

Секция «Искусственный интеллект и цифровая трансформация в бизнесе и государственном управлении»

**Цифровая трансформация в контрольно-надзорной деятельности: риск-ориентированный подход.**

**Научный руководитель – Беланов Иван Сергеевич**

*Прошин Игорь Николаевич*

*Студент (магистр)*

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного администрирования (факультет), Москва, Россия

*E-mail: i-proshin2002@mail.ru*

Внедрение информационных технологий (далее - ИТ) в государственные структуры стало неотъемлемой частью цифровой трансформации управления. Использование ИТ повышает доступность и эффективность предоставления государственных услуг, сокращает затраты на техническое обслуживание и упрощает поддержку множества сфер государственного управления. Наибольший прогресс наблюдается в области цифровизации контрольно-надзорной деятельности, где достигнут значительный прогресс в повышении открытости и снижении бюрократических ограничений. Показательно, что средний показатель оценки официального сайта федеральных органов достиг отметки в 20 баллов из 24 возможных в 2022 году [1], что свидетельствует о высоком уровне цифровой готовности органов власти.

Одним из центральных компонентов цифровой трансформации является риск-ориентированный подход (далее - РОП), предусматривающий применение цифровых технологий для анализа рисков и оптимального распределения ресурсов. Современные аналитические инструменты позволяют проводить глубокий анализ больших массивов данных (Big Data), использовать технологии машинного обучения и повышать точность прогнозирования рисков, что делает контрольные мероприятия более эффективными и экономически целесообразными.

Принципиальным отличием цифрового РОП от аналогового является отказ от субъективных экспертных оценок и документально подтвержденных фактов. Цифровой подход основан на обработке огромных объемов данных, что обеспечивает более точное и объективное прогнозирование рисков. Метод дифференциации объектов контроля по уровню риска позволяет повысить продуктивность деятельности контролирующих органов, снизить административные нагрузки и минимизировать вмешательства в деятельность добросовестных хозяйствующих субъектов.

Однако, вместе с положительными аспектами, цифровизация создает новые вызовы. Одна из существенных угроз — увеличение вероятности кибератак и утечек конфиденциальных данных, что негативно сказывается на стабильности системы государственного управления. Несмотря на эти риски, современные технологии, такие как блокчейн и смарт-контракты, могут повысить надежность и прозрачность контрольных мероприятий [15].

Полный переход к цифровому РОП осложнен множеством факторов. Организации сталкиваются с проблемами интеграции устаревших ИТ-инфраструктур, необходимостью замены оборудования и постоянным обновлением программного обеспечения. Создаваемая единая информационная среда и инфраструктура хранения данных повышают контроль и осведомленность проверяющих органов, но вызывают опасения по поводу сохранности персональных данных и предотвращения неправомерных действий.

Интеграция искусственного интеллекта (далее - ИИ) в процессы анализа данных ускоряет выявление правонарушений и позволяет быстро реагировать на потенциальные угрозы. В стране действует государственная стратегия развития искусственного интеллекта до

2030 года, нацеленная на широкое внедрение технологий машинного обучения и самообучающегося ИИ в государственном секторе [13].

Основные достоинства цифрового РОП включают:

- увеличение скорости выявления нарушений;
- оперативное перераспределение ресурсов;
- сокращение числа необязательных проверок;
- улучшение взаимопонимания между органами власти и подконтрольными субъектами.

Несмотря на очевидные преимущества, цифровизация несет риски, связанные с низкой зрелостью имеющихся систем и возможной нестабильностью работы технологий. Необходимость доработки нормативной базы и технических стандартов продолжает оставаться важной задачей.

Таким образом, полная реализация потенциала цифрового РОП возможна только при наличии надежных информационных инфраструктур, оснащенных необходимыми инструментами защиты от несанкционированного доступа, а также наличия ясных и эффективных правовых норм, регулирующих порядок безопасного использования данных.

#### Источники и литература

- 1) Открытость государства и России // Доклад Счетной палаты РФ. – 2023. – С. 17.
- 2) Открытость государства и России // Доклад Счетной палаты РФ. – 2023. – С. 18-19.
- 3) Гагарина Г.Ю., Мирошников С.Н. Некоторые вопросы управления социально-экономическим развитием субъектов Российской Федерации на основе системы стратегического планирования // Управленческое консультирование. 2018. № 12 (120). С. 70-90.
- 4) Яшин, Н. С. Совершенствование риск-ориентированного подхода в системе менеджмента качества в условиях цифровизации / Н. С. Яшин, М. А. Круподерова // Инновационная деятельность. – 2022. – № 4(63). – С. 70-80.
- 5) Ширинкина Е.В. Теория и методология управления человеческим капиталом предприятий в условиях развития цифровой экономики: автореф. дис. . . . д-ра экон. наук. Екатеринбург, 2021. 326 с.
- 6) Яшин, Н. С. Совершенствование риск-ориентированного подхода в системе менеджмента качества в условиях цифровизации / Н. С. Яшин, М. А. Круподерова // Инновационная деятельность. – 2022. – № 4(63). – С. 70-80.
- 7) Мирошников С. Н. Направления развития контрольно-надзорной деятельности: риск-ориентированный подход и цифровизация //Современные подходы к противодействию коррупции: тренды и перспективы. – 2019. – С. 84-88.
- 8) Мирошников С. Н. Направления развития контрольно-надзорной деятельности: риск-ориентированный подход и цифровизация //Современные подходы к противодействию коррупции: тренды и перспективы. – 2019. – С. 84-88.
- 9) Яшин, Н. С. Совершенствование риск-ориентированного подхода в системе менеджмента качества в условиях цифровизации / Н. С. Яшин, М. А. Круподерова // Инновационная деятельность. – 2022. – № 4(63). – С. 70-80.
- 10) Ястребов А. П. Риск-ориентированный подход к управлению качеством разработки корпоративных информационных систем //Моделирование и анализ безопасности и риска в сложных системах. – 2020. – С. 44-45.

- 11) Кунин В. А., Упорова И. В. Риск-ориентированный подход контрольно-надзорной деятельности: международный опыт и особенности применения в российских условиях // Экономика и управление. – 2019. – №. 2 (160). – С. 59-68.
- 12) Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management. Integrating with Strategy and Performance. - URL: <https://www.coso.org/documents/2017-coso-erm-integrating-with-strategy-and-performance-executive-summary.pdf> (датаобращения: 30.12.2024)
- 13) Национальная стратегия развития искусственного интеллекта на период до 2030 года // Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации». – URL: <https://www.garant.ru/products/ipo/prime/doc/72738946/> (дата обращения: 2.01.2025)
- 14) Гоглев Н. Н. и др. Управление рисками с применением современных технологий искусственного интеллекта и анализа больших данных // Цифровая экономика. – 2022. – №. 2. – С. 18.
- 15) Кунин В. А., Упорова И. В. Риск-ориентированный подход контрольно-надзорной деятельности: международный опыт и особенности применения в российских условиях // Экономика и управление. – 2019. – №. 2 (160). – С. 59-68.
- 16) Шичанин, М. А. Особенности применения автоматизированной (цифровой) модели риск-ориентированного подхода к организации публичного финансового контроля / М. А. Шичанин // Традиции и новации в системе современного российского права. – 2022. – С. 369-371.