

РЕГИОНАЛЬНАЯ И ОТРАСЛЕВАЯ ЭКОНОМИКА/REGIONAL AND SECTORAL ECONOMICS

DOI: https://doi.org/10.60797/IRJ.2026.166.84 EDN: TYCUEB

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В АНТИКОРРУПЦИОННОМ КОНТРОЛЕ

Научная статья

Алексеев С.Л.[1, *], Мустафина Г.Г.[2], Кочетков Н.В.[3]
[1] ORCID : 0000-0002-6765-8347;
[2] ORCID : 0009-0009-5785-8511;
[3] ORCID : 0009-0000-9731-5452;
[1, 2] Казанский национальный исследовательский технический университет имени А. Н. Туполева-КАИ, Казань, Российская Федерация
[1] Российская инженерная академия менеджмента и агробизнеса, Пушкино, Российская Федерация
[3] Казанский государственный аграрный университет, Казань, Российская Федерация

* Корреспондирующий автор (tany_1313[at]mail.ru)

Аннотация

В статье рассматриваются перспективы применения искусственного интеллекта в государственном антикоррупционном контроле с акцентом на региональный уровень. Показано, как модели машинного обучения и анализ больших данных усиливают риск-ориентированные проверки закупок, мер поддержки и кадровых процессов, снижая долю рутинных процедур. Обсуждаются архитектуры внедрения (платформенный подход, межведомственные витрины), а также риски — смещения, уязвимость к манипуляциям и требования подотчетности.

В заключении авторы приходят к следующим выводам, что перспективы применения ИИ в государственном антикоррупционном контроле в целом можно оценить как высокие, но зависящие от социальной инфраструктуры данных и подотчетности. Для субъектов Федерации наиболее продуктивным выглядит сочетание федеральной платформы (типовые данные и сервисы) и региональных прикладных сценариев, привязанных к реальным болевым точкам отраслей и муниципалитетов. Если регионы смогут институционализировать управление данными, закрепить процедуры алгоритмической прозрачности и подготовить кадры для работы с риск-сигналами, ИИ станет не разовой инновацией, а устойчивым элементом профилактики коррупции и повышения качества управления.

Ключевые слова: искусственный интеллект, антикоррупционный контроль, экономическая безопасность, государственные закупки, риск-ориентированный подход, региональное управление, большие данные, машинное обучение, выявление сговоров, цифровые платформы, алгоритмическая подотчетность, объяснимость, комплаенс.

PROSPECTS FOR THE USE OF ARTIFICIAL INTELLIGENCE IN ANTI-CORRUPTION MONITORING

Research article

Alexeev S.L.[1, *], Mustafina G.G.[2], Kochetkov N.V.[3]
[1] ORCID : 0000-0002-6765-8347;
[2] ORCID : 0009-0009-5785-8511;
[3] ORCID : 0009-0000-9731-5452;
[1, 2] Kazan National Research Technical University named after A.N. Tupolev-KAI, Kazan, Russian Federation
[1] Russian Engineering Academy of Management and Agribusiness, Pushkino, Russian Federation
[3] Kazan State Agrarian University, Kazan, Russian Federation

* Corresponding author (tany_1313[at]mail.ru)

Abstract

The article examines the prospects for applying artificial intelligence in state anti-corruption control with an emphasis on the regional level. It demonstrates how machine learning models and big data analysis enhance risk-based audits of procurement, support measures and HR processes, thereby reducing the proportion of routine procedures. Introduction architectures (platform-based approach, inter-agency portals) are discussed, as well as risks such as bias, vulnerability to manipulation and accountability requirements.

In conclusion, the authors come to the following observations: the prospects for the application of AI in state anti-corruption control can be assessed as generally high, but dependent on the social infrastructure of data and accountability. For the constituent entities of the Federation, the most productive approach appears to be a combination of a federal platform (standardised data and services) and regional application scenarios linked to the real pain points of sectors and municipalities. If the regions can institutionalise data management, establish procedures for algorithmic transparency and train staff to handle risk signals, AI will become not a one-off innovation, but a sustainable element of corruption prevention and improved governance.

Keywords: artificial intelligence, anti-corruption control, economic security, public procurement, risk-based approach, regional management, big data, machine learning, collusion detection, digital platforms, algorithmic accountability, explainability, compliance.

Введение

Антикоррупционный контроль на государственном уровне все заметнее смещается от модели реагирования на выявленный факт к модели управления рисками — с попыткой заранее распознать узкие места в процедурах и потоках данных, где вероятность злоупотреблений максимальна. Этот сдвиг подпитывается цифровизацией управленческих процессов в рамках парадигмы электронного государства [1], [2]: закупки, бюджетное исполнение, кадровые решения, предоставление мер поддержки и оказание государственных услуг оставляют цифровые следы, которые можно сопоставлять между собой и проверять на аномалии. В российских условиях такой поворот особенно важен на уровне субъектов Федерации, где значительная часть решений принимается ближе к получателю ресурсов и услуг, а разнообразие отраслей и муниципальных практик резко повышает неоднородность рисков [3].

Методы и принципы исследования

Базовый метод — компаративный анализ международных и российских подходов к применению искусственного интеллекта (ИИ) в антикоррупционной деятельности и смежных контрольно-надзорных практиках (закупки, финансовый контроль, комплаенс). Сопоставление выполнялось по функциональным блокам антикоррупционного цикла: профилактика и управление рисками, выявление и первичная верификация сигналов, документирование и доказательность, меры реагирования, а также организационная архитектура обмена данными между участниками контроля на региональном уровне. Для сопоставимости использовались единые критерии сравнения: степень допустимой автоматизации и роль человека в контуре («human-in-the-loop»), требования к объяснимости и воспроизводимости выводов, тип используемых данных (реестры, транзакции, тексты, графы связей), интеграция с действующими государственными системами и реестрами (включая ЕИС в сфере закупок), режимы доступа к сведениям и ограничения обработки персональных данных.

Второй опорный метод — нормативно-догматический анализ. Он применялся для реконструкции правового статуса «риск-сигнала», формируемого аналитическими инструментами, и для разграничения юридически значимых решений и вспомогательных процедур аналитического сопровождения. В рамках данного подхода анализировались базовые требования российского регулирования к контрольно-надзорным процессам и к обработке информации: целевое ограничение использования данных, требования информационной безопасности и защиты персональных сведений, допустимость использования результатов автоматизированного анализа при планировании и проведении контрольных мероприятий, а также вопросы распределения ответственности между владельцем данных, разработчиком модели и уполномоченным должностным лицом, принимающим решение.

Третий метод — институциональный и процессный анализ, позволяющий рассматривать ИИ не как автономный продукт, а как элемент управленческого контура регионального контроля. В качестве аналитической рамки использовалась логика «данные — модель — риск-сигнал — проверка — решение — обратная связь», где на каждом этапе фиксируются входы и выходы, роли участников (оператор данных, аналитический центр, контролер, ИБ-служба), а также контрольные процедуры (журналирование, версионирование моделей, регламенты эскалации). Это обеспечивало воспроизводимость выводов в смысле возможности повторить рассуждение и проверить применимость предложенных принципов к различным региональным организационным конфигурациям.

Дополнительно применялись методы контент-анализа и функционального моделирования. Контент-анализ использовался для систематизации типовых сценариев применения ИИ (ранжирование объектов по риску, выявление аномалий и сговоров, поиск связей и аффилированности, обработка текстов и жалоб, сопоставление реестров), что отражено в классификации сценариев (табл. 1), а также для выделения устойчивых «узких мест» внедрения (дисциплина данных, процедурная совместимость, риск ошибок и ложных срабатываний), обобщенных в виде матрицы рисков (табл. 2). Функциональное моделирование применялось для описания типовой схемы встраивания ИИ в регламенты контроля: результат алгоритма трактуется как подсказка и основание для постановки проверяемой гипотезы, а не как решение по существу.

Ключевые принципы исследования включают: принцип правовой нейтральности модели (алгоритм не подменяет юридическую квалификацию и дискрецию должностного лица), принцип проверяемости (каждый сигнал привязан к конкретным полям данных и документам), принцип минимизации и целевого ограничения обработки сведений, принцип подотчетности и аудируемости (журналирование, контроль доступа, сохранение версий моделей и правил), принцип управляемой адаптации (обновление правил и моделей при изменении практик и рисков), а также принцип институциональной совместимости (встраивание в существующие полномочия и процедуры без размывания ответственности между участниками).

Основные результаты

Мировые тенденции наиболее наглядно проявляются в сфере публичных закупок, где накоплены стандартизированные данные о процедурах, участниках и результатах торгов. Исследования по «красным флагам» показывают, что многие коррупционные и квазикоррупционные практики оставляют измеримые следы: нетипичная длительность процедур, ограниченная конкуренция, повторяемость победителей, специфика критериев оценки и дробление контрактов. На практике это позволяет строить модели, которые не доказывают злоупотребление, но стабильно выделяют подозрительные торги для последующего аудита и разбирательства [4].

Эта линия поддерживается и обзорными работами, где фиксируется быстрый рост прикладных подходов к выявлению мошенничества и коррупции в закупках: от классических правил и индикаторов до ансамблевых моделей, графовой аналитики и гибридов «правила + машинное обучение». Важное наблюдение состоит в том, что технологическая сложность сама по себе не гарантирует лучшего результата: выигрыш дают правильно подобранные признаки риска, прозрачная интерпретация для аудитора и устойчивость модели к изменениям в регуляторике и поведении участников [5].

Отдельный класс задач — выявление сговоров и картельных паттернов. Здесь ценность ИИ заключается в способности работать с ограниченной информацией, когда у контролера есть лишь итоговые параметры торгов, а детальная «цифровая криминалистика» недоступна. Алгоритмы, комбинирующие теоретические свойства аукционного поведения и методы классификации, позволяют формировать вероятностные сигналы о возможном сговоре и тем самым усиливать конкуренционную политику и антикоррупционный контроль без тотального «ручного» просмотра массивов процедур [6].

Российским примером масштабного внедрения аналитических инструментов для выявления сговоров является государственная информационная система ФАС России «Антикартель»: в публичных материалах ФАС указывается, что система в автоматизированном режиме анализирует данные ЕИС в сфере закупок и ГИС «Торги», использует элементы машинного обучения и обеспечивает ежедневный анализ 100% закупочных процедур с формированием риск-сигналов для последующей проверки. Концептуально эта линия развивалась на базе более раннего скрининговго сервиса («Большой цифровой кот»/«АнтиКартель»), где скоринговые индексы строились на структурных и поведенческих признаках участников торгов и параметрах, извлекаемых из ЕИС и данных электронных площадок [7], [8].

В странах с ограниченными ресурсами контроля акцент все чаще делается на инструментах приоритизации: не «найти все», а «выбрать то, что стоит проверки в первую очередь». Примером служат решения, где машинное обучение используется для раннего выявления неэффективностей (перерасход, срыв сроков), а параллельно строятся индексы риска по процессным нарушениям, опирающиеся на открытые данные. В таких архитектурах ключевым продуктом становится не модель как таковая, а понятный интерфейс для инспектора: объяснимые признаки, логику ранжирования и воспроизводимую процедуру принятия решения о начале проверки [9].

За рамками закупок ИИ активно развивается в сфере аудита и бюджетного контроля. Особенно показательны эмпирические работы, где прогнозный показатель коррупции используется для более эффективного таргетирования проверок: при одинаковом объеме аудита «машинно-направленный» выбор объектов способен обнаруживать существенно больше нарушений, чем случайная выборка. Концептуально это переводит контроль из режима «проверяем все понемногу» в режим «проверяем глубже там, где вероятнее проблема», что критично для регионов с ограниченным кадровым и финансовым ресурсом контрольных органов [10].

Для высших органов внешнего финансового контроля (и аналогичных институтов) ИИ рассматривается как средство повышения охвата и качества аналитики: от классификации транзакций по риску до выявления завышения цен и нетипичных платежных цепочек. При этом профессиональное сообщество аудиторов подчеркивает, что внедрение требует новых компетенций и стандартизации [11]: модели должны сопровождаться документацией, тестами устойчивости и ясным распределением ответственности между разработчиком, владельцем процесса и аудитором [12].

В контуре внешнего государственного аудита также формируется российский опыт цифровой трансформации. Примером служит развитие цифровых рабочих мест и аналитических витрин в Счетной палате РФ (АРМ «Цифровой инспектор» как система «единого окна» для сбора, обработки и визуализации данных, а также сокращения трудозатрат инспекторского состава). Отчет Счетной палаты о работе в 2024 г. фиксирует использование аналитических систем и инструментов ИИ и приводит суммарные результаты: экономический эффект 148,9 млрд руб., включая возврат 95,9 млрд руб. в бюджеты всех уровней, что показывает масштаб задач, где риск-ориентированная аналитика может усиливать традиционный аудит [13], [14].

Усиление аналитических возможностей неизбежно поднимает вопрос доверия к алгоритму и его правовой легитимности. В зарубежной регуляторике и практике управления ИИ заметен переход к «обязательствам оценки» — режимам, где применение алгоритмов в чувствительных доменах сопровождается предварительными и последующими оценками воздействия, раскрытием ключевых параметров и процедурами контроля смещений. Для антикоррупционного контроля это особенно важно: чем выше ставка решения, тем сильнее требования к объяснимости, независимому аудиту модели и возможности оспаривания результата [15].

Российская специфика состоит в одновременном наличии крупных государственных цифровых контуров и выраженной региональной неоднородности их использования. С одной стороны, базовые реестры и платформы формируют потенциал «сквозной» аналитики; с другой — качество первичных данных, зрелость процессов и дисциплина заполнения различаются между ведомствами, муниципалитетами и отраслевыми сегментами. В этой ситуации практический эффект ИИ почти всегда зависит от того, удалось ли сформировать единые справочники, идентификаторы и правила сопоставления (например, для участников закупок, бенефициаров, объектов имущества, мер поддержки), а также от качества последующего мониторинга применения стандартных процедур электронных проверок [16].

Потенциал подобных подходов подтверждается и корпоративной практикой, где антифрод-системы работают в режиме реального времени, обрабатывая массовые потоки операций и формируя риск-скоринг для экспертной проверки. По данным публичных сообщений, антифрод-платформа Сбера на основе ИИ помогла в 2025 г. предотвратить потери клиентов более чем на 360 млрд руб.; в качестве одной из технологических характеристик отраслевой практики упоминается обработка порядка 150 тыс. транзакций в секунду при миллисекундных задержках ответа. Близкая по логике аналитика применима к региональным закупкам и, в частности, к капитальному строительству: корпоративные кейсы BI-аналитики демонстрируют, как дашборды и контроль аномалий позволяют выявлять переплаты, обход конкурентных процедур, устойчивые связки сотрудников и поставщиков и другие маркеры злоупотреблений, формируя основу для адресных проверок [17], [18], [19].

В российском дискурсе все чаще обсуждается, что государственные антикоррупционные задачи требуют не «универсального ИИ», а набора специализированных сервисов, встроенных в правоприменение: мониторинг конфликта интересов, сопоставление деклараций с косвенными признаками благосостояния, выявление

аффилированности поставщиков и заказчиков, анализ обращений и сообщений о нарушениях. Важно, что эти сценарии должны быть технологически реализуемы в регионах: через типовые модули, унифицированные требования к данным и методические рекомендации по интерпретации результатов [20].

Одним из направлений, где сходятся технологические и правовые вопросы, является формирование государственных информационных систем, ориентированных на межведомственный сбор и анализ данных по соблюдению антикоррупционных ограничений. Такие решения усиливают потенциал сквозного сопоставления сведений и снижают зависимость от ручной проверки. Однако именно здесь наиболее остро проявляются вопросы допустимости, полноты и качества данных, а также порядка использования результатов аналитики в дисциплинарных и контрольных процедурах [21].

В прикладном плане ИИ может давать на региональном уровне несколько устойчивых преимуществ. Во-первых, повышается масштабируемость контроля: алгоритмы способны ежедневно просматривать массивы процедур, которые физически невозможно анализировать вручную. Во-вторых, ускоряется цикл реакции: риск-сигнал формируется вблизи момента принятия решения, а не постфактум. В-третьих, становится возможным переход от точечных проверок к мониторингу системных причин (например, типовые схемы дробления закупок или повторяющиеся исключения из конкурентных процедур). Наконец, появляется более управляемая воспроизводимость контроля: одинаковые правила отбора и ранжирования применяются к сопоставимым данным [22].

Модельный (анонимизированный) пример регионального пилота: в одном из субъектов РФ при органе внутреннего финансового контроля развертывается витрина данных закупок, ежедневно забирающая из ЕИС планы-графики, извещения, протоколы и сведения о контрактах и обогащающая их данными регионального казначейского сопровождения и реестров контрагентов. На витрине построен риск-скоринг по типовым «красным флагам» (аномальная цена и отклонение от рыночных бенчмарков, дробление лотов, повторяемость победителей, минимальное число участников, короткие сроки и т.п.). Результат модели используется как сигнал для камеральной проверки: проверяющий получает ранжирование процедур и пояснимые признаки, что снижает трудоемкость первичного отбора и увеличивает долю результативных проверок за счет концентрации на верхнем квантиле риска.

Типовые сценарии применения ИИ в региональном контуре удобно рассматривать через связку «объект контроля — данные — аналитический метод — управленческое действие». На практике это позволяет заранее решить главный вопрос внедрения: что именно должно измениться в работе контрольного органа после появления риск-сигнала. Ниже в таблице 1 приведена укрупненная матрица таких сценариев, ориентированная на задачи субъектов Федерации и муниципального уровня.

Таблица 1 - Задачи антикоррупционного контроля и ИИ-инструменты на региональном уровне

DOI: https://doi.org/10.60797/IRJ.2026.166.84.1

Объект контроля	Тип данных (пример)	ИИ-инструмент	Ожидаемый эффект	Ключевые условия для региона
Госзакупки и закупки МУП/ГУП	ЕИС/региональные подсистемы; контракты; участники; цены; сроки	Риск-скоринг, аномалии, граф связей, выявление сговоров	Приоритезация проверок; раннее предупреждение	Справочники, идентификаторы участников, доступ к первичному протоколу
Субсидии и меры поддержки	Заявки; реестры получателей; параметры отбора; взаимосвязи аффилированности	Классификация риска, контроль дублирования, выявление «клонов»	Снижение злоупотреблений и повторного финансирования	Интеграция реестров, качество данных о бенефициарах
Кадровые решения и конфликт интересов	Данные о должностях; родственники; контрагенты; имущественные связи	Граф-аналитика, поиск аффилированности, правила + ML	Выявление скрытых конфликтов, таргетинг проверок	Правовые основания доступа; корректная модель согласий/допусков
Обращения граждан и сообщения о нарушениях	Тексты, вложения, маршрутизация, сроки ответа	NLP-классификация тем; кластеризация; извлечение сущностей	Быстрее обработка, лучше маршрутизация, выявление серий	Единый реестр обращений; обучение на размеченных данных
Бюджетное исполнение и платежи	Транзакции; назначения платежей; исполнители; цепочки платежей	Аномалии, профили транзакций, группировка по паттернам	Сигналы для внутреннего контроля и КСП	Доступ к детализации; единые коды операций и контрагентов

Критически важно, что почти все сценарии требуют не столько особо сложных математических моделей, сколько семантической совместимости данных. Для регионов это означает работу с мастер-данными и унификацией атрибутов: единые идентификаторы организаций и физических лиц, нормализация адресов, связка объектов имущества и правообладателей, согласованные отраслевые справочники по видам работ и услуг. Без такого слоя интероперабельности любые ИИ-модели будут лишь тиражировать ошибки исходных реестров и создавать ложные срабатывания, обесценивающие доверие к системе.

Если рассматривать закупки как ключевой узел региональных коррупционных рисков, то важны два класса аналитики: индикаторы процесса (что происходило на этапе выбора способа закупки, подготовки документации, допуска заявок) и индикаторы результата (цена, сроки, качество исполнения). Практика показывает, что цифровые методы позволяют системно фиксировать нетипичные сочетания признаков. Важный вывод для регионов состоит в том, что такие индикаторы должны быть частью методики контроля: формироваться автоматически, документироваться и использоваться как повод для углубленной проверки [23].

Секторальные приоритеты регионов позволяют довольно быстро выбрать сценарии с максимальной отдачей. В капитальном строительстве и ремонтах ИИ-подходы применимы для выявления аномалий в сметах, сопоставления цен на материалы и работы по сопоставимым объектам, контроля цепочек субподрядов и анализа изменений контрактов по дополнительным соглашениям. В здравоохранении и социальной сфере перспективны модели, которые сопоставляют закупочные цены и объемы с нормативами потребления и статистикой оказания услуг, выявляя нетипичные «провалы» конкуренции и повторяемость поставщиков. В земельно-имущественных отношениях графовая аналитика помогает обнаруживать пересечение бенефициаров между подрядчиками, получателями льгот и должностными лицами, а также аномальные траектории смены собственников и арендаторов [24].

Региональный уровень также удобен для трансляции организационных новаций. Во многих субъектах Федерации контуры контроля распределены между финансовыми органами, отраслевыми ведомствами, контрольно-счетными органами, органами внутреннего финансового аудита, а также взаимодействуют с прокуратурой и антимонопольными структурами. ИИ-инструменты способны сыграть роль «общего языка» между ними, если результаты представлены как стандартизированные риск-карточки: источник данных, признаки, уровень риска, объяснение, история изменений и статус реакции. Тогда обмен сигналами становится процедурным, а не ситуативным, что особенно важно для муниципального уровня, где кадровая и методическая устойчивость ниже.

Наконец, отдельного внимания заслуживает вопрос устойчивости к дрейфу - когда изменяются либо процессы (новые способы закупок, измененные сроки и требования), либо поведение участников (адаптация к индикаторам риска), либо нормативная база. Для регионов рационально закладывать цикл пересмотра моделей и признаков риска не реже одного раза в год, а для наиболее чувствительных сценариев — ежеквартально, сопровождая это анализом ложных срабатываний и упущенных случаев. Такая практика требует дисциплины, но она же обеспечивает управляемость и юридическую защищенность: любой риск-сигнал можно восстановить, объяснить и сопоставить с версией модели, действовавшей на момент формирования рекомендации.

Второй критический пласт — организационная архитектура внедрения. В большинстве регионов затруднительно воспроизвести «в миниатюре» федеральные центры компетенций по данным и ИИ. Поэтому реалистична модель, где ядро данных и типовые сервисы (витрины, словари, базовые модели) создаются как федерально-региональная платформа, а субъект Федерации развивает прикладные сценарии, адаптируя признаки риска под местные отрасли и практику контрольно-надзорных органов. Платформенный подход снижает барьеры входа, обеспечивает сопоставимость показателей между регионами и одновременно позволяет учитывать региональные особенности (структура контрактов, отраслевые приоритеты, зрелость цифровых контуров).

Содержательно зрелая система ИИ-контроля строится как цепочка: данные → модели → управленческое действие → обратная связь. Региону необходимо заранее определить источники корректной информации, порядок исправления ошибок (data governance) и ответственных за витрины данных. Затем — выбрать модели, которые объяснимы инспектору и устойчивы к изменениям процессов. После этого — встроить результат в регламент: кто получает сигнал, какие статусы устанавливаются, какие документы формируются, как фиксируется мотивировка. И, наконец, организовать обратную связь: результат проверки возвращается в набор данных, чтобы уточнять признаки риска и отслеживать «дрейф» модели.

На этом этапе возникает важная развилка между полной автоматизацией и «человеком в контуре». Для антикоррупционного контроля в регионах практичнее второй вариант: модель ранжирует и объясняет, но решение о запуске проверки принимает уполномоченное лицо, фиксируя основания. Это снижает риск неправомерного вмешательства в права проверяемых и одновременно делает алгоритм инструментом повышения качества управленческого выбора. Такой дизайн также помогает справиться с неизбежными ошибками первого периода, когда модели учатся на исторических данных, а процессы и законодательство продолжают меняться.

Отдельно следует отметить потенциал генеративных моделей (включая большие языковые модели) как инструмента производительности, а не как детектора коррупции. На региональном уровне они могут ускорять подготовку справок, обобщение материалов проверок, первичную классификацию обращений и поиск по массивам регламентов и контрактной документации. Однако их использование требует строгих ограничений: запрет на автоматическую выдачу юридических выводов, контроль утечек данных, журналирование запросов и обязательную верификацию результатов человеком. Иначе выигрыши времени легко будут нивелированы репутационными и правовыми рисками.

Риск-профилирование и автоматизация не являются нейтральными: они меняют поведение участников и распределение внимания контрольных органов. Поэтому встроенная подотчетность должна проектироваться одновременно с моделью. Практически это означает набор процедур контроля качества, прозрачности и устойчивости,

которые могут быть стандартизированы для регионов и применяться как к собственным моделям субъекта Федерации, так и к решениям федеральной платформы (см. таблицу 2).

Таблица 2 - Риски применения ИИ и меры управленческого контроля

DOI: https://doi.org/10.60797/IRJ.2026.166.84.2

Риск	Как проявляется	Мера управленческого контроля
Смещения и неполнота данных	модель «наказывает» отрасли/муниципалитеты с более полной отчетностью	контроль качества, стратификация выборок, тесты справедливости и дрейфа
Манипулирование (gaming)	участники подстраивают поведение под индикаторы, не снижая реальный риск	ротация признаков, сочетание правил и ML, мониторинг адаптивного поведения
«Черный ящик»	инспектор не может объяснить, почему объект в приоритете	использование объяснимых моделей, карточки признаков, протоколы решений
Ложные срабатывания	перегруз контрольного органа, падение доверия	калибровка порогов, пилоты, контроль полезности сигнала (audit yield)
Риски персональных данных	нецелевой доступ, утечка, «избыточное» профилирование	минимизация данных, разграничение доступа, журналирование, DPIA-подобные процедуры
Зависимость от поставщика	невозможность смены решения без потери модели/данных	контрактные требования к переносимости, открытые форматы, независимый аудит

Оценка эффективности ИИ в антикоррупционном контроле требует корректных метрик. Точность модели в статистическом смысле важна, но недостаточна: контрольному органу нужны показатели полезности сигнала (доля результативных проверок среди рекомендованных), экономия времени на анализе типовых процедур, сокращение срока выявления рисков, а также воспроизводимость решений при смене персонала. Для регионов дополнительно значима сопоставимость: единые подходы к расчёту метрик позволяют видеть, где проблема в данных, где — в процессах, а где — в отраслевой специфике.

Обсуждение

Оценка эффективности ИИ в антикоррупционном контроле требует корректных метрик. Точность модели в статистическом смысле важна, но недостаточна: контрольному органу нужны показатели полезности сигнала (доля результативных проверок среди рекомендованных), экономия времени на анализе типовых процедур, сокращение срока выявления рисков, а также воспроизводимость решений при смене персонала. Для регионов дополнительно значима сопоставимость: единые подходы к расчёту метрик позволяют видеть, где проблема в данных, где — в процессах, а где — в отраслевой специфике.

В организационном плане внедрение целесообразно вести по логике «коридора доверия»: сначала — вспомогательные сценарии с низкими ставками (маршрутизация обращений, поиск дубликатов, подсветка нетипичных параметров контрактов), затем — сценарии приоритизации проверок, и только после накопления практики — более сложные случаи, затрагивающие персональные данные и конфликты интересов. Такой порядок позволяет сформировать у региональных контрольных команд навыки работы с данными и интерпретации сигналов, а также выстроить коммуникацию с прокуратурой, КСП и отраслевыми ведомствами вокруг единых критериев риска.

В долгосрочной перспективе ключевое преимущество ИИ на региональном уровне связано с интеграцией разрозненных контуров контроля. Там, где сегодня существуют отдельные проверки закупок, субсидий и кадровых решений, платформа данных и граф связей может выявлять сквозные схемы: повторяемость контрагентов, пересечение бенефициаров, совпадение адресов и контактных данных, переход сотрудников между связанными организациями. Именно такой междоменный анализ позволяет переходить от локального устранения нарушений к профилактике — изменению правил и процедур так, чтобы риск-схемы становились дороже и заметнее.

Для регионов принципиально важно заранее определить границы использования результатов ИИ в юридически значимых действиях. В дисциплинарных, контрольных и процессуальных контекстах риск-сигнал корректно трактовать как основание для начала проверки и постановки вопросов, а не как доказательство. Отсюда вытекает практическое требование: каждый вывод модели должен сопровождаться трассировкой (какие данные использовались, какая версия модели применялась, какие признаки повлияли на итоговый балл), а также возможностью независимой перепроверки по первичным документам. Такой подход одновременно защищает права проверяемых и повышает качество управленческого решения, поскольку переводит ИИ-подсказку в формат проверяемого и оспоримого аргумента.

Наряду с технологической и организационной составляющими требуется институционализация — появление понятных ролей и процедур управления моделями. Для регионов это может быть закреплено через проектный офис (или межведомственную рабочую группу) по аналитике коррупционных рисков, который утверждает перечень приоритетных сценариев, поддерживает единые словари признаков, согласует пороги срабатывания, контролирует качество данных и организует независимую проверку моделей. Важный принцип — разделение функций: разработка и сопровождение модели не должны совпадать с функцией принятия окончательного решения по конкретному делу. Такая конструкция снижает риск конфликта интересов и повышает доверие к цифровому контролю со стороны ведомств, муниципалитетов и граждан.

Заключение

Перспективы применения ИИ в государственном антикоррупционном контроле в целом можно оценить как высокие, но зависящие от социальной инфраструктуры данных и подотчетности. Для субъектов Федерации наиболее продуктивным выглядит сочетание федеральной платформы (типовые данные и сервисы) и региональных прикладных сценариев, привязанных к реальным болевым точкам отраслей и муниципалитетов. Если регионы смогут институционализировать управление данными, закрепить процедуры алгоритмической прозрачности и подготовить кадры для работы с риск-сигналами, ИИ станет не разовой инновацией, а устойчивым элементом профилактики коррупции и повышения качества управления.

Благодарности

Авторы статьи выражают слова искренней благодарности Управлению Раиса Республики Татарстан по антикоррупционной политике.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Acknowledgement

The authors express their sincere gratitude to the Anti-Corruption Policy Rais of the Republic of Tatarstan.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Алякин А.А. Функционирование единой информационной системы по техническому регулированию на базе парадигмы электронного государства / А. А. Алякин, А. В. Докукин, И. Б. Перепелкин // Транспортное дело России. — 2009. — № 3. — С. 153–155. — EDN: KUVBUH.

2. Ломакин М.И. Функции единой информационной системы по техническому регулированию в рамках концепции электронного государства / М.И. Ломакин, А.В. Докукин // Перспективы науки. — 2011. — № 12 (27). — С. 230–233. — EDN: PBAFMV.

3. Shamekhina E.V. Digital transformation of anti-corruption: a retrospective and development prospects / E.V. Shamekhina // National Security/nota bene. — 2023. — № 4. — P. 52–60.

4. Decarolis F. Corruption red flags in public procurement: new evidence from Italian calls for tenders / F. Decarolis, C. Giorgiantonio // EPJ Data Science. — 2022. — Vol. 11. — № 1. — Art. 16.

5. Schneider dos Santos E. Detection of fraud in public procurement using data-driven methods: a systematic mapping study / E. Schneider dos Santos [et al.] // EPJ Data Science. — 2025. — Vol. 14. — Art. 52.

6. Tas B.K.O. A machine learning approach to detect collusion in public procurement with limited information / B.K.O. Tas // Journal of Computational Social Science. — 2024. — Vol. 7. — № 2. — P. 1913–1935. — DOI: 10.1007/s42001-024-00293-4.

7. ФАС России. Президент России подписал закон о создании ГИС «Антикартель»: Информация ФАС России от 25.06.2025. — URL: https://storage.consultant.ru/ondb/attachments/202506/25/iddoc_295176_idnews_63118_Informatsija_FAS_Rossii_ot_25_06_2025_1Sc.pdf (дата обращения: 26.02.2026).

8. Тесленко А.В. Большой цифровой кот: промежуточные итоги и перспективы: презентация / А.В. Тесленко. — URL: https://ilns.ranepa.ru/files/konferentsii/bolshoy-tsifrovoy-kot.pdf (дата обращения: 26.02.2026).

9. Salazar A. VigIA: prioritizing public procurement oversight with machine learning models and risk indices / A. Salazar, J.F. Pérez, J. Gallego // Data & Policy. — 2024. — Vol. 6. — Art. e75. — DOI: 10.1017/dap.2024.83.

10. Ash E. A Machine Learning Approach to Analyze and Support Anticorruption Policy / E. Ash, S. Galletta, T. Giommoni // American Economic Journal: Economic Policy. — 2025. — Vol. 17. — № 2. — P. 162–193. — DOI: 10.1257/pol.20210618.

11. Ломакин М.И. Методологические проблемы стандартизации в условиях развития цифровой экономики / М.И. Ломакин, А.В. Докукин, А.П. Шалаев // Стандарты и качество. — 2018. — № 11. — С. 80–83. — EDN: YMIABN.

12. Genaro-Moya D Artificial Intelligence and Public Sector Auditing: Challenges and Opportunities for Supreme Audit Institutions / D. Genaro-Moya, A.M. López-Hernández, M. Godz // World. — 2025. — Vol. 6. — № 2. — Art. 78. — DOI: 10.3390/world6020078.

13. Чистобородов А.Г. Создание АРМ «Цифровой инспектор» Счетной палаты Российской Федерации: презентация / А.Г. Чистобородов. — URL: https://sp03.ru/docfiles/file838_828.pdf (дата обращения: 26.02.2026).

14. Счетная палата Российской Федерации. Итоги работы Счетной палаты в 2024 году. — Москва, 2025. — 134 с. — URL: https://ach.gov.ru/upload/iblock/d34/r9je39e5z05455o9ksar608z6j12jwad.pdf (дата обращения: 26.02.2026).

15. Oduro S. Obligations to assess: Recent trends in AI accountability regulations / S. Oduro, E. Moss, J. Metcalf // Patterns. — 2022. — Vol. 3. — № 11. — Art. 100608.

16. Докукин А.В. Повышение качества информационного обеспечения мониторинга правотворчества и правоприменения / А.В. Докукин // Информационно-экономические аспекты стандартизации и технического регулирования. — 2013. — № 6 (16). — С. 10. — EDN: TNYISR.

17. В Сбере рассказали, как помогли россиянам уберечь от мошенников более 360 млрд рублей // Банки.ру. — 2026. — URL: https://www.banki.ru/news/lenta/?id=11020738 (дата обращения: 26.02.2026).

18. ИИ против мошенников: как антифрод-системы учатся распознавать угрозы // РБК Тренды. — 2025. — URL: https://trends.rbc.ru/trends/industry/679f706c9a7947e64f4f0d30 (дата обращения: 26.02.2026).

19. Волков А. У нас воруют: как BI помогает остановить коррупцию в строительстве / А. Волков // Хабр. — 2025. — URL: https://habr.com/ru/companies/cynteka/articles/945248/ (дата обращения: 26.02.2026).

20. Крылова Д.В. Использование искусственного интеллекта в вопросах выявления и противодействия коррупции: обзор международного опыта / Д.В. Крылова, А.А. Максименко // Государственное управление. Электронный вестник. — 2021. — № 84. — С. 241–255. — DOI: 10.24412/2070-1381-2021-84-241-255.

21. Абакумова Е.Б. Правовой режим применения цифровых технологий и искусственного интеллекта в антикоррупционной деятельности государства. Часть 2 / Е.Б. Абакумова // Право и государство: теория и практика. — 2025. — № 9. — С. 133–136. — DOI: 10.61726/6246.2025.45.34.001.

22. Аносов А.В. Технологии искусственного интеллекта в системе противодействия коррупции / А.В. Аносов // Право и государство: теория и практика. — 2024. — № 12 (240). — С. 541–543. — DOI: 10.47643/1815-1337_2024_12_541.

23. Басангов Д.А. Особенности использования цифровых технологий в выявлении коррупционных признаков публичных закупок / Д.А. Басангов // Образование и право. — 2025. — № 1. — С. 415–421. — DOI: 10.24412/2076-1503-2025-1-415-421.

24. Алексеев С.Л. Экономико-антикоррупционные проблемы управления финансовой устойчивостью акторов экономики (вопросы теории и практики) / С.Л. Алексеев, Н.М. Якушкин, А.А. Аюпов [и др.]. — Казань: Татарский институт переподготовки кадров агробизнеса, 2025. — 208 с. — EDN: TBSEGU.

Список литературы на английском языке / References in English

1. Alyakin A.A. Funktsionirovanie yedinoi informatsionnoi sistemi po tekhnicheskomu regulirovaniyu na baze paradigmi elektronnogo gosudarstva [Functioning of a unified information system for technical regulation based on the e-government paradigm] / A. A. Alyakin, A. V. Dokukin, I. B. Perepelkin // Transportnoe delo Rossii [Transport business of Russia]. — 2009. — № 3. — P. 153–155. — EDN: KUVBUH. [in Russian]

2. Lomakin M.I. Funktsii yedinoi informatsionnoi sistemi po tekhnicheskomu regulirovaniyu v ramkakh kontseptsii elektronnogo gosudarstva [Functions of the unified information system for technical regulation within the framework of the concept of electronic government] / M.I. Lomakin, A.V. Dokukin // Perspektivi nauki [Prospects of Science]. — 2011. — № 12 (27). — P. 230–233. — EDN: PBAFMV. [in Russian]

3. Shamekhina E.V. Digital transformation of anti-corruption: a retrospective and development prospects / E.V. Shamekhina // National Security/nota bene. — 2023. — № 4. — P. 52–60.

4. Decarolis F. Corruption red flags in public procurement: new evidence from Italian calls for tenders / F. Decarolis, C. Giorgiantonio // EPJ Data Science. — 2022. — Vol. 11. — № 1. — Art. 16.

5. Schneider dos Santos E. Detection of fraud in public procurement using data-driven methods: a systematic mapping study / E. Schneider dos Santos [et al.] // EPJ Data Science. — 2025. — Vol. 14. — Art. 52.

6. Tas B.K.O. A machine learning approach to detect collusion in public procurement with limited information / B.K.O. Tas // Journal of Computational Social Science. — 2024. — Vol. 7. — № 2. — P. 1913–1935. — DOI: 10.1007/s42001-024-00293-4.

7. FAS Rossii. Prezident Rossii podpisal zakon o sozdanii GIS «Antikartel»: Informatsiya FAS Rossii ot 25.06.2025 [Federal Antimonopoly Service of Russia (FAS). The President of Russia signed the law establishing the state information system “Antikartel”. Information note, 25 June 2025]. — URL: https://storage.consultant.ru/ondb/attachments/202506/25/iddoc_295176_idnews_63118_Informatsija_FAS_Rossii_ot_25_06_2025_1Sc.pdf (accessed: 26.02.2026). [in Russian]

8. Teslenko A.V. Bolshoi tsifrovoi kot: promezhutochnie itogi i perspektivi: prezentatsiya [Big Digital Cat: intermediate results and prospects. Presentation] / A.V. Teslenko. — URL: https://ilns.ranepa.ru/files/konferentsii/bolshoy-tsifrovoy-kot.pdf (accessed: 26.02.2026). [in Russian]

9. Salazar A. VigIA: prioritizing public procurement oversight with machine learning models and risk indices / A. Salazar, J.F. Pérez, J. Gallego // Data & Policy. — 2024. — Vol. 6. — Art. e75. — DOI: 10.1017/dap.2024.83.

10. Ash E. A Machine Learning Approach to Analyze and Support Anticorruption Policy / E. Ash, S. Galletta, T. Giommoni // American Economic Journal: Economic Policy. — 2025. — Vol. 17. — № 2. — P. 162–193. — DOI: 10.1257/pol.20210618.

11. Lomakin M.I. Metodologicheskie problemi standartizatsii v usloviyakh razvitiya tsifrovoi ekonomiki [Methodological problems of standardization in the context of the development of the digital economy] / M.I. Lomakin, A.V. Dokukin, A.P. Shalaev // Standarti i kachestvo [Standards and quality]. — 2018. — № 11. — P. 80–83. — EDN: YMIABN. [in Russian]

12. Genaro-Moya D Artificial Intelligence and Public Sector Auditing: Challenges and Opportunities for Supreme Audit Institutions / D. Genaro-Moya, A.M. López-Hernández, M. Godz // World. — 2025. — Vol. 6. — № 2. — Art. 78. — DOI: 10.3390/world6020078.

13. Chistoborodov A.G. Sozdanie ARM «Tsifrovoi inspektor» Schetnoi palati Rossiiskoi Federatsii: prezentatsiya [Creation of the automated workplace “Digital Inspector” of the Accounts Chamber of the Russian Federation. Presentation] / A.G. Chistoborodov. — URL: https://sp03.ru/docfiles/file838_828.pdf (accessed: 26.02.2026). [in Russian]

14. Schetnaya palata Rossiiskoi Federatsii. Itogi raboti Schetnoi palati v 2024 godu [Accounts Chamber of the Russian Federation. Results of the Accounts Chamber’s work in 2024]. — Moscow, 2025. — 134 p. — URL: https://ach.gov.ru/upload/iblock/d34/r9je39e5z05455o9ksar608z6j12jwad.pdf (accessed: 26.02.2026). [in Russian]

15. Oduro S. Obligations to assess: Recent trends in AI accountability regulations / S. Oduro, E. Moss, J. Metcalf // Patterns. — 2022. — Vol. 3. — № 11. — Art. 100608.

16. Dokukin A.V. Povishenie kachestva informatsionnogo obespecheniya monitoringa pravotvorchestva i pravoprimeneniya [Improving the quality of information support for monitoring lawmaking and law enforcement] / A.V. Dokukin // Informatsionno-ekonomicheskie aspekti standartizatsii i tekhnicheskogo regulirovaniya [Information and economic aspects of standardization and technical regulation]. — 2013. — № 6 (16). — P. 10. — EDN: TNYISR. [in Russian]

17. V Sbere rasskazali, kak pomogli rossiyanam uberech ot moshennikov bolee 360 mlrd rublei [Sber explained how it helped Russians save over 360 billion rubles from fraudsters] // Banki.ru. — 2026. — URL: https://www.banki.ru/news/lenta/?id=11020738 (accessed: 26.02.2026). [in Russian]

18. II protiv moshennikov: kak antifrod-sistemi uchatsya raspoznavat ugrozi [AI vs fraudsters: how antifraud systems learn to recognize threats] // RBK Trendi [RBC Trends]. — 2025. — URL: https://trends.rbc.ru/trends/industry/679f706c9a7947e64f4f0d30 (accessed: 26.02.2026). [in Russian]

19. Volkov A. U nas voruyut: kak BI pomogaet ostanovit korruptsiyu v stroitelstve [“They steal from us”: how BI helps stop corruption in construction] / A. Volkov // Khabr [Habr]. — 2025. — URL: https://habr.com/ru/companies/cynteka/articles/945248/ (accessed: 26.02.2026). [in Russian]

20. Krilova D.V. Ispolzovanie iskusstvennogo intellekta v voprosakh viyavleniya i protivodeistviya korruptsii: obzor mezhdunarodnogo opita [Use of Artificial Intelligence in Detecting and Combating Corruption: A Review of International Experience] / D.V. Krilova, A.A. Maksimenko // Gosudarstvennoe upravlenie. Elektronnii vestnik [Public Administration. Electronic Bulletin]. — 2021. — № 84. — P. 241–255. — DOI: 10.24412/2070-1381-2021-84-241-255. [in Russian]

21. Abakumova E.B. Pravovoi rezhim primeneniya tsifrovikh tekhnologii i iskusstvennogo intellekta v antikorruptsionnoi deyatelnosti gosudarstva. Chast 2 [Legal regime for the use of digital technologies and artificial intelligence in the anti-corruption activities of the state. Part 2] / E.B. Abakumova // Pravo i gosudarstvo: teoriya i praktika [Law and state: theory and practice]. — 2025. — № 9. — P. 133–136. — DOI: 10.61726/6246.2025.45.34.001. [in Russian]

22. Anosov A.V. Tekhnologii iskusstvennogo intellekta v sisteme protivodeistviya korruptsii [Artificial intelligence technologies in the anti-corruption system] / A.V. Anosov // Pravo i gosudarstvo: teoriya i praktika [Law and state: theory and practice]. — 2024. — № 12 (240). — P. 541–543. — DOI: 10.47643/1815-1337_2024_12_541. [in Russian]

23. Basangov D.A. Osobennosti ispolzovaniya tsifrovikh tekhnologii v viyavlenii korruptsionnikh priznakov publichnikh zakupok [Features of the use of digital technologies in identifying signs of corruption in public procurement] / D.A. Basangov // Obrazovanie i pravo [Education and Law]. — 2025. — № 1. — P. 415–421. — DOI: 10.24412/2076-1503-2025-1-415-421. [in Russian]

24. Alekseev S.L. Ekonomiko-antikorruptsionnie problemi upravleniya finansovoi ustoichivostyu aktorov ekonomiki (voprosi teorii i praktiki) [Economic and anti-corruption problems of managing the financial stability of economic actors (theoretical and practical issues)] / S.L. Alekseev, N.M. Yakushkin, A.A. Ayupov [et al.]. — Kazan: Tatar Institute for Retraining of Agribusiness Personnel, 2025. — 208 p. — EDN: TBSEGU. [in Russian]