



## РЕГИОНАЛЬНАЯ И ОТРАСЛЕВАЯ ЭКОНОМИКА/REGIONAL AND SECTORAL ECONOMICS

DOI: <https://doi.org/10.60797/IRJ.2026.165.97> EDN: GCLBDH

## ПОВЫШЕНИЕ КАЧЕСТВА АНТИКОРРУПЦИОННОГО КОНТРОЛЯ ЧЕРЕЗ ИНТЕГРАЦИЮ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Научная статья

Алексеев С.Л.<sup>1\*</sup>, Сергеева Ю.С.<sup>2</sup>, Кочетков Н.В.<sup>3</sup><sup>1</sup> ORCID : 0000-0002-6765-8347;<sup>2</sup> ORCID : 0000-0003-1659-1186;<sup>3</sup> ORCID : 0009-0000-9731-5452;<sup>1</sup> Казанский национальный исследовательский технический университет имени А. Н. Туполева-КАИ, Казань, Российская Федерация<sup>1,2</sup> Российская инженерная академия менеджмента и агробизнеса, Пушкино, Российская Федерация<sup>3</sup> Казанский государственный аграрный университет, Казань, Российская Федерация

\* Корреспондирующий автор (tany\_1313[at]mail.ru)

**Аннотация**

В статье анализируются возможности использования искусственного интеллекта в российском антикоррупционном контроле при опоре на государственную информационную систему «Посейдон». Выделены региональные сценарии: верификация деклараций, выявление конфликтов интересов, риск-скоринг закупок и мер поддержки. Показано, какие требования к данным, безопасности и подотчетности алгоритмов необходимы для межведомственной аналитики и повышения адресности проверок. В заключении авторы приходят к выводу о том, что система «Посейдон» может стать не только хранилищем сведений, но и платформой профилактики: от раннего выявления рисков до обратной связи для изменения процедур, которые генерируют коррупционные возможности.

**Ключевые слова:** искусственный интеллект, антикоррупционный контроль, ГИС «Посейдон», декларации о доходах, конфликт интересов, аналитика закупок, риск-ориентированный надзор, экономическая безопасность, финансовая безопасность, информационная безопасность, межведомственная интеграция.

## QUALITY IMPROVEMENT OF ANTI-CORRUPTION CONTROL THROUGH THE INTEGRATION OF ARTIFICIAL INTELLIGENCE SYSTEMS

Research article

Alexeev S.L.<sup>1\*</sup>, Sergeeva Y.S.<sup>2</sup>, Kochetkov N.V.<sup>3</sup><sup>1</sup> ORCID : 0000-0002-6765-8347;<sup>2</sup> ORCID : 0000-0003-1659-1186;<sup>3</sup> ORCID : 0009-0000-9731-5452;<sup>1</sup> Kazan National Research Technical University named after A.N. Tupolev-KAI, Kazan, Russian Federation<sup>1,2</sup> Russian Engineering Academy of Management and Agribusiness, Pushkino, Russian Federation<sup>3</sup> Kazan State Agrarian University, Kazan, Russian Federation

\* Corresponding author (tany\_1313[at]mail.ru)

**Abstract**

The article analyses the possibilities of using artificial intelligence in Russian anti-corruption control based on the "Poseidon" state information system. Regional scenarios are highlighted: verification of declarations, identification of conflicts of interest, risk scoring of procurement and support measures. It shows what requirements for data, security, and algorithm accountability are necessary for interdepartmental analytics and improving the targeting of inspections. In conclusion, the authors conclude that the 'Poseidon' system can become not only a repository of information, but also a platform for prevention: from early risk detection to feedback for changing procedures that generate opportunities for corruption.

**Keywords:** artificial intelligence, anti-corruption control, GIS 'Poseidon', income declarations, conflict of interest, procurement analytics, risk-based supervision, economic security, financial security, information security, interdepartmental integration.

**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: 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.

Под применением ИИ в контрольно-надзорной и антикоррупционной деятельности целесообразно понимать не только использование больших языковых моделей, но и весь спектр методов аналитики данных: классификацию и

ранжирование объектов по риску, выявление нетипичных паттернов, построение графов связей, обработку текстов обращений и документов, сопоставление реестров, а также формирование объяснимых подсказок инспектору. Важно, что эти методы не подменяют юридическую квалификацию и не создают «автоматического обвинителя»: они меняют экономику контроля, позволяя сузить поле проверки, раньше формировать проверяемые гипотезы и направлять ресурсы на наиболее вероятные нарушения. Эффект ИИ определяется не столько точностью модели в лаборатории, сколько тем, как она встроена в регламенты, доказательные стандарты и дисциплину данных.

Основная тема исследования — перспективы внедрения ИИ-инструментов в региональный антикоррупционный контроль как систему профилактики и управления рисками. Проблема заключается в разрыве между доступностью цифровых данных и способностью контрольных контуров превращать их в управленческие решения: сведения распределены по ведомствам и муниципалитетам, имеют неодинаковое качество, а результаты аналитики должны быть интерпретируемыми, воспроизводимыми и привязанными к конкретным документам и процедурам.

Цель работы — обосновать направления применения ИИ в антикоррупционном контроле на уровне субъекта Федерации и сформулировать условия, при которых такие решения повышают адресность контроля при соблюдении правовых и организационных требований. Для достижения цели анализируются типовые прикладные сценарии (прежде всего в публичных закупках и иных распределительных процедурах), уточняются требования к данным и межведомственной сопоставимости, а также описываются принципы представления результата в виде «риск-сигнала», пригодного для документальной проверки и последующей обратной связи.

Актуальность исследования обусловлена ростом объема цифрового следа и усложнением управленческих цепочек при одновременной ограниченности кадровых и временных ресурсов региональных контрольных подразделений: без автоматизации аналитики риск-ориентированный мониторинг трудно масштабировать. Научная новизна работы состоит в том, что ИИ рассматривается не как отдельный технологический продукт, а как элемент управленческого контура — от витрин данных и правовых оснований доступа до подотчетности алгоритмов и метрик результата. Теоретическая значимость заключается в уточнении понятийных границ ИИ в государственном контроле и в сопряжении риск-ориентированного подхода с требованиями доказуемости и процессуальных гарантий. Практическая значимость определяется возможностью использовать выводы и предложенные принципы при проектировании региональных модулей риск-аналитики: для приоритизации проверок, повышения качества данных, настройки регламентов работы с сигналами и оценки эффекта (доля подтвержденных нарушений среди приоритетных кейсов, снижение трудозатрат и сокращение сроков выявления проблемных процедур).

### **Методы и принципы исследования**

Базовый метод — компаративный анализ зарубежного и российского регулирования и практики. Сопоставление выполнялось по функциональным блокам антикоррупционного цикла: профилактика и управление рисками, выявление и проверка сигналов, документирование и доказательность, меры реагирования, а также организационная архитектура межведомственного обмена данными. Для сопоставимости использовались единые критерии сравнения: степень допустимой автоматизации, требования к объяснимости и проверяемости выводов, распределение ответственности между оператором данных, разработчиком модели и контролером, режимы доступа к данным и ограничения на обработку персональных сведений, требования к журналированию и аудиту решений, а также механизмы обжалования и процессуальные гарантии.

Второй опорный метод — нормативно-догматический анализ. Он применялся для реконструкции правового статуса «риск-сигнала», формируемого аналитическими инструментами, и для разграничения юридически значимых действий и вспомогательных процедур аналитического сопровождения. В рамках этого подхода анализировались логика правовых норм, их иерархия и взаимосвязи, а также типовые юридические риски внедрения алгоритмов в контрольно-надзорные процессы: недопустимость подмены дискреции контролера, риск непрозрачного влияния модели на решение, проблема воспроизводимости выводов и допустимости доказательств, а также требования к целевому ограничению обработки данных.

Третий метод — институциональный и процессный анализ, позволяющий описать ИИ не как автономный продукт, а как элемент управленческого контура. Здесь использовались принципы системности и прослеживаемости: от источников данных и их качества до регламентов принятия решений и обратной связи. В качестве аналитической рамки применялась логика «данные — модель - решение — контроль качества», где на каждом этапе фиксируются входы, выходы, роли участников и контрольные процедуры. Это обеспечивало воспроизводимость теоретических выводов в смысле возможности повторить рассуждение и проверить соответствие предложенных принципов требованиям к управляемости, подотчетности и информационной безопасности.

Дополнительно применялись методы контент-анализа и функционального моделирования. Контент-анализ использовался для систематизации типовых сценариев применения ИИ в антикоррупционной деятельности (ранжирование объектов по риску, выявление аномалий, графовые связи, обработка текстов, сопоставление реестров) и для выделения устойчивых «узких мест» внедрения, связанных с дисциплиной данных и процедурной совместимостью. Функциональное моделирование применялось для построения типовой схемы встраивания ИИ в регламенты контроля, где 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 формирует юридическую квалификацию), принцип проверяемости (каждый сигнал должен быть привязан к конкретным документам и полям данных), принцип минимизации и целевого ограничения обработки сведений, принцип подотчетности и аудируемости (журналирование, версионирование, контроль доступа), 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).

## Основные результаты

Мировые тенденции наиболее наглядно проявляются в сфере публичных закупок, где накоплены стандартизированные данные о процедурах, участниках и результатах торгов [1], [2]. 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 [3]. 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 политику защиты конкуренции и антикоррупционный контроль без тотального «ручного» просмотра массивов процедур [6].

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 [7].

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 [8].

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 [9]: модели должны сопровождаться документацией, тестами устойчивости и ясным распределением ответственности между разработчиком, владельцем процесса и аудитором [10].

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 [11]. При переносе этих тенденций в российский контекст критично учитывать нормативные и организационные границы. Вот расширенный вариант текста с пояснениями значимости каждого закона:

Антикоррупционный контроль встроен в систему публичного управления и опирается на нормы Федерального закона от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» (Собрание законодательства Российской Федерации. 2008. № 52 (часть I). Ст. 6228), который устанавливает базовые определения коррупционных правонарушений, закрепляет принципы профилактики и организационные основы противодействия коррупции, а также определяет обязанности государственных и муниципальных служащих по декларированию доходов, расходов, имущества и обязательств имущественного характера — именно эти данные формируют ключевой массив сведений, подлежащих автоматизированной верификации. Закон также вводит институт конфликта интересов и обязанность его урегулирования, что создаёт нормативную основу для алгоритмического выявления ситуаций, в которых личная заинтересованность должностного лица может повлиять на объективность принимаемых решений.

С указанным законом тесно связаны механизмы служебного поведения и ограничений: Федеральный закон от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» (Собрание законодательства Российской Федерации. 2004. № 31. Ст. 3215) устанавливает запреты и ограничения для гражданских служащих, включая запрет на участие в коммерческой деятельности, получение вознаграждений от физических и юридических лиц, а также требования к представлению сведений о доходах и имуществе; именно нарушения этих ограничений чаще всего становятся предметом антикоррупционных проверок, и их цифровизация позволяет выстраивать автоматизированные контуры мониторинга. Федеральный закон от 2 марта 2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации» (Собрание законодательства Российской Федерации. 2007. № 10. Ст. 1152) распространяет аналогичные ограничения и обязанности на муниципальный уровень, что принципиально важно, поскольку значительная доля коррупционных рисков локализована именно в муниципальных закупках, земельных и градостроительных решениях, где объёмы бюджетных средств сочетаются с ослабленным внешним контролем. Федеральный закон от 3 декабря 2012 г. № 230-ФЗ «О контроле за соответствием расходов лиц, замещающих



государственные должности, и иных лиц их доходам» (Собрание законодательства Российской Федерации. 2012. № 50. Ст. 6953) вводит механизм расходного контроля, позволяющий выявлять расхождения между задекларированными доходами и фактическими расходами на приобретение недвижимости, транспортных средств и ценных бумаг; для ИИ-систем этот закон создаёт формализуемый критерий — порог несоответствия расходов и доходов, который может автоматически инициировать углублённую проверку.

Существенная часть цифрового следа формируется в рамках контрактной системы: Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (Собрание законодательства Российской Федерации. 2013. № 14. Ст. 1652) обеспечивает сквозную прозрачность закупочного цикла — от планирования и обоснования начальной (максимальной) цены контракта до приёма результатов; данные Единой информационной системы (ЕИС), формируемые в соответствии с этим законом, представляют собой наиболее структурированный источник для алгоритмического анализа признаков сговора, дробления закупок и завышения цен. Федеральный закон от 18 июля 2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» (Собрание законодательства Российской Федерации. 2011. № 30. Ст. 4571) распространяет требования информационной открытости на закупки государственных корпораций, компаний с государственным участием и иных организаций, что расширяет периметр антикоррупционного мониторинга на квазигосударственный сектор, где традиционно ниже уровень процедурной стандартизации и, соответственно, выше потенциал для злоупотреблений.

Контрольно-надзорная деятельность в целом развивается в логике риск-ориентированного подхода, закреплённого в Федеральном законе от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» (Собрание законодательства Российской Федерации. 2020. № 31 (часть I). Ст. 5007). Этот закон вводит систему категорирования подконтрольных субъектов по уровням риска и индикаторы риска нарушения обязательных требований, тем самым создавая правовой прецедент для использования скоринговых и предиктивных моделей в публичном управлении; алгоритмы машинного обучения, применяемые в антикоррупционном контроле, концептуально опираются на ту же логику ранжирования объектов по вероятности нарушения.

Одновременно любые межведомственные витрины и модели неизбежно сталкиваются с требованиями законодательства об информации и персональных данных. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448) определяет правовые режимы доступа к информации, порядок её предоставления из одной государственной информационной системы в другую и условия межведомственного взаимодействия, что критично при построении аналитических платформ, объединяющих данные из реестров собственности, налоговых баз и закупочных систем. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3451) устанавливает требования к обработке сведений, позволяющих идентифицировать физическое лицо, включая принципы минимизации данных, целевого ограничения и получения согласия; для антикоррупционных ИИ-систем это означает необходимость обезличивания или агрегирования данных на этапе обучения моделей и строгого разграничения доступа на этапе эксплуатации. Режимы защиты информации дополняются требованиями к использованию электронной подписи, закреплёнными в Федеральном законе от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (Собрание законодательства Российской Федерации. 2011. № 15. Ст. 2036), который обеспечивает юридическую значимость электронных документов и транзакций; в контексте антикоррупционного контроля электронная подпись позволяет фиксировать авторство и неизменность документов, формирующих доказательную базу, а также удостоверить результаты автоматизированных проверок при их передаче в контрольные и правоохранительные органы.

Эта нормативная рамка задаёт для ИИ-решений ключевой принцип: алгоритм может формировать приоритеты и подсказки, но юридически значимые выводы должны быть проверяемы и воспроизводимы в понятных для контроля и суда категориях.

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 [12].

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 [13].

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 [14].

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 [15].

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.2026.165.97.1>

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. С целью реализации предлагаемой концепции антикоррупционного контроля в прикладном инструментарии, целесообразно различать три слоя решений. Первый — слой данных: регулярные выгрузки из ЕИС и региональных подсистем, справочники контрагентов, реестры контрактов и исполнений, данные жалоб и результатов контроля, а также (при наличии правовых оснований) сведения о связях и аффилированности. Второй — слой моделей: риск-скоринг закупок, выявление аномалий в процессных параметрах, детекция сговоров (в т.ч. на основе экранов и графов совместного участия), обработка текстов закупочной документации и обращений граждан. Третий — слой принятия решений: «карточки риск-сигналов», встроенные в регламенты, с указанием причин срабатывания, перечня документов для проверки и ожидаемого типа нарушения. Качество внедрения измеряется не только метриками машинного обучения (точность, полнота, доля ложных срабатываний), но и операционными показателями: долей сигналов, доведенных до проверки, временем анализа кейса, экономией трудозатрат и долей подтвержденных нарушений в верхнем приоритете.

## Обсуждение

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 [16].

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 [17].

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: качество данных → 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).

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. Для иллюстрации прикладного сценария рассмотрим алгоритм выявления аномалий в электронном аукционе по 44-ФЗ на уровне субъекта Федерации. Исходные данные — события и атрибуты закупки (извещение, НМЦК, сроки, требования, протоколы), результаты (количество заявок, допуск/отклонение, динамика ценовых предложений, победитель), а также контекст (история заказчика и поставщика, отрасль, ОКПД2, география поставки, тип контракта). Алгоритм работает в несколько шагов:

- 1) нормализация данных и связывание сущностей (закупка-заказчик-участники-контракт);
- 2) расчет набора «процессных» и «поведенческих» признаков;
- 3) расчет риск-балла гибридной моделью (правила + обучаемый классификатор/анализ аномалий);
- 4) формирование карточки риск-сигнала с объяснением (какие признаки повысили оценку риска);
- 5) передача в контур контроля для приоритизации проверок и последующая фиксация результата (подтверждено/не подтверждено), используемая как обратная связь для настройки порогов и модели.

Таблица 2 - Риски применения ИИ и меры управленческого контроля

DOI: <https://doi.org/10.60797/IRJ.2026.165.97.2>

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

Ключевые параметры, которые целесообразно проверять в таком модуле, представлены в таблице 3.

Таблица 3 - Пример параметров для выявления аномалий в электронном аукционе (44-ФЗ)

DOI: <https://doi.org/10.60797/IRJ.2026.165.97.3>

Параметр / признак	Как измеряется (пример)	Риск-сигнал для проверки (пример интерпретации)
Длительность этапа подачи заявок	Дней от публикации извещения до окончания приема заявок; сравнение с медианой по ОКПД2/ценовому диапазону	Необычно короткий срок при сложном объекте закупки может снижать конкуренцию и требовать анализа обоснования сроков
Частота изменений документации	Количество изменений; время внесения изменений относительно дедлайна	Поздние изменения (за 1–2 дня до окончания приема) повышают риск «заточки» требований и требуют проверки мотивировки

Параметр / признак	Как измеряется (пример)	Риск-сигнал для проверки (пример интерпретации)
Число поданных заявок	Общее число заявок; доля процедур с 0–1 заявкой у заказчика/в отрасли	Систематически низкая конкуренция у конкретного заказчика или по лоту - сигнал на анализ ограничивающих требований
Доля отклоненных заявок	Отклоненные/поданные; причины отклонения по протоколам	Аномально высокая доля отклонений может указывать на дискриминационные требования или формальное «отсеивание» конкурентов
Динамика цены на торгах	Скидка к НМЦК; число ценовых шагов; распределение ставок по времени	Минимальная скидка при наличии нескольких участников либо «ступенчатые» ставки близко к окончанию — повод анализировать координацию
Повторяемость победителей	Концентрация побед; доля контрактов/НМЦК у топ-1/топ-3 поставщиков по заказчику за период	Высокая концентрация при низкой конкуренции требует проверки обоснованности требований и связей участников
Стабильные «группы участников»	Ко-участие: сколько раз одинаковые компании встречаются в одних торгах; граф совместного участия	Постоянное совместное участие одних и тех же компаний без смены победителей — сигнал возможного сговора/раздела рынка
Пороговые требования к опыту/ресурсам	Извлеченные из документации требования (NLP-поиск типовых формулировок); сравнение с типовыми практиками отрасли	Нетипично завышенные требования могут ограничивать доступ и требуют проверки соразмерности предмету закупки
Дробление закупок	Серии схожих лотов (по ОКПД2, описанию, сумме) в коротком окне; суммарный объем	Серийные закупки с близкими параметрами могут указывать на обход процедур и требуют агрегированного анализа
Изменение цены/условий в ходе исполнения	Число допсоглашений; изменение цены и сроков относительно исходных	Частые существенные изменения условий после заключения контракта — риск недобросовестного планирования/«вывода» средств
Конфликт интересов в цепочке	Связи между заказчиком/комиссией и поставщиком (при наличии правового основания и данных)	Выявленные аффилированности требуют процедурной фиксации и юридически корректной проверки
Апелляции и жалобы	Наличие/частота жалоб по заказчику и лотам; результаты рассмотрения	Повторяющиеся обоснованные жалобы повышают приоритет контроля и уточняют набор проверяемых признаков

*Примечание: параметры и пороги должны калиброваться под отрасль и практику региона; сигналы используются для приоритизации проверки и не являются доказательством нарушения*

Набор признаков может быть расширен, но даже базовый слой позволяет выявлять типовые «узкие места»: аномально короткие сроки подачи заявок по сравнению с отраслевой нормой; регулярные победы одного участника у конкретного заказчика при низкой конкуренции; существенные отклонения цены от сопоставимых закупок; нехарактерная доля отклоненных заявок; серийные закупки с близкими параметрами, которые по отдельности не подпадают под пороги, но в совокупности формируют риск дробления. Важно, что речь идет не о доказательстве коррупции, а о формировании проверяемых гипотез, которые экономят время аудитора и повышают адресность контроля.

Запрос на статистические показатели и динамику по годам особенно релевантен для выбора приоритетов региональных проектов. По данным Счетной палаты РФ, доля извещений, признанных несостоявшимися, в 2017–2023 гг. выросла и по итогам 2023 года приблизилась к каждой второй конкурентной процедуре; при этом по стоимостному

объему несостоявшиеся извещения составляют около 60% общего объема. В структуре причин несостоявшихся закупок доминируют отсутствие заявок и участие единственной заявки (в среднем свыше 90% в 2022–2023 гг.), а по итогам 2023 года единственная заявка подавалась в 42,7% случаев, формируя более половины стоимостного объема опубликованных извещений. Такая динамика одновременно указывает на недостаточность конкуренции и подчеркивает прикладную ценность алгоритмов, которые выделяют наиболее рискованные процедуры для последующей проверки (см. рис. 1).



Рисунок 1 - Динамика признания извещений несостоявшимися

DOI: <https://doi.org/10.60797/IRJ.2026.165.97.4>

Примечание: отчет Счетной палаты от 26 сентября 2024 по данным ЕИС

Встраивание подобных модулей в региональный контур требует опоры на существующие государственные информационные системы. С практической точки зрения логично рассматривать интеграцию с платформами, которые уже аккумулируют сведения для мониторинга антикоррупционных ограничений и проверок. В качестве примерной архитектуры можно описать гипотетический модуль «Риск-аналитика закупок», который получает поток событий из ЕИС и региональных подсистем, рассчитывает риск-баллы и формирует карточки сигналов для уполномоченных подразделений. В российской практике потенциальной точкой сборки межведомственных данных выступает государственная информационная система «Посейдон», развиваемая как инструмент контроля соблюдения отдельных ограничений и требований к служебному поведению; при этом внедрение ИИ-модуля в такую систему требует четкого разграничения ролей: платформа хранит и агрегирует данные, модель формирует сигнал, а решение о проверке и квалификации остается за компетентным органом.

Таким образом, научная новизна настоящей работы заключается в совмещении трех компонентов, которые в исследованиях обычно рассматриваются раздельно:

- (1) конкретизации международных трендов именно для задач регионального контроля;
- (2) предложении типового набора измеримых параметров «процессной аномальности» для электронного аукциона по 44-ФЗ, пригодного для встраивания в риск-скоринг;
- (3) описании управленческого контура подотчетности алгоритмов, где результат модели оформляется как проверяемый артефакт (карточка риск-сигнала) и возвращается в обучение через обратную связь по итогам проверок.

### Заключение

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. В целом перспективы применения ИИ в антикоррупционном контроле на государственном уровне связаны не столько с заменой человека, сколько с повышением адресности и доказуемости контроля. Для регионов наибольший эффект ожидается от комбинации риск-скоринга закупок, выявления аномалий и признаков сговора, интегрированных в межведомственный контур данных и подкрепленных регламентами подотчетности. При соблюдении требований к качеству данных, безопасности и объяснимости алгоритмов ИИ может стать инструментом профилактики: ускорять выявление проблемных зон, снижать долю рутинных проверок и создавать обратную связь для коррекции нормативных и процедурных «узких мест», которые воспроизводят коррупционные риски на уровне субъекта Федерации.

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

Выражаем благодарность Управлению Раиса Республики Татарстан по антикоррупционной политике.

### Конфликт интересов

Не указан.

### Рецензия

Семенов А.В., ПАО «ГАЗПРОМ», Санкт-Петербург Российская Федерация, Санкт-Петербургский университет технологий управления и экономики, Санкт-Петербург Российская Федерация  
DOI: <https://doi.org/10.60797/IRJ.2026.165.97.5>

### Acknowledgement

We express our gratitude to the Rais Office for Anti-Corruption Policy of the Republic of Tatarstan.

### Conflict of Interest

None declared.

### Review

Semenov A.V., GAZPROM PJSC, Saint-Petersburg Russian Federation, Saint Petersburg University of Management Technologies and Economics, Saint-Petersburg Russian Federation  
DOI: <https://doi.org/10.60797/IRJ.2026.165.97.5>

### 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 KUVBUN.
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. Фарахiev Д.М. Государственная информационная система «Посейдон»: современный взгляд на противодействие коррупции / Д.М. Фарахiev // Вестник Московского университета МВД России. — 2023. — № 1. — С. 250–254. — DOI: 10.24412/2073-0454-2023-1-250-254.
4. Бабков Д.И. Антикоррупционный потенциал системы «Посейдон» / Д.И. Бабков // Юридическая наука и практика. — 2023. — Т. 19, № 4. — С. 34–41. — DOI: 10.25205/2542-0410-2023-19-4-34-41.
5. Агеев В.Н. Информационные технологии как средство противодействия коррупции в Российской Федерации / В.Н. Агеев // National Security / nota bene. — 2023. — № 6. — С. 49–60. — DOI: 10.7256/2454-0668.2023.6.69405.



6. Докунин А.В. Основы разработки стандартов информационной безопасности / А. В. Докукин, Т. Б. Ершова, В. А. Коновалов, А. А. Стреха // Стандарты и качество. — 2008. — № 8. — С. 46–48. — EDN MUMYGP.
7. Жарова А.К. Защита информации ограниченного доступа в ГИС в области противодействия коррупции / А.К. Жарова // Проблемы экономики и юридической практики. — 2023. — Т. 19, № 5. — С. 30–34. — EDN: NIUBZA.
8. Adam I. Are emerging technologies helping win the fight against corruption? A review of the state of evidence / I. Adam, M. Fazekas // Information Economics and Policy. — 2021. — Vol. 57. — Art. 100950.
9. García Rodríguez M.J. Collusion detection in public procurement auctions with machine learning algorithms / M.J. García Rodríguez, V. Rodríguez-Montequín, P. Ballesteros-Pérez [et al.] // Automation in Construction. — 2022. — Vol. 133. — Art. 104047.
10. 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.
11. 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. — ISBN 978-5-605-17470-7. — EDN TBSEGU.
12. Алексеев С. Л. Экономико-антикоррупционная безопасность акторов экономики: Учебник / С. Л. Алексеев, Н. М. Якушкин, Ю. С. Сергеева. — Казань: Татарский институт переподготовки кадров агробизнеса, 2025. — 236 с. — ISBN 978-5-605-17478-3. — EDN WITRPI.
13. Кочетков Н. В. Роль антикоррупционного контроля в обеспечении экономической безопасности субъектов Российской Федерации / Н. В. Кочетков, С. Л. Алексеев // Экономика и предпринимательство. — 2024. — № 11(172). — С. 349–353. — DOI: 10.34925/EIP.2024.172.11.062. — EDN PRTDIN.
14. Schneider dos Santos E. Detection of fraud in public procurement using data-driven methods: a systematic mapping study / E. Schneider dos Santos, M. Machado dos Santos, M. Castro [et al.] // EPJ Data Science. — 2025. — Vol. 14. — Article 52.
15. Стреха А. А. Совершенствование системы информационного обеспечения процессов разработки и применения стандартов / А. А. Стреха, А. В. Докукин, В. Е. Галкин // Транспортное дело России. — 2014. — № 6. — С. 132–134. — EDN TKUQYF.
16. 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.
17. 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. — ISBN 978-5-605-17470-7. — EDN TBSEGU.

### Список литературы на английском языке / References in English

1. Alyakin A. A. Funkcionirovanie edinoj informacionnoj sistemy po tekhnicheskomu regulirovaniyu na baze paradigmьy elektronnoho gosudarstva [Functioning of the 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. Funkcii edinoj informacionnoj sistemy po tekhnicheskomu regulirovaniyu v ramkah koncepcii elektronnoho gosudarstva [Functions of the unified information system for technical regulation within the framework of the e-government concept] / M. I. Lomakin, A. V. Dokukin // Perspektivy nauki [Prospects of Science]. — 2011. — № 12 (27). — P. 230–233. — EDN PBAFMV. [in Russian]
3. Farakhiev D.M. Gosudarstvennaya informacionnaya sistema «Posejdon»: sovremennyy vzglyad na protivodejstvie korrupcii [State information system "Poseidon": a modern look at combating corruption] / D.M. Farakhiev // Vestnik Moskovskogo universiteta MVD Rossii [Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia]. — 2023. — № 1. — P. 250–54. — DOI: 10.24412/2073-0454-2023-1-250-254. [in Russian]
4. Babkov D.I. Antikorrupcionnyj potencial sistemy «Posejdon» [Anti-corruption potential of the Poseidon system] / D.I. Babkov // Yuridicheskaya nauka i praktika [Legal Science and Practice]. — 2023. — Vol. 19, № 4. — P. 34–41. — DOI: 10.25205/2542-0410-2023-19-4-34-41. [in Russian]
5. Ageev V.N. Informacionnye tekhnologii kak sredstvo protivodejstviya korrupcii v Rossijskoj Federacii [Information technology as a means of combating corruption in the Russian Federation] / V.N. Ageev // National Security / nota bene. — 2023. — № 6. — P. 49–60. — DOI: 10.7256/2454-0668.2023.6.69405. [in Russian]
6. Dokunin A.V. Osnovy razrabotki standartov informacionnoj bezopasnosti [Fundamentals of developing information security standards] / A. V. Dokukin, T. B. Ershova, V. A. Konovalov, A. A. Strekha // Standarty i kachestvo [Standards and quality]. — 2008. — № 8. — P. 46–48. — EDN MUMYGP. [in Russian]
7. Zharova A.K. Zashchita informacii ogranichennoho dostupa v GIS v oblasti protivodejstviya korrupcii [Protection of restricted access information in GIS in the field of combating corruption] / A.K. Zharova // Problemy ekonomiki i yuridicheskoy praktiki [Problems of Economics and Legal Practice]. — 2023. — Vol. 19, № 5. — P. 30–34. — EDN: NIUBZA. [in Russian]
8. Adam I. Are emerging technologies helping win the fight against corruption? A review of the state of evidence / I. Adam, M. Fazekas // Information Economics and Policy. — 2021. — Vol. 57. — Art. 100950.
9. García Rodríguez M.J. Collusion detection in public procurement auctions with machine learning algorithms / M.J. García Rodríguez, V. Rodríguez-Montequín, P. Ballesteros-Pérez [et al.] // Automation in Construction. — 2022. — Vol. 133. — Art. 104047.



10. 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.
11. Alekseev S.L. Ekonomiko-antikorrupcionnye problemy upravleniya finansovoj ustojchivost'yu aktorov ekonomiki (voprosy 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. — ISBN 978-5-605-17470-7. — EDN TBSEGU. [in Russian]
12. Alekseev S. L. Ekonomiko-antikorrupcionnaya bezopasnost' aktorov ekonomiki: Uchebnik [Economic and anti-corruption security of economic actors: Textbook] / S. L. Alekseev, N. M. Yakushkin, Yu. S. Sergeeva. — Kazan: Tatar Institute for Retraining of Agribusiness Personnel, 2025. — 236 p. — ISBN 978-5-605-17478-3. — EDN WITRPI. [in Russian]
13. Kochetkov N. V. Rol' antikorrupcionnogo kontrolya v obespechenii ekonomicheskoy bezopasnosti sub"ektov Rossijskoj Federacii [The Role of Anti-Corruption Control in Ensuring Economic Security of the Subjects of the Russian Federation] / N. V. Kochetkov, S. L. Alekseev // *Ekonomika i predprinimatel'stvo* [Economy and Entrepreneurship]. — 2024. — № 11 (172). — P. 349–353. — DOI: 10.34925/EIP.2024.172.11.062. — EDN PRTDIN. [in Russian]
14. Schneider dos Santos E. Detection of fraud in public procurement using data-driven methods: a systematic mapping study / E. Schneider dos Santos, M. Machado dos Santos, M. Castro [et al.] // *EPJ Data Science*. — 2025. — Vol. 14. — Article 52.
15. Strekha A. A. Sovershenstvovanie sistemy informacionnogo obespecheniya processov razrabotki i primeneniya standartov [Improving the information support system for the processes of development and application of standards] / A. A. Strekha, A. V. Dokukin, V. E. Galkin // *Transportnoe delo Rossii* [Transport business of Russia]. — 2014. — № 6. — P. 132–134. — EDN TKUQYF. [in Russian]
16. Basangov D.A. Osobennosti ispol'zovaniya cifrovyyh tekhnologij v vyyavlenii korrupcionnyh priznakov publicnyh 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]
17. Alekseev S.L. Ekonomiko-antikorrupcionnye problemy upravleniya finansovoj ustojchivost'yu aktorov ekonomiki (voprosy 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. — ISBN 978-5-605-17470-7. — EDN TBSEGU. [in Russian]