

Эволюция модели управления на основе данных в Российской Федерации: исторический генезис, современные институциональные ограничения и перспективы развития в условиях трансформации нормативно-правовой среды

Научный руководитель – Купцова Ирина Валентиновна

Хадыева Диана Айратовна

Аспирант

Московский государственный университет имени М.В.Ломоносова, Факультет государственного управления, Кафедра регионального и муниципального управления, Москва, Россия

E-mail: dianahadyeva@gmail.com

Цифровая трансформация государственного управления определена Указом Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» как одна из национальных целей развития [1]. Ключевым требованием выступает достижение «цифровой зрелости» - автоматизация транзакций в рамках единых отраслевых цифровых платформ и внедрение модели управления на основе данных.

Национальная стратегия развития ИИ на период до 2030 года, утвержденная Указом Президента РФ от 10.10.2019 № 490, закрепляет необходимость формирования у госслужащих компетенций для работы с «доверенными технологиями ИИ» [2].

Концептуальные основы перехода к управлению на основе данных, заложенные в проекте ОГАС под руководством академика В.М. Глушкова в 1960–1970-х годах, обретают новую актуальность в контексте современной стратегии цифровой трансформации [4]. Проект ОГАС предполагал создание автоматизированной системы управления народным хозяйством на принципиально новых кибернетических разработках с тотальной информатизацией всех экономических и управленческих процессов.

Отказ от внедрения проекта ОГАС привел к тому, что задача комплексной информатизации госуправления, поставленная еще в 1960-х годах, продолжает оставаться нерешенной: в деятельности органов власти сохраняется бумажный документооборот, нередко дублирующий электронный. Задача создания единых отраслевых цифровых платформ, закрепленная в Указе № 309, является историческим продолжением и развитием на новом технологическом уровне идеи интеграции информационных потоков для повышения эффективности госуправления.

Согласно исследованию Финансового университета при Правительстве Российской Федерации (январь 2026 г.), в настоящее время сохраняется комплекс системных барьеров, препятствующих эффективному внедрению технологий ИИ в деятельность госучреждений [5]:

1) технологические: значительная часть федеральных и региональных органов власти продолжает функционировать на устаревшем, зачастую несовместимом между собой ПО и оборудовании, что делает интеграцию современных решений в сфере ИИ сложной и дорогостоящей задачей;

2) кадровые: наблюдается острый дефицит компетенций у госслужащих, многие из которых не обладают навыками работы с новыми технологиями. Отсутствие масштабных программ переподготовки и адаптации персонала создает риски скрытого сопротивления изменениям и неэффективного использования внедряемых систем;

3) нормативно-правовые: действующее законодательство не в полной мере регламентирует вопросы ответственности за решения, принятые с использованием ИИ, а также этические аспекты применения соответствующих технологий в госуправлении.

Приказ ФСТЭК № 117, вступающий в силу с 01.03.2026, радикально изменяет модель обеспечения информационной безопасности в государственном секторе через расширение субъектного состава на все информационные системы государственных органов, учреждений и унитарных предприятий и подрядные организации; введение специальных требований к системам с ИИ, включая защиту от сбоев и атак на модели; переход от «бумажной» к операционной безопасности с установлением предельных сроков устранения критических уязвимостей (24 часа) [3].

Параллельно осуществляется разработка рамочного федерального закона «Об искусственном интеллекте», концепция и структура которого обсуждаются в Государственной Думе в январе-феврале 2026 г [7]. Ключевыми принципами будущего регулирования определены технологический суверенитет, безопасность и ответственность. Для государственных информационных систем и объектов критической информационной инфраструктуры предлагается ввести обязательную сертификацию и создать реестр российского и доверенного ИИ.

Опыт Алтайского края демонстрирует эффективный подход к решению кадровой проблемы: в рамках федеральной программы «Профессионалитет» создан Центр цифровизации промышленности на базе Алтайского государственного технического университета. Подготовка специалистов осуществляется с использованием исключительно отечественного программного обеспечения, создана единая доменная среда, объединившая университет и колледжи, обучение прошли 2500 студентов [6].

На основе проведенного анализа представляется целесообразным реализация следующего комплекса мер:

1) Институциональных: преобразование региональных центров компетенций в центры управления безопасностью с наделением их контрольными функциями в отношении подведомственных учреждений; внедрение системы типовых конфигураций безопасности для бюджетных учреждений.

2) Технологических: внедрение систем непрерывного мониторинга (SIEM и EDR) для обеспечения обнаружения атак в реальном времени; обязательное использование специализированных средств защиты для систем с ИИ; создание реестра доверенных решений в сфере ИИ с обязательной сертификацией.

3) Кадровых: запуск общенациональной программы переподготовки для госслужащих на базе ведущих образовательных организаций; обеспечение выполнения кадрового норматива по наличию профильного образования у специалистов по информационной безопасности (не менее 30%); тиражирование опыта формирования команд поддержки изменений на муниципальном уровне.

4) Нормативно-правовых: принятие рамочного федерального закона об ИИ; проведение анализа готовности всех регионов к требованиям Приказа ФСТЭК № 117 с составлением дорожных карт устранения нарушений.

Источники и литература

- 1) Указ Президента Российской Федерации от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»
- 2) Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации».

- 3) Приказ Федеральной службы по техническому и экспортному контролю от 11.04.2025 № 117 «Об утверждении требований о защите информации...».
- 4) Глушкова В.В., Жабин С.А. «ОГАС В.М. Глушкова: История проекта построения информационного общества» // Центр социальных и трудовых исследований. 2016.
- 5) Финансовый университет при Правительстве Российской Федерации: <https://www.fa.ru/university/structure/university/uso/press-service/press-releases/vnedrenie-tekhnologiy-iskusstvennogo-intellekta-v-deyatelnost-gosudarstvennykh-uchrezhdeniy-otsenka->
- 6) РЕД СОФТ: <https://redos.red-soft.ru/about/news/keysy/altayskiy-kray-vybral-resheniya-red-soft-dlya-realizatsii-pervogo-proekta-po-razvitiyu-kadrovogo-pot/>
- 7) Государственная Дума Российской Федерации: <http://duma.gov.ru/news/62564/>.