Профильным системообразующим актом выступает Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [2], который задает понятийный аппарат и общие принципы оборота данных. Важнейшим элементом правового ландшафта является Федеральный закон № 152-ФЗ «О персональных данных» [3], определяющий жесткие рамки работы с чувствительной информацией граждан.

Стратегический вектор управления задается комплексом документов государственного планирования: Стратегией национальной безопасности РФ [4], Доктриной информационной безопасности РФ [5], а также стратегиями развития отрасли информационных технологий. Концептуальной задачей законодателя на современном этапе выступает поиск оптимального баланса между необходимостью стимулирования технологических инноваций (через дерегулирование и экспериментальные правовые режимы) и жестким контролем за обеспечением безопасности критической информационной инфраструктуры (КИИ). При этом государство обязано поддерживать высокий уровень открытости, что регламентировано нормами Федерального закона № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов» [7].

2. Стратегические документы и институциональная архитектура многоуровневого управления.

Ключевым драйвером трансформации отрасли является национальная программа «Цифровая экономика Российской Федерации» [8]. Архитектура программы включает в себя федеральные проекты, охватывающие нормативное регулирование, развитие инфраструктуры, поддержку сквозных технологий, цифровое государственное управление и подготовку кадров.

Институциональное ядро на федеральном уровне представлено Министерством цифрового развития, связи и массовых коммуникаций РФ, которое координирует деятельность других ведомств. Однако наибольший интерес с точки зрения практической реализации государственной политики представляет перенос цифровых инициатив на уровень субъектов федерации и местного самоуправления. Эффективность управления информационной сферой напрямую зависит от слаженности работы территориальных органов исполнительной власти.

Анализ региональных практик показывает существенную дифференциацию в подходах. Так, детальное рассмотрение структуры исполнительной власти в субъектах РФ на примере Ленинградской области демонстрирует создание специализированных комитетов цифрового развития, которые интегрируют в себе функции связи, защиты информации и развития электронного правительства, формируя единую нормативно-правовую базу регионального уровня. Напротив, система и структура управления Тюменской области показывает пример глубокой интеграции ИТ-департамента с экономическим блоком правительства, что позволяет региону занимать лидирующие позиции в рейтингах цифровой зрелости благодаря внедрению интеллектуальных транспортных систем и систем поддержки принятия управленческих решений.

Муниципальный уровень управления информационной сферой является наиболее близким к гражданину, но одновременно и наиболее уязвимым

звеном из-за дефицита финансирования и кадров. Тем не менее, передовые муниципальные образования активно внедряют новые стандарты. Примечателен опыт применения распоряжений администрации МО ГО Сыктывкар по части оценки компетенций муниципальных служащих по итогам аттестации, где уровень владения цифровыми инструментами работы с данными и электронным документооборотом становится обязательным критерием профессиональной пригодности.

3. Практические аспекты цифрового государственного управления и отраслевая цифровизация.

Основой практической реализации государственного управления информационной сферой стало создание Системы межведомственного электронного взаимодействия (СМЭВ) [6], которая кардинально изменила логику работы госаппарата, исключив необходимость требования от граждан документов, уже имеющихся в распоряжении органов власти. Витриной этой трансформации выступает Единый портал государственных и муниципальных услуг (ЕПГУ). По данным Минцифры РФ на 2026 год, проникновение портала охватывает подавляющее большинство экономически активного населения [9, с. 42], а количество доступных проактивных сервисов непрерывно растет.

Важным вектором практической цифровизации выступает внедрение ИТ-решений в социальную сферу, в частности, в образование. Управление инфраструктурой образовательных учреждений требует современных подходов. Например, разработка и внедрение муниципальных или региональных веб-приложений для учета материально-технической базы и школьного спортивного инвентаря позволяет значительно оптимизировать расходы бюджетов, повысить прозрачность закупок и автоматизировать рутинные управленческие процессы администраций школ, что является прямым следствием реализации политики цифрового госуправления на микроуровне.

4. Ключевые вызовы и системные риски.

Несмотря на видимые успехи, система государственного управления информационной сферой сталкивается с серьезнейшими вызовами, требующими немедленного научного и практического осмысления:

1. Технологическая и инфраструктурная зависимость. Процесс импортозамещения в сфере ИТ идет неравномерно. Значительная доля оборудования, серверных мощностей, микроэлектроники и базового программного обеспечения (операционные системы, системы управления базами данных) исторически зависела от западных вендоров. Санкционный режим обнажил критические уязвимости государственного сектора в этой части [10, с. 74].

2. Риски кибербезопасности и защита КИИ. С переходом госуправления в цифровую среду экспоненциально возросло количество компьютерных атак на государственные информационные системы. Ежегодные отчеты профильных ведомств фиксируют миллионы инцидентов, направленных на деструктивное воздействие, кражу персональных данных и парализацию работы электронных сервисов [11, с. 15].

3. Кадровый голод в высокотехнологичных отраслях. Темпы цифровой трансформации значительно опережают возможности системы образования по подготовке профильных специалистов. Дефицит кадров (инженеров, программистов, специалистов по анализу данных и информационной безопасности) оценивается в сотни тысяч человек, что становится главным тормозом технологического прорыва [12, с. 8].

4. Этические, социальные и правовые дилеммы. Внедрение алгоритмов искусственного интеллекта и нейросетей в системы принятия государственных решений, камеры уличного наблюдения и биометрическую идентификацию порождает сложные этико-правовые коллизии. Возникают угрозы нарушения приватности, несанкционированного профилирования граждан и возникновения так называемых «цифровых диктатур».

5. Перспективы и рекомендации по совершенствованию управления.

Для нивелирования выявленных рисков и повышения эффективности государственного управления информационной сферой необходимо реализовать комплекс системных мер:

- **Институциональная реформа:** усиление роли межведомственных проектных офисов и создание единого научно-технологического центра при Правительстве РФ для синхронизации всех разрозненных цифровых инициатив.
- **Стимулирование технологического суверенитета:** кратное увеличение грантовой поддержки отечественных разработчиков, создание преференций на госзакупках для программно-аппаратных комплексов российского производства (ПАК) и развитие собственной микроэлектронной базы.
- **Кадровая трансформация госслужбы:** пересмотр программ профессиональной переподготовки (на примере упомянутых практик аттестации муниципальных служащих) с фокусом на владение инструментами аналитики больших данных, понимание архитектуры информационных систем и основ кибергигиены.
- **Правовое регулирование ИИ:** разработка детализированного национального кодекса этики использования систем искусственного интеллекта в государственном управлении, введение механизмов обязательного аудита алгоритмов на предмет предвзятости и дискриминации.

Заключение Государственное управление информационной сферой и цифровыми технологиями в Российской Федерации находится на этапе глубинной парадигмальной трансформации. Переход от простой «информатизации» отдельных ведомств к построению целостной платформенной экосистемы государства объективно сопровождается рядом трудностей структурного, технологического и кадрового характера.

Проведенный анализ показывает, что успешная реализация стратегических целей невозможна без обеспечения подлинного цифрового суверенитета. Опыт регионов, таких как Ленинградская и Тюменская области, а также муниципальных образований, доказывает необходимость гибкого подхода, учитывающего территориальную специфику. Будущее информационной сферы России зависит от того, насколько быстро и эффективно институты государственной власти смогут адаптировать нормативную базу, преодолеть технологическую зависимость и сформировать кадровый потенциал, способный не только обслуживать, но и создавать передовые цифровые решения.

Список использованных источников и литературы:

1. Лапина М.Н. Информационная сфера в системе национальной безопасности России // Государственное управление. Электронный вестник. — 2022. — № 85. — С. 15–28.

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. — 2006. — № 31 (ч. 1). — Ст. 3448.

3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. — 2006. — № 31 (ч. 1). — Ст. 3451.

4. Указ Президента РФ от 31 декабря 2020 г. № 805 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. — 2021. — № 1. — Ст. 1.

5. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. — 2016. — № 50. — Ст. 7075.

6. Распоряжение Правительства РФ от 17 ноября 2015 г. № 2325-р «Об утверждении Концепции создания и развития системы

межведомственного электронного взаимодействия» // Собрание законодательства РФ. — 2015. — № 48. — Ст. 6752.

7. Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Собрание законодательства РФ. — 2009. — № 7. — Ст. 772.

8. Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р «Об утверждении программы “Цифровая экономика Российской Федерации”» // Собрание законодательства РФ. — 2017. — № 32. — Ст. 5130.

9. Министерство цифрового развития РФ. Отчёт о реализации программы «Цифровая экономика» за 2025 год. — М., 2026. — 142 с.

10. Смирнов Д.А. Технологический суверенитет России: вызовы и стратегии // Вестник МГИМО. — 2025. — Т. 18, № 1. — С. 70–85.

11. Центр информационной безопасности ФСБ России. Ежегодный отчёт о состоянии кибербезопасности в РФ. — М., 2026. — 89 с.

12. Министерство труда и социальной защиты РФ. Прогноз потребности экономики в кадрах цифровой экономики до 2030 года. — М., 2025. — 56 с.

13. Коваленко В.И., Петрова А.Н. Цифровая трансформация исполнительной власти: региональный аспект // Вестник государственного и муниципального управления. — 2025. — № 3. — С. 112–120.