

Научная статья
УДК 338.2:351.712.2
DOI: 10.25683/VOLBI.2026.76.1688

Tatiana Vasilievna Mokeeva
Candidate of Economics,
Associate Professor of Graduate School of Industrial Economics,
Peter the Great
St. Petersburg Polytechnic University
Saint Petersburg, Russian Federation
mokeeva_tv@spbstu.ru

Татьяна Васильевна Мокеева
канд. экон. наук,
доцент Высшей инженерно-экономической школы,
Санкт-Петербургский политехнический университет
Петра Великого
Санкт-Петербург, Российская Федерация
mokeeva_tv@spbstu.ru

ВНЕДРЕНИЕ РИСК-ОРИЕНТИРОВАННОГО УПРАВЛЕНИЯ ГОСУДАРСТВЕННЫМИ ЗАКУПКАМИ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ЗАКАЗЧИКОВ

5.2.3 — Региональная и отраслевая экономика

Аннотация. Предметом исследования выступает система риск-ориентированного управления государственными и корпоративными закупками, темой — экономическая безопасность закупочной деятельности в условиях цифровой трансформации. Цель работы — обоснование дифференцированной системы управления закупочными рисками, адаптированной к масштабу организации-заказчика. Гипотеза исследования состоит в том, что доминирующий в нормативном дискурсе акцент на правовых и коррупционных рисках оставляет вне поля зрения организационно-управленческие, экономические и информационные риски, непосредственно определяющие устойчивость закупочной деятельности. Методология работы основана на анализе научной литературы и нормативно-правовых источников, частотном анализе упоминаемости рисков, кейс-анализе применения инструментов искусственного интеллекта, а также на обобщении опубликованных эмпирических исследований рынка закупок. В результате предложена авторская классификация закупочных рисков с выделением неявных цифровых рисков и рисков скрытых затрат; систематизированы информационные риски применения больших языковых моделей

и сформулированы принципы их безопасного использования; обоснован дифференцированный инструментарий — от чек-листов для малых предприятий до предиктивной аналитики для крупных корпораций. Научный вклад состоит в расширении представлений о закупочных рисках за пределы их правовой интерпретации и во введении категории неявных рисков скрытых затрат. Результаты применимы в деятельности заказчиков различного масштаба, органов-регуляторов и контрольных органов сферы регулируемых закупок. Ограничения исследования связаны с преимущественно качественным характером оценки рисков; дальнейшие исследования целесообразно направить на разработку методики их количественной оценки и на верификацию прогностической силы языковых моделей в отраслевом разрезе.

Ключевые слова: риск-ориентированное управление, государственные закупки, закупочные риски, экономическая безопасность, цифровизация закупок, скрытые затраты, предиктивная аналитика, искусственный интеллект, галлюцинации языковых моделей, отравление данных, Федеральный закон № 44-ФЗ, Федеральный закон № 223-ФЗ

Для цитирования: Мокеева Т. В. Внедрение риск-ориентированного управления государственными закупками в целях обеспечения экономической безопасности заказчиков // Бизнес. Образование. Право. 2026. № 3(76). С. 107—114. DOI: 10.25683/VOLBI.2026.76.1688.

Original article

INTRODUCTION OF RISK-BASED MANAGEMENT IN PUBLIC PROCUREMENT TO ENSURE ECONOMIC SECURITY OF PROCURING ENTITIES

5.2.3 — Regional and sectoral economy

Abstract. The subject of the study is the system of risk-based management of public and corporate procurement; its theme is the economic security of procurement activity under digital transformation. The aim of the work is to substantiate a differentiated risk-management system adapted to the scale of the procuring entity. The research hypothesis holds that the emphasis on legal and corruption risks prevailing in the regulatory discourse leaves aside the organizational and managerial, economic and information risks that directly determine the resilience of pro-

curement activity. The methodology is based on content analysis of the scholarly literature and regulatory sources, frequency analysis of risk occurrence, case analysis of AI tools, and a synthesis of published empirical studies of the procurement market. As a result, an original classification of procurement risks is proposed, distinguishing implicit digital risks and implicit hidden-cost risks; the information risks of applying large language models are systematized and principles for their safe use are formulated; and a differentiated toolkit is substantiated,

ranging from checklists for small organizations to predictive analytics for large corporations. The scientific contribution lies in extending the understanding of procurement risks beyond their legal interpretation and in introducing the category of implicit hidden-cost risks. The results are applicable to procuring entities of various scales, control bodies in the area of regulated procurement. The study is limited by the predominantly qualitative nature of risk

assessment; future research should develop a methodology for its quantitative assessment and verify the predictive power of language models across industry segments.

Keywords: risk-based management, public procurement, procurement risks, economic security, procurement digitalization, hidden costs, predictive analytics, artificial intelligence, language model hallucinations, data poisoning, Federal Law No. 44-FZ, Federal Law No. 223-FZ

For citation: Mokeeva T. V. Introduction of risk-based management in public procurement to ensure economic security of procuring entities. *Biznes. Obrazovanie. Pravo = Business. Education. Law*. 2026;3(76):107—114. DOI: 10.25683/VOLBI.2026.76.1688.

Введение

Актуальность. Современная система государственных и корпоративных закупок в Российской Федерации переживает период масштабной цифровой трансформации. Электронные торговые площадки, реестры контрактов и поставщиков, системы автоматизированного контроля — всё это формирует принципиально новую закупочную среду, регулируемую федеральными законами от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» и от 18 июля 2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц». Вместе с тем практика свидетельствует о том, что цифровизация сама по себе не устраняет риски закупочной деятельности, а в ряде случаев порождает новые специфические угрозы. Данное противоречие определяет актуальность разработки комплексных подходов к риск-ориентированному управлению закупками.

Изученность проблемы. Теоретико-правовые основы регулирования государственных и корпоративных закупок исследованы в работах Л. В. Андреевой [1] и В. В. Кикавца [2], рассматривающих закупки преимущественно сквозь призму правового регулирования и контрактной дисциплины. Экономические аспекты закупочной деятельности и проблема транзакционных издержек раскрыты А. А. Яковлевым с соавторами [3], а также в работе М. В. Островной и Е. А. Подколзиной, посвященной ограничениям конкуренции на российском рынке государственных закупок [4]. Восприятие проблем и эффективности госзакупок самими их участниками проанализировано А. А. Яковлевым с соавторами [5]. Институциональные риски государственного управления рассмотрены И. Смотрицкой и С. Черных [6]. Современные подходы к управлению рисками в системе государственных закупок, включая этапную идентификацию рисков и меры их минимизации, развиваются в работах С. Н. Коваленко с соавторами [7] и В. В. Петрушевской и Я. О. Арчиковой [8]. Наиболее близкими к предмету настоящего исследования являются работы Д. А. Созаевой, в которых предложена концепция риск-ориентированного управления регулируемыми закупками и введено понятие неявных рисков [9; 10]. Вопросы применения искусственного интеллекта в конкурентных закупках освещены Д. А. Казанцевым, П. Догналом и П. Догналом-мл. [11], однако преимущественно в правовом ключе. Проблематика объяснимости алгоритмических решений раскрыта в работе С. Вахтер, Б. Миттельштадта и К. Рассела [12]. Между тем, несмотря на значительный объем накопленных исследований, производственно-хозяйственные, организационно-управленческие и информационные риски, в т. ч. порождаемые внедрением технологий искусственного интеллекта (далее — ИИ), остаются недостаточно изученными

и не сведены в единую классификацию. Именно они в значительной мере определяют устойчивость и бесперебойность функционирования организаций-заказчиков.

Целесообразность разработки темы. Проведенный анализ литературы показывает, что в существующих исследованиях закупочные риски рассматриваются преимущественно фрагментарно и в отрыве друг от друга: правовые и коррупционные риски изучены наиболее полно, тогда как организационно-управленческие, экономические и информационные риски, а также риски скрытых затрат и риски применения ИИ не систематизированы и не увязаны с масштабом организации-заказчика. Целесообразность разработки темы обусловлена, во-первых, необходимостью восполнения этого пробела за счет построения целостной классификации закупочных рисков, выходящей за пределы их правовой интерпретации; во-вторых, практической потребностью заказчиков различного масштаба в дифференцированном инструментарии управления рисками в условиях цифровой трансформации закупок; в-третьих, появлением нового класса информационных рисков, связанных с внедрением больших языковых моделей, который до настоящего времени не получил системного осмысления применительно к закупочной деятельности.

Научная новизна исследования состоит в разработке классификации закупочных рисков с выделением неявных цифровых рисков и рисков скрытых затрат, а также в систематизации информационных рисков применения ИИ-инструментов применительно к закупочной практике [9; 10].

Теоретическая значимость определяется вкладом в развитие представлений о рисках закупочной деятельности за пределами их правовой и коррупционной интерпретации. **Практическая значимость** определяется возможностью непосредственного применения предложенного инструментария заказчиками различного масштаба.

Цель исследования — разработка дифференцированной системы риск-ориентированного управления закупками, адаптированной к масштабу организации и обеспечивающей экономическую безопасность закупочной деятельности.

Задачи исследования:

- идентифицировать и классифицировать закупочные риски на основе обобщения научной литературы и правоприменительной практики;
- оценить масштаб скрытых затрат при повторных процедурах; систематизировать информационные риски применения ИИ;
- разработать дифференцированные рекомендации для заказчиков различного масштаба.

Методологическую основу исследования составляет совокупность общенаучных и специальных методов. Метод анализа научной литературы и нормативно-правовых источников

применялся для первичной идентификации закупочных рисков: систематизировались виды рисков, описанные в исследованиях по экономической безопасности регулируемых закупок [9; 10], а также риски, зафиксированные в опубликованных экспертных обзорах и материалах правоприменительной практики применительно к организациям различного масштаба и правового статуса — от субъектов малого предпринимательства до публично-правовых компаний. Значимость отдельных видов рисков оценивалась методом частотного анализа их упоминаемости в проанализированных источниках. Для оценки масштаба скрытых затрат при повторных закупочных процедурах использованы результаты опубликованных исследований рынка государственных закупок лекарственных средств [13]. При анализе информационных рисков ИИ применялись методы кейс-анализа и сравнительного анализа доступных инструментов на основе больших языковых моделей по критериям локализации данных, доступности из Российской Федерации и применимости в закупочной практике.

Основная часть

Состояние проблемы управления рисками в системе государственных закупок. В действующей нормативной базе проблема управления рисками в сфере государственного заказа решается весьма ограниченно. Традиционный подход сводится к сравнительному анализу санкций Кодекса РФ об административных правонарушениях (далее — КоАП РФ), Бюджетного кодекса РФ и Федерального закона от 5 апреля 2013 г. № 44-ФЗ с точки зрения возможных мер ответственности. Отдельные проблемы правового регулирования корпоративных закупок применительно к практике Закона № 223-ФЗ рассма-

триваются в научно-практическом пособии О. А. Беляевой «Корпоративные закупки: проблемы правового регулирования» (2018). Указ Президента РФ о национальном плане противодействия коррупции на 2021—2024 гг. стимулировал ряд ведомств к разработке карт рисков. Анализ данных карт позволяет констатировать их существенную ограниченность: они фиксируют исключительно коррупционную составляющую риска — умысел при планировании, при определении поставщика и при исполнении контракта.

Между тем значительная часть ошибок и неблагоприятных исходов закупочной деятельности не имеет коррупционной природы. Если заказчик нечасто приобретает тот или иной товар, он может упустить оптимальный момент для размещения закупки: своевременное планирование могло бы обеспечить приобретение продукции по более выгодной цене либо с более длительным жизненным циклом [9; 14]. Подобные риски носят сугубо экономический характер и не предполагают чьего-либо умысла.

Специфика правоприменительной культуры по Закону № 223-ФЗ также порождает самостоятельную категорию правовых рисков: часть заказчиков обуславливает соблюдение нормативных требований исключительно угрозой санкций. Медийная среда усугубляет ситуацию, акцентируя внимание преимущественно на случаях уголовного преследования и тем самым закрепляя в профессиональном сообществе сугубо правовую интерпретацию понятия «закупочный риск» [5].

Классификация закупочных рисков. По результатам проведенного исследования предлагается классификация закупочных рисков, разграничивающая явные и неявные риски (табл. 1).

Таблица 1

Классификация закупочных рисков (авторская разработка)

Группа рисков	Виды рисков	Примеры проявления
Явные правовые риски	Нарушение законов № 44-ФЗ и № 223-ФЗ; нарушение КоАП РФ; несоблюдение норм национального режима; нарушения антимонопольного законодательства (картели)	Применение закупочных способов, исключенных из собственного Положения; игнорирование требований о баллах при национальном режиме
Явные организационно-управленческие риски	Сбои в коммуникации между подразделениями; дублирование закупок в территориально распределенных структурах; несоблюдение внутренних регламентов; отсутствие категорийного управления	Параллельное размещение однородных закупок разными подразделениями; отсутствие регулярных запросов от бизнес-заказчиков; недостаточная мотивация специалистов по закупкам
Неявные цифровые риски	Неполнота и недостоверность данных в электронных сервисах; сбои и отказы электронных торговых систем; недостаточная цифровая компетентность персонала; киберугрозы	Ошибки при работе с Единой информационной системой (далее — ЕИС) вследствие низкой ИТ-компетентности; новые формы кибермошенничества в электронных закупках; неактуальность реестровой информации
Неявные риски скрытых затрат	Транзакционные издержки повторных процедур; неучитываемые затраты рабочего времени; упущенная выгода из-за выбора неоптимального времени для закупки; недоучет полной стоимости эксплуатации за весь срок службы (совокупная стоимость владения)	Приобретение более дешевого оборудования с коротким жизненным циклом; многократные повторные аукционы по жизненно важным лекарственным препаратам

Первые две группы: явные правовые и организационно-управленческие риски — поддаются нормативной идентификации и в той или иной мере охвачены существующими системами внутреннего контроля. Неявные риски, напротив, систематически недооцениваются, поскольку их последствия не всегда выражены в форме санкций или прямых убытков, тогда как их суммарный ущерб для экономической безопасности организации может быть весьма значительным [3; 9; 10].

Наиболее значимые риски цифровой среды. Обобщение научных публикаций и материалов правоприменительной практики обнажает парадоксальную тенденцию: заказчики, активно использующие инструменты цифровизации, воспринимают ее одновременно как источник операционных рисков. Среди всего многообразия угроз в качестве трех наиболее значимых устойчиво выделяются риски, непосредственно связанные с цифровой средой.

Первое место занял риск неполноты и недостоверности данных в электронных сервисах. Второе место — риски, обусловленные недостаточной ИТ-компетентностью персонала и отказами электронных систем, что особенно актуально для малых и средних организаций без собственных ИТ-подразделений. Третье место — риск новых форм кибермошенничества. Примечательно, что традиционно доминирующие в регуляторном дискурсе правовые и коррупционные риски не входят в тройку наиболее острых с точки зрения самих заказчиков, что свидетельствует о существенном расхождении между регуляторной повесткой и реальной практикой [9].

Скрытые затраты как угроза экономической безопасности. Особого внимания заслуживает категория рисков скрытых затрат, не отражаемых в традиционной системе учета. Как показывают опубликованные исследования рынка государственных закупок лекарственных средств, при повторном размещении процедур по жизненно важным лекарственным препаратам возникают значительные скрытые затраты: временные затраты специалистов на подготовку и согласование документации, технические и административные издержки [13]. По имеющимся оценкам, совокупный объем таких издержек по отдельным группам препаратов достигает сотен миллионов рублей, что подтверждает масштаб проблемы и ее значимость для экономической безопасности заказчиков.

Проблема совокупной стоимости владения (*Total Cost of Ownership, TCO*) представляет собой еще одно измерение скрытых затрат. При оценке заявок исключительно по цене предложения заказчик может приобрести объект, совокупные эксплуатационные расходы которого существенно превысят аналогичные показатели более дорогого аналога. Концепция *TCO* остается практически неостребованной в системе государственного заказа — главным образом в силу нормативных ограничений, высокой трудоемкости расчетов и нестабильности рыночной конъюнктуры [9; 14].

Информационные риски применения ИИ. Дискуссия о цифровизации закупок нередко сводится к опыту крупных корпораций, располагающих собственными ИТ-департаментами. Вместе с тем уже сегодня доступны общедоступные инструменты на основе больших языковых моделей (*ChatGPT, DeepSeek, YandexGPT, GigaChat*), позволяющие решать практические закупочные задачи без значительных финансовых затрат [11]. Возможности применения ИИ на этапе планирования закупок и сопутствующие риски автоматизации исследованы Н. В. Немцовой, Е. С. и С. С. Стаурскими [15]. Применение данных инструментов не требует глубоких технических знаний — достаточно грамотно сформулированного промпта с указанием роли, задачи, формата ответа и требования верифицируемых источников.

Для объективного сопоставления доступных инструментов на основе больших языковых моделей целесообразно опираться на независимые рейтинги качества. Одним из таких источников выступает открытая краудсорсинговая платформа *LLM Arena*, оценивающая большие языковые модели применительно к русскому языку. Платформа собирает парные сравнения ответов моделей, выполняемые пользователями, и ранжирует модели с помощью модели Брэдли—Терри, отображая их рейтинг по шкале Эло. Ранг (*UB*) представляет собой ранг модели

по верхней границе доверительного интервала: он определяется как единица плюс число моделей, статистически превосходящих данную. Модель *A* считается статистически лучше модели *B*, если нижняя граница ее оценки превышает верхнюю границу оценки модели *B* (при 95%-м доверительном интервале). Фрагмент таблицы лидеров по состоянию на конец 2025 — начало 2026 г. приведен в табл. 2.

Таблица 2

**Фрагмент таблицы лидеров
больших языковых моделей
по версии платформы *LLM Arena***

Ранг (UB)	Модель	<i>Arena Elo</i>	Организация	Лицензия
1	<i>Gemini 3 Pro Preview</i>	1162	<i>Google</i>	Проприетарная
1	<i>Gemini 3.1 Pro Preview</i>	1151	<i>Google</i>	Проприетарная
1	<i>Gemini 2.5 Pro Preview (03-25)</i>	1135	<i>Google</i>	Проприетарная
1	<i>GPT-5.1</i>	1129	<i>OpenAI</i>	Проприетарная
1	<i>Gemini 2.5 Flash Preview (thinking)</i>	1114	<i>Google</i>	Проприетарная
3	<i>GPT-5 Chat</i>	1105	<i>OpenAI</i>	Проприетарная
3	<i>GPT-5.2</i>	1104	<i>OpenAI</i>	Проприетарная
3	<i>Claude Opus 4.1</i>	1101	<i>Anthropic</i>	Проприетарная
5	<i>Claude Sonnet 4.5</i>	1086	<i>Anthropic</i>	Проприетарная
5	<i>GPT-4.1 (2025-04-14)</i>	1086	<i>OpenAI</i>	Проприетарная
5	<i>DeepSeek V3.2</i>	1082	<i>DeepSeek</i>	MIT (открытая)
5	<i>o4-mini (2025-04-16)</i>	1082	<i>OpenAI</i>	Проприетарная
6	<i>Qwen3 Max</i>	1072	<i>Qwen (Alibaba)</i>	<i>Apache 2.0</i> (открытая)
6	<i>DeepSeek V3.1</i>	1066	<i>DeepSeek</i>	MIT (открытая)
6	<i>DeepSeek R1</i>	1063	<i>DeepSeek</i>	Открытая

Примечание: сост. по данным *LLM Arena* (<https://llmarena.ru/>).

Как следует из представленных данных, лидирующие позиции занимают проприетарные зарубежные модели семейств *Gemini* (*Google*), *GPT* (*OpenAI*) и *Claude* (*Anthropic*), тогда как открытые модели *DeepSeek* и *Qwen*, распространяемые под свободными лицензиями (*MIT, Apache 2.0*) и потому пригодные для развертывания в изолированном контуре, располагаются близко к ним по совокупной оценке. Наглядная визуализация доверительных интервалов оценок силы моделей приведена на рисунке.

Вместе с тем для закупочной деятельности определяющим является не столько место модели в рейтинге качества, сколько правовой режим обработки данных (а именно соответствие Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных»), доступность инструмента из Российской Федерации и возможность его развертывания в изолированном контуре. С этих позиций доступные заказчику инструменты целесообразно разделить на три категории: отечественные, зарубежные (китайские) открытые и зарубежные проприетарные. Их сравнительная характеристика приведена в табл. 3.

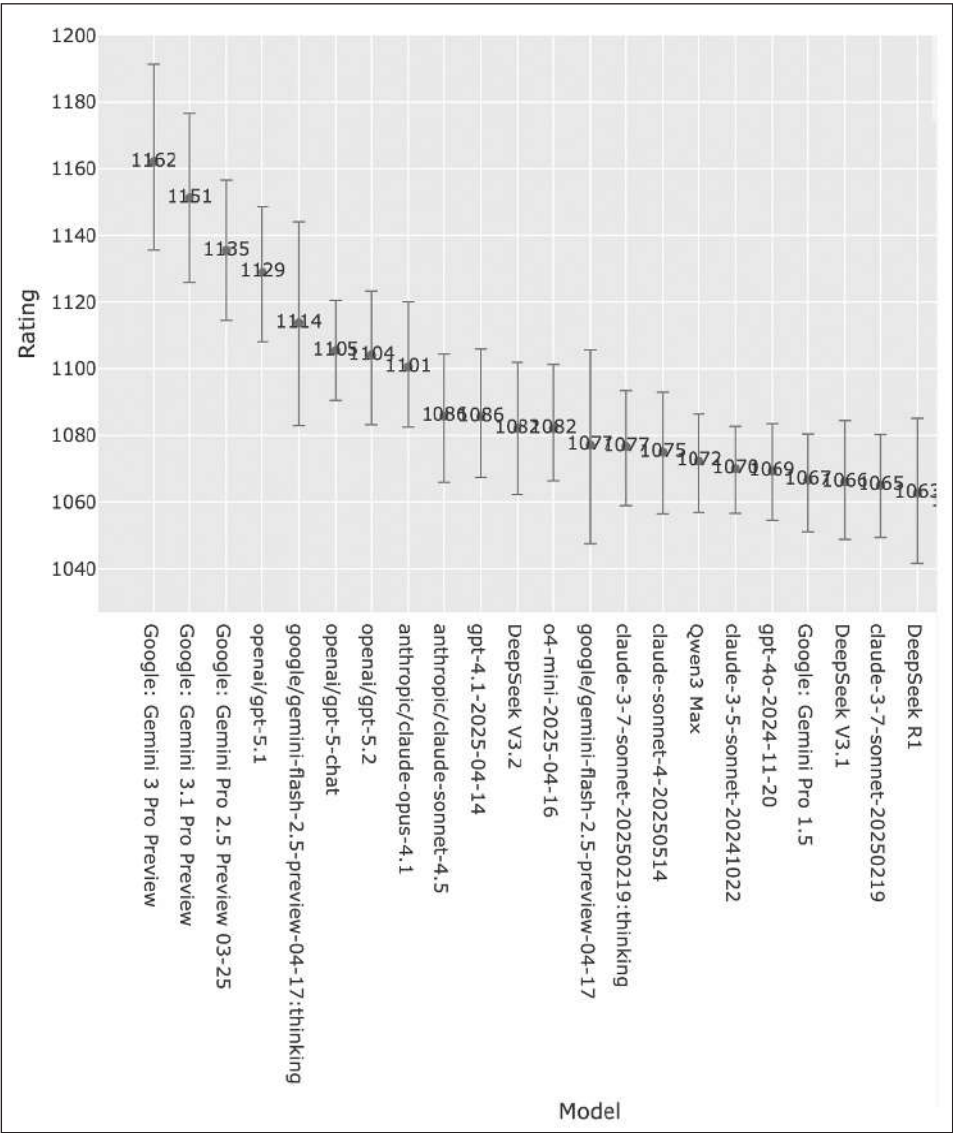


Рис. Доверительные интервалы оценки силы моделей (метод бутстрапа) по данным платформы LLM Arena

Таблица 3

Сравнительная характеристика инструментов на основе больших языковых моделей с точки зрения закупочной практики

Инструмент (категория)	Разработчик, страна	Локализация данных и соответствие Закону № 152-ФЗ	Доступ из РФ	Значимость для закупочной практики
YandexGPT / Alice AI (отечественная)	Яндекс, Россия	Серверы в России, соответствие Закону № 152-ФЗ; корпоративные тарифы с гарантиями безопасности	Полный доступ без VPN, оплата в рублях	Глубокое понимание русскоязычного и нормативного контекста, низкая стоимость API; приемлема для регулируемых закупок, включая работу с персональными данными
GigaChat (отечественная)	ПАО Сбербанк, Россия	Серверы в России, соответствие Закону № 152-ФЗ; открытые веса GigaChat 3 (MIT) и корпоративное развертывание в изолированном контуре	Полный доступ без VPN, оплата в рублях	Понимание русской деловой и правовой лексики, мультимодальность; изолированный контур минимизирует риск утечки конфиденциальных данных
T-Pro / T-Lite (отечественная, открытая)	Т-Банк, Россия	Открытые веса (Apache 2.0); развертывание в собственном контуре без передачи данных вовне	Доступ без VPN; локальное развертывание	Специализация на русскоязычных и финансовых задачах; полный контроль над данными при локальном развертывании, что важно для чувствительной информации
Cotype (отечественная)	MWS AI (МТС), Россия	Серверы в России, соответствие Закону № 152-ФЗ; развертывание во внутреннем контуре организации	Полный доступ без VPN, оплата в рублях	Корпоративная ориентация и мультимодальность (договоры, формы, чертежи); адаптирована под бизнес-сценарии, пригодна для документарных задач заказчика

Инструмент (категория)	Разработчик, страна	Локализация данных и соответствие Закону № 152-ФЗ	Доступ из РФ	Значимость для закупочной практики
<i>DeepSeek / Qwen</i> (открытая, Китай)	<i>DeepSeek; Alibaba</i> , Китай	Публичный сервис хранит данные в Китае; при развертывании в российском облаке или в собственном контуре трансграничной передачи не возникает	Доступ без VPN, бесплатно; открытые веса	Высокое качество и низкая стоимость; для персональных данных пригодны только в варианте локального (изолированного) развертывания на территории Российской Федерации
<i>ChatGPT / Claude / Gemini</i> (зарубежная, проприетарная)	<i>OpenAI; Anthropic; Google</i> , США	Данные обрабатываются на зарубежных серверах; трансграничная передача в «неадекватную» юрисдикцию; требованиям Закона № 152-ФЗ по локализации не соответствует	Только через VPN и иностранные способы оплаты	Наиболее высокие аналитические возможности, однако использование для конфиденциальных и персональных данных заказчика юридически недопустимо; применимы лишь к обезличенным данным

Примечание: сост. автором.

Сопоставление показывает, что выбор инструмента для закупочных задач определяется прежде всего правовым режимом обработки данных, а не только положением модели в рейтинге качества. Для работы с конфиденциальной и персональной информацией заказчика приемлемы прежде всего отечественные решения (*YandexGPT, GigaChat, T-Pro, Cotype*), обеспечивающие хранение данных на территории Российской Федерации, а также открытые модели, развернутые в изолированном контуре. Зарубежные проприетарные сервисы, несмотря на лидирующие позиции в рейтинге, для этих целей юридически неприемлемы и допустимы лишь при работе с обезличенными или общедоступными данными.

Апробация трех типовых задач показала практический потенциал ИИ, а именно:

- Задача 1: **проверка технического задания на соответствие принципу конкурентности**. Из четырех предложений, подобранных языковой моделью для обоснования начальной (максимальной) цены контракта, три оказались достоверными, одно было сгенерировано без фактического основания.

- Задача 2: **анализ договора**. По реально заключенному договору из реестра ЕИС языковая модель идентифицировала 17 условий с повышенными рисками для поставщика.

- Задача 3: **подготовка возражений на жалобу Федеральной антимонопольной службы**. Модель предложила два аргумента сверх использованных заказчиком в реальной ситуации, один из которых, по экспертной оценке, мог изменить исход рассмотрения дела в его пользу.

Вместе с тем применение ИИ сопряжено с комплексом специфических информационных рисков, систематизированных в табл. 4.

Таблица 4

Информационные риски применения ИИ в закупочной деятельности (авторская разработка)

Вид риска	Механизм возникновения	Меры снижения
Галлюцинации языковой модели	Языковая модель комбинирует статистически вероятные последовательности токенов, не обладая логическим пониманием предметной области, что порождает достоверно оформленный, но фактически недостоверный контент	Обязательная верификация каждого фактического утверждения по первоисточнику; запрос модели указывать ссылки с последующей их проверкой
Утечка конфиденциальных данных	Загружаемые в публичные ИИ-сервисы документы потенциально включаются в обучающие датасеты, создавая ненулевую вероятность воспроизведения чувствительных данных в ответах третьим лицам	Использование корпоративных ИИ-решений с изолированным контуром данных; анонимизация документов перед загрузкой в публичные сервисы
Технологическая зависимость	Внезапная блокировка зарубежных ИИ-сервисов ведет к разрыву операционных процессов, выстроенных на базе данных инструментов	Формирование резервного контура на базе отечественных ИИ-платформ; недопущение монозависимости от единственного провайдера
Эффект «черного ящика»	Языковая модель зачастую не может объяснить логику выводов. Юридически значимые решения (протоколы комиссии, контракты) требуют верифицируемого фактического основания	Использование результатов ИИ исключительно как вспомогательного материала; запрос обоснования каждого вывода с подтверждением источников
Переучивание на смещенных данных	Если обучающая выборка содержит аномалии (нетипичные ценовые всплески), модель формирует систематически ошибочные прогнозы, принимаемые за закономерность	Предварительная очистка исторических данных; выявление и устранение статистических аномалий; привлечение экспертов для интерпретации результатов
Отравление обучающих данных	Недобросовестные поставщики целенаправленно формируют «цифровой след» — массово публикуют прайс-листы, накручивают отзывы — с целью манипулирования результатами ИИ-анализа заказчика	Диверсификация источников данных; кросс-верификация через независимые реестры (Федеральная налоговая служба, арбитражные суды, ЕИС); формирование критической культуры работы с открытыми данными

На основе анализа выявленных рисков сформулированы шесть принципов безопасного применения ИИ-инструментов:

1) принцип обязательной верификации — ни одно фактическое утверждение ИИ не используется без проверки по первоисточнику;

2) принцип объяснимости — результаты принимаются при наличии верифицируемой фактической базы;

3) принцип технологической независимости — обязательное наличие резервного контура на базе отечественных платформ;

4) принцип информационной гигиены — разграничение открытых и конфиденциальных данных при работе с публичными сервисами;

5) принцип постепенного освоения — начало с низкорисковых задач;

6) принцип кадрового приоритета — ИИ повышает эффективность специалиста, но не замещает его профессиональное суждение и юридическую ответственность.

Дифференцированные подходы к риск-ориентированному управлению. Предлагаемая система строится на принципе соразмерности, при котором применяемый инструментарий должен соответствовать масштабу организации и ее ресурсным возможностям.

Для малых организаций наиболее доступным инструментом является система чек-листов, структурированных по этапам закупочного процесса [планирование, обоснование начальной (максимальной) цены контракта/договора, разработка документации, рассмотрение заявок, исполнение контракта], дополненная верифицируемыми ИИ-подсказками. Важно подчеркнуть: автоматизация не отменяет логику содержательных этапов, а чек-лист должен охватывать не только формальные требования, но и параметры качества закупки.

Для организаций среднего масштаба рекомендуется переход к полноценному риск-ориентированному управлению: карты рисков с формализованными процедурами идентификации и оценки последствий, категорийное управление, а также система *KPI* по удовлетворенности внутренних бизнес-заказчиков. Такой подход позволяет перейти от реагирования на отдельные инциденты к системному управлению закупочными рисками на всех этапах закупочного цикла [6; 10].

Крупные организации располагают ресурсами для формирования трехуровневой системы защиты (закупщики — комплаенс — внутренний аудит) и развертывания предиктивной аналитики: прогнозирование вероятности несостоятельности торгов, оценка рисков расторжения контракта по профилю контрагента, построение сетевых графов аномальных связей по кодам ОКПД 2, формирование дашбордов поддержки управленческих решений [10; 16].

Заключение

Проведенное исследование позволяет сформулировать следующие **выводы**:

1. Существующий нормативный дискурс избыточно сфокусирован на правовых и коррупционных рисках, оставляя в тени организационно-управленческие, экономические и информационные риски, непосредственно влияющие на устойчивость закупочной деятельности.

2. Цифровизация закупок порождает специфические риски — информационные, операционные, киберриски, — которые заказчики воспринимают как более острые угрозы, чем традиционные правовые.

3. Феномен скрытых затрат при повторных закупочных процедурах представляет реальную угрозу экономической безопасности: по данным опубликованных исследований, на рынке лекарственного обеспечения их совокупный объем по отдельным группам препаратов достигает сотен миллионов рублей [13].

4. Применение ИИ-инструментов несет не только операционные выгоды, но и новый класс информационных рисков (галлюцинации, утечки данных, технологическая зависимость, «черный ящик», переучивание на смещенных данных, отравление данных), управление которыми требует формирования системы принципов безопасного использования.

5. Внедрение риск-ориентированного управления должно быть дифференцировано: малые заказчики — чек-листы и верифицируемые ИИ-подсказки; средние — карты рисков и категорийное управление; крупные — многоуровневый комплаенс и предиктивная аналитика.

Дальнейшие исследования целесообразно направить на разработку методики количественной оценки закупочных рисков для организаций различных правовых форм, а также на верификацию прогностической силы языковых моделей в различных отраслевых сегментах.

СПИСОК ИСТОЧНИКОВ

1. Андреева Л. В. Государственные закупки в России: правовое регулирование и меры по его совершенствованию. М. : Проспект, 2019. 232 с.
2. Кикавец В. В. Публичные закупки в практике зарубежных стран. М. : Проспект, 2021. 176 с.
3. Балаева О. Н., Яковлев А. А., Родионова Ю. Д., Есаулов Д. М. Трансакционные издержки в сфере госзакупок РФ: оценка на макроуровне на основе микроданных // Журнал институциональных исследований. 2018. Т. 10. № 3. С. 58—84. DOI: 10.17835/2076-6297.2018.10.3.058-084.
4. Островная М. В., Подколзина Е. А. Ограничения конкуренции на примере российских государственных закупок // Вопросы экономики. 2018. № 2. С. 56—73. DOI: 10.32609/0042-8736-2018-2-56-73.
5. Яковлев А. А., Балаева О. Н., Родионова Ю. Д., Ткаченко А. В. Проблемы и эффективность госзакупок глазами их участников // ЭКО. 2020. № 11. С. 83—103. DOI: 10.30680/ECO0131-7652-2020-11-83-103.
6. Смотрицкая И., Черных С. Современные концепции государственного управления и институциональные риски // Общество и экономика. 2020. № 6. С. 41—52. DOI: 10.31857/S020736760010114-4.
7. Коваленко С. Н., Семенова Н. А., Коваленко Ю. Н., Сивкова А. Е. Управление рисками и процессом противодействия коррупции в системе государственных закупок // Вестник Алтайской академии экономики и права. 2024. № 9. Ч. 2. С. 213—221. DOI: 10.17513/vaael.3723.
8. Петрушевская В. В., Арчигова Я. О. Управление рисками в системе государственных закупок бюджетного учреждения // Финансовый менеджмент. 2025. № 4. С. 4—13.

9. Созаева Д. А. Неявные риски в системе государственных и муниципальных закупок и методология их выявления // Проблемы теории и практики управления. 2021. № 6. С. 250—262.
10. Созаева Д. А. Современная концепция риск-ориентированного управления регулируемыми закупками // Проблемы анализа риска. 2023. Т. 20. № 6. С. 58—68.
11. Казанцев Д. А., Догнал П., Догнал-мл. П. Использование искусственного интеллекта для проведения конкурентных закупок: проблемы правового регулирования // Journal of Digital Technologies and Law. 2024. Т. 2. № 3. С. 585—610. DOI: 10.21202/jdtl.2024.30.
12. Wachter S., Mittelstadt B., Russell C. Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR // Harvard Journal of Law & Technology. 2018. Vol. 31. No. 2. Pp. 841—887.
13. Созаева Д. А., Денисова А. И., Александров Г. А., Гончар К. В. Совершенствование методологии оценки экономической эффективности государственных закупок лекарственных средств // Финансовый журнал. 2023. Т. 15. № 4. С. 63—81. DOI: 10.31107/2075-1990-2023-4-63-81.
14. Кикавец В. В. История правового регулирования государственных закупок в России: финансовый аспект. М.: Проспект, 2019. 128 с.
15. Немцова Н. В., Стаурский Е. С., Стаурский С. С. Возможности искусственного интеллекта на этапе планирования государственных закупок // Управленческий учет. 2023. № 6. С. 223—229. DOI: 10.25806/uu62023223-229.
16. Яковлев А. А., Ткаченко А. В., Родионова Ю. Д. Причины заключения контрактов с заранее определенными поставщиками: результаты эмпирического исследования // Вопросы экономики. 2018. № 10. С. 90—105. DOI: 10.32609/0042-8736-2018-10-90-105.

REFERENCES

1. Andreeva L. V. Public procurement in Russia: legal regulation and measures for its improvement. Moscow, Prospekt, 2019. 232 p. (In Russ.)
2. Kikavets V. V. Public procurement in the practice of foreign countries. Moscow, Prospekt, 2021. 176 p. (In Russ.)
3. Balaeva O. N., Yakovlev A. A., Rodionova Yu. D., Esaulov D. M. Transaction Costs in the Public Procurement in Russia: Macrolevel Assessment Based on Microdata. *Zhurnal institutsional'nykh issledovaniy = Journal of Institutional Studies*. 2018;10(3):58—84. (In Russ.) DOI: 10.17835/2076-6297.2018.10.3.058-084.
4. Ostrovskaya M. V., Podkolzina E. A. Restrictions of competition: The case of Russian public procurement. *Voprosy Ekonomiki*. 2018;2:56—73. (In Russ.) DOI: 10.32609/0042-8736-2018-2-56-73.
5. Yakovlev A. A., Balaeva O. N., Rodionova Yu. D., Tkachenko A. V. Problems and Efficiency of Public Procurement through the Eyes of their Participants. *ECO*. 2020;11:83—103. (In Russ.) DOI: 10.30680/ECO0131-7652-2020-11-83-103.
6. Smotrinskaya I., Chernyh S. Modern concepts of public administration and institutional risks. *Obshchestvo i ekonomika = Society and Economics*. 2020;6:41—52. (In Russ.) DOI: 10.31857/S020736760010114-4.
7. Kovalenko S. N., Semenova N. A., Kovalenko Y. N., Sivkova A. E. Risk management and anti-corruption process in the public procurement system. *Vestnik Altaiskoi akademii ekonomiki i prava = Bulletin of the Altai Academy of Economics and Law*. 2024;9-2:213—221. (In Russ.) DOI: 10.17513/vaael.3723.
8. Petrushevskaya V. V., Archikova Ya. O. Risk management in the public procurement system of a budget institution. *Finansovyi menedzhment = Financial management*. 2025;4:4—13. (In Russ.)
9. Sozaeva D. A. Implicit risks in the system of state and municipal procurement and the methodology for identifying them. *Problemy teorii i praktiki upravleniya*. 2021;6:250—262. (In Russ.)
10. Sozaeva D. A. Modern concept of risk-based management of regulated procurement. *Problemy analiza riska = Issues of Risk Analysis*. 2023;20(6):58—68. (In Russ.)
11. Kazantsev D. A., Dohnal P., Dohnal Jr. P. Using Artificial Intelligence for Competitive Procurements: Legal Regulation Issues. *Journal of Digital Technologies and Law*. 2024;2(3):585—610. DOI: 10.21202/jdtl.2024.30.
12. Wachter S., Mittelstadt B., Russell C. Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology*. 2018;31(2):841—887.
13. Denisova A. I., Sozaeva D. A., Gonchar K. V., Aleksandrov G. A. Improving the Methodology for Assessing the Economic Efficiency of Public E-procurement of Medicines. *Finansovyi zhurnal = Financial Journal*. 2023;15(4):63—81. (In Russ.) DOI: 10.31107/2075-1990-2023-4-63-81.
14. Kikavets V. V. History of legal regulation of public procurement in Russia: financial aspect. Moscow, Prospekt, 2019. 128 p. (In Russ.)
15. Nemtsova N. V., Staursky E. S., Staursky S. S. Artificial intelligence capabilities at the stage of public procurement planning. *Upravlencheskii uchët = Management Accounting*. 2023;6:223—229. (In Russ.) DOI: 10.25806/uu62023223-229.
16. Yakovlev A. A., Tkachenko A. V., Rodionova Yu. D. Reasons for contracting predetermined suppliers: Results of an empirical study. *Voprosy Ekonomiki*. 2018;10:90—105. (In Russ.) DOI: 10.32609/0042-8736-2018-10-90-105.

Статья поступила в редакцию 10.06.2026; одобрена после рецензирования 05.07.2026; принята к публикации 06.07.2026.
The article was submitted 10.06.2026; approved after reviewing 05.07.2026; accepted for publication 06.07.2026.