УДК 338.24:004.89:658.5

УПРАВЛЯЕМАЯ ИНТЕГРАЦИЯ AI-АГЕНТОВ В БИЗНЕС-ПРОЦЕССЫ ОРГАНИЗАЦИИ: АРХИТЕКТУРА, МЕТОДИКА И РИСК-ОРИЕНТИРОВАННАЯ ОЦЕНКА ЭФФЕКТА

Оригинальная статья
Original paper

Е. С. ПИСКУН, А. А. АЗИЗОВ, Е. В. КРЯЧЕВ
Белорусский государственный университет информатики и радиоэлектроники
(г. Минск, Республика Беларусь)

Аннотация. Цель исследования — разработка воспроизводимой архитектуры и методики управляемой интеграции AI-агентов в бизнес-процессы организации. Актуальность обусловлена тем, что 88 % [17] организаций используют ИИ хотя бы в одной бизнес-функции, однако полностью масштабировали AI-решения только 7 % [18]. Эмпирические данные сервисного сектора показывают рост производительности при применении generative AI на 14 % [19] в среднем и на 34 % [19] у менее опытных работников. В статье предложен контур, объединяющий событийные данные ERP/CRM/BPM/Service Desk, XES/OCEL-журналы, BPMN-модели, process mining, conformance checking, what-if simulation, RAG и governance-механизмы. Научная новизна состоит в формализации цикла discover-audit-simulate-recommend-control, ролевой архитектуры из пяти специализированных агентов и риск-ориентированной модели оценки эффекта. Расчетный сценарий обработки заявок показал сокращение длительности цикла с 44 до 27 мин. (–38,6 %), снижение трудоемкости аналитика с 10 до 4 мин. (–60,0 %) и рост покрытия отклонений с 57 до 91 % (+34 п.п.).

Ключевые слова. AI-агенты, бизнес-процессы, process mining, BPMN, XES, OCEL, conformance checking, what-if simulation, RAG, governance, Human-in-the-Loop.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

CONTROLLED INTEGRATION OF AI AGENTS INTO ORGANIZATIONAL BUSINESS PROCESSES: ARCHITECTURE, METHOD AND RISK-ORIENTED EFFECT ASSESSMENT

E. S. PISKUN, A. A. AZIZOV, E. V. KRYCHEV
Belarusian State University of Informatics and Radioelectronics
(Minsk, Republic of Belarus)

Abstract. The paper develops a reproducible architecture and method for the controlled integration of AI agents into organizational business processes. The topic is relevant because 88% [17] of organizations report AI use in at least one business function, whereas only 7% [18] have fully scaled AI across the enterprise. Evidence from service work shows that generative AI increases productivity by 14% [19] on average and by 34% [19] for novice and low-skilled workers. The proposed framework combines ERP/CRM/BPM/Service Desk event data, XES/OCEL logs, BPMN models, process mining, conformance checking, what-if simulation, RAG and governance mechanisms. The contribution lies in the discover-audit-simulate-recommend-control cycle, a five-agent role architecture and a risk-oriented effect assessment model. The illustrative application-handling scenario demonstrates a cycle-time reduction from 44 to 27 minutes, analyst-effort reduction from 10 to 4 minutes per case, and deviation-coverage growth from 57% to 91%.

Keywords. AI agents, business processes, process mining, BPMN, XES, OCEL, conformance checking, what-if simulation, RAG, governance, Human-in-the-Loop.

1. Введение

Распространение генеративного ИИ и агентных систем переводит корпоративную автоматизацию от точечных экспериментов к задаче управляемого организационного внедрения.

По данным McKinsey Global Survey, в 2025 г. использование ИИ хотя бы в одной бизнес-функции достигло 88 % [17], однако полномасштабное внедрение на уровне всей организации зафиксировано только у 7 % респондентов [18]. Следовательно, ключевым ограничением становится не доступность моделей, а способность встроить их в регламентированные workflow, KPI и контуры контроля.

Для сервисных процессов AI-агенты особенно значимы при наличии массовых повторяемых кейсов, цифрового следа, SLA и базы знаний. В исследовании на выборке 5179 сотрудников клиентской поддержки доступ к generative AI повышал производительность в среднем на 14 %, а у менее опытных работников — на 34 % [19]. При этом эффект неоднороден и зависит от типа задач, зрелости данных и качества организационного сопровождения.

Автономизация процессов одновременно увеличивает риск ошибок, утечек данных и действий с избыточными полномочиями. Агент, подключенный к API, документам и RAG-хранилищам, должен рассматриваться не как универсальный чат-ассистент, а как ограниченный компонент процессной архитектуры, где правила доступа, источники данных, допустимые инструменты и ответственность владельца процесса формализованы заранее [12–16].

В методике риск-ориентированной оценки LLM-решений для сервисного сектора экономический эффект декомпозирован на экономию времени, повышение качества и предотвращенные потери [20]. В работе по Isolated Multiagent Arbitration показано, что финансовая оценка автономных агентов должна учитывать prompt injection, RAG poisoning и excessive agency как источники остаточного риска [21]. Настоящая статья использует эти положения для построения целостного контура интеграции AI-агентов в бизнес-процессы.

Цель работы — разработать архитектуру и методику интеграции AI-агентов, обеспечивающие автоматизацию повторяемых задач анализа, контроля, сценарной оценки и подготовки рекомендаций при сохранении аудируемости, безопасности и управленческой ответственности.

2. Теоретическая база и исследовательский разрыв

Process mining рассматривает события информационных систем как основу для восстановления фактической модели процесса; базовыми задачами являются process discovery, conformance checking и enhancement [1; 2]. Для интероперабельности event logs используется стандарт XES [3], а для процессов с несколькими взаимосвязанными объектами применяется OCEL 2.0 [4].

Нормативный слой процесса задается BPMN 2.0.2 / ISO/IEC 19510 [5], тогда как сценарная оценка изменений опирается на методы business process management, дискретно-событийной и агентной симуляции [6–9; 11]. Исследования возможностей LLM в process mining подтверждают перспективность направления, но в основном оценивают отдельные функции моделей, а не организационный контур их применения [10].

Безопасное внедрение AI-агентов требует управления рисками на уровне системы. NIST AI RMF 1.0 определяет функции govern, map, measure и manage [12], профиль NIST AI 600-1 уточняет риски generative AI [13], а ISO/IEC 42001 и ISO/IEC 23894 задают требования к менеджменту и оценке AI-рисков [14; 15]. OWASP Top 10 for LLM Applications выделяет prompt injection, sensitive information disclosure, excessive agency и weaknesses of vector/embedding systems как критичные классы угроз [16].

Исследовательский разрыв состоит в отсутствии компактного шаблона, который связывает событийные данные, нормативную модель, симуляцию, генерацию рекомендаций и governance-контроль в одном воспроизводимом цикле. Предлагаемый подход закрывает этот разрыв за счет разделения аналитической, генеративной и контрольной функций.

Таблица 1. Сравнение подходов к автоматизации анализа бизнес-процессов

Подход	Сильная сторона	Ограничение	Роль в предлагаемом контуре
Ручной бизнес-анализ	Контекстная экспертиза и анализ исключений	Низкая масштабируемость	Постановка правил и HITL-проверка
Process mining	Проверяемая фактическая модель и метрики	Требуются качественные event logs	Discovery и conformance checking
Одиночный LLM-ассистент	Быстрое формирование объяснений и текста	Слабая воспроизводимость без логов и RBAC	RAG-пояснение и проект рекомендации
Мультиагентный контур	Связь данных, BPMN, симуляции и контроля	Требует governance-инфраструктуры	Целевой шаблон внедрения

3. Требования к организации, процессу и данным

Наиболее рациональным объектом внедрения являются средние и крупные сервисные организации с повторяемыми обращениями, формализованными маршрутами и цифровыми журналами выполнения операций. Минимальный состав данных включает идентификатор кейса, действие, временные метки, статус, исполнителя и атрибуты контекста; для межобъектных процессов целесообразно применять OCEL, позволяющий связать событие с заявкой, клиентом, договором или платежом [3; 4].

Ключевые ограничения связаны с качеством данных: отсутствием сквозного case ID, неполными временными метками, дублированием событий, несогласованными справочниками и действиями вне информационного контура. При таких дефектах агентная система будет воспроизводить ошибки исходных данных, поэтому нормализация и валидация event logs являются обязательным этапом методики [1–4].

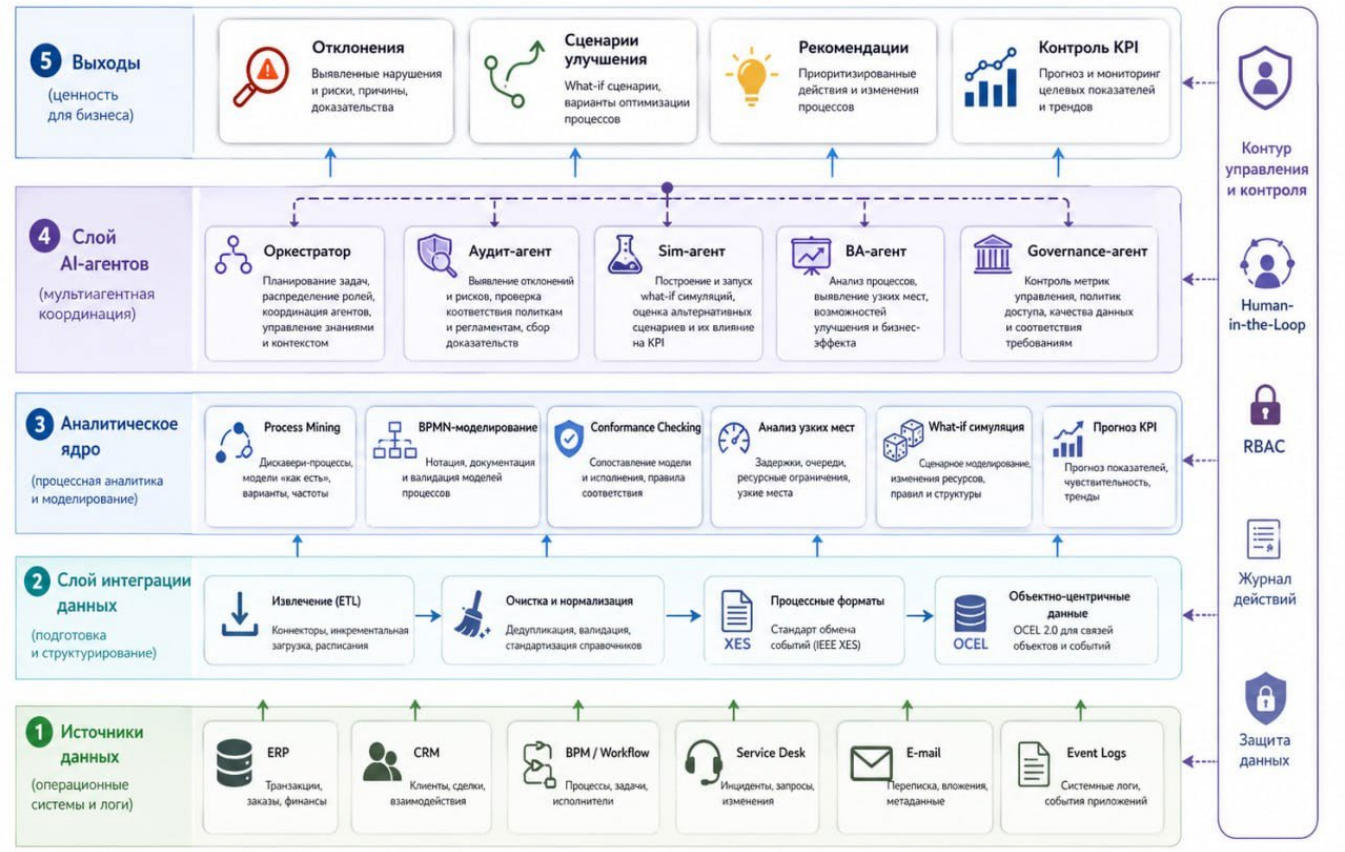
Таблица 2. Критерии готовности процесса к пилотному внедрению

Блок	Минимальное условие	Признак достаточности
Данные	Есть case ID, статусы, роли и временные метки	Не менее 80 % кейсов восстанавливаются в единую трассу
Нормативный слой	Есть BPMN, SLA или контрольные правила	Отклонения проверяются машинно, а не только вручную
Интеграция	Доступны API, выгрузки или шлюз данных	Поступление данных регулярно и версионируется
База знаний	Регламенты доступны для RAG	Документы имеют владельца, дату версии и уровень доверия
Governance	Определены RBAC, audit trail и HITL	Критические действия невозможны без подтверждения

4. Архитектура управляемого мультиагентного контура

Архитектура включает пять уровней: источники данных, интеграционный слой, аналитическое ядро, слой AI-агентов и слой бизнес-выходов. Поперечный контур управления и контроля задает RBAC, Human-in-the-Loop, журналирование и защиту данных, что соответствует риск-ориентированной логике NIST, ISO и OWASP [12–16]. Логика архитектуры представлена на рис. 1.

Рис. 1. Вариант 1 — слоистая архитектура мультиагентной системы аудита и симуляции бизнес-процессов



Источник: разработано авторами.

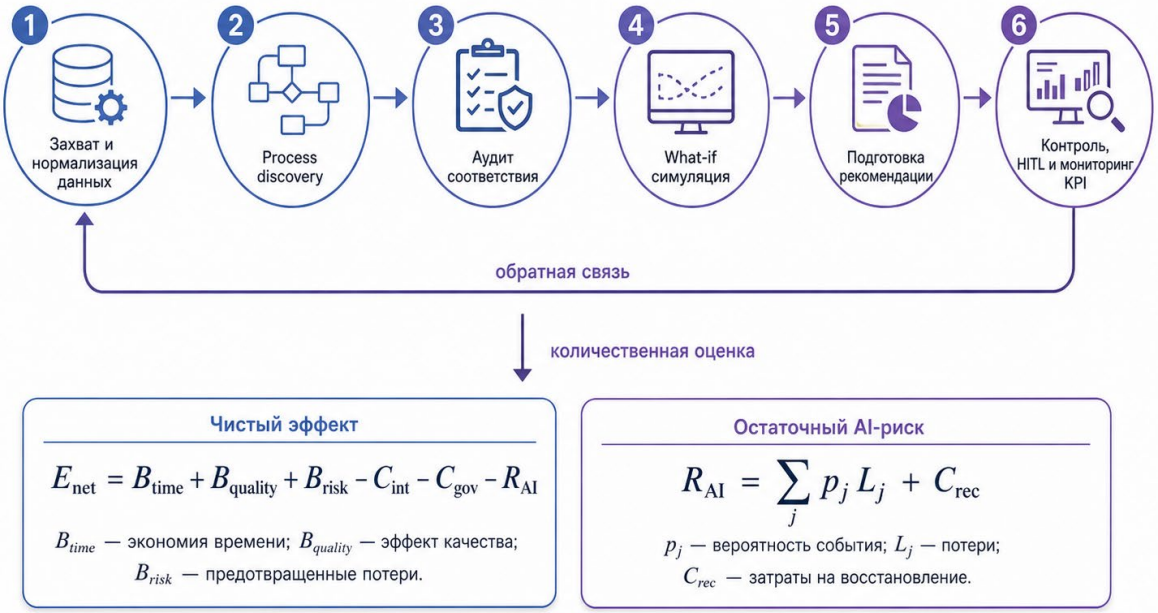
На аналитическом уровне выполняются process discovery, conformance checking, анализ узких мест и what-if simulation [1; 2; 8; 11]. Агентный слой представлен пятью ролями: оркестратор распределяет задачи; аудит-агент выявляет отклонения; sim-агент оценивает заранее заданные сценарии; BA-агент формирует проверяемую рекомендацию; governance-агент контролирует права, допустимые инструменты и необходимость эскалации. Такое разделение исключает прямое смешение генерации текста и исполнения действий.

Минимальный технологический стек включает коннекторы к ERP/CRM/BPM/Service Desk, хранилище событий, модуль XES/OCEL, BPMN-репозиторий, process mining engine, симуляционный модуль, RAG-хранилище, API-шлюз tool-calling, сервис аутентификации и корпоративный audit trail. Для процессов с персональными данными предпочтительна локальная или гибридная инфраструктура с ограничением внешней передачи данных.

5. Методика интеграции и риск-ориентированная оценка эффекта

Методика строится как цикл discover-audit-simulate-recommend-control: захват и нормализация событий; восстановление фактической модели; аудит соответствия BPMN/SLA; сценарная симуляция; подготовка рекомендации; постконтроль KPI и обновление правил. В отличие от разового аналитического отчета цикл возвращает результаты в процессный мониторинг и формирует основу непрерывного улучшения.

Рис. 2. Методический цикл интеграции AI-агентов и риск-ориентированной оценки эффекта



Источник: разработано авторами

(1) T_case = Σ_{i=1}^{n} t_i. [6–9]

(2) R_ready = 0,25D + 0,20P + 0,20I + 0,20G + 0,15E. [5–7; 12–15]

(3) E_net = B_time + B_quality + B_risk – C_int – C_gov – R_AI. [12; 15; 20; 21]

(4) R_AI = Σ_j p_j L_j + C_rec. [12–16; 21]

(5) B_time = N(T_before – T_after)C_min k_capture. [20]

(6) K_dev = D_found / D_total.

В формуле (1) длительность кейса определяется суммой этапов; формула (2) агрегирует готовность данных (D), формализованность процесса (P), интеграционную готовность (I), уровень governance (G) и измеримость эффекта (E). При R_ready < 0,6 приоритетом является подготовка данных; диапазон 0,6–0,8 соответствует ограниченному пилоту; значение выше 0,8 указывает на возможность масштабирования.

Формула (3) трактует чистый эффект как разность выгод, интеграционных и governance-затрат и остаточного AI-риска. Формула (4) задает риск в виде ожидаемых потерь по классам событий; она корректнее простой аддитивной записи частных рисков, поскольку явно связывает вероятность p_j и величину потерь L_j. Формулы (5) и (6) используются для детализации экономии времени и покрытия отклонений.

Таблица 3. Расчетный сценарий обработки заявок

Этап	До, мин.	После, мин.	Механизм изменения
Регистрация и классификация	5	4	Извлечение сущностей и маршрутизация по шаблону
Поиск регламента и истории кейса	12	5	RAG по верифицированной базе знаний
Проверка SLA и отклонений	10	6	Conformance checking и rule engine
Сценарий решения и KPI-прогноз	12	8	Ограниченный набор what-if сценариев
Согласование и фиксация	5	4	Шаблон рекомендации и HITL-контроль
Итого	44	27	Сокращение на 17 мин., или 38,6 %

В расчетном сценарии длительность обработки заявки снижается с 44 до 27 мин. (–38,6 %), трудоемкость аналитика — с 10 до 4 мин. на кейс (–60,0 %), а покрытие отклонений — с 57 до 91 % (+34 п.п.). Эти значения не являются универсальным бенчмарком; они демонстрируют порядок эффекта для регламентированного сервисного процесса и требуют калибровки на фактических event logs организации. Направление эффекта согласуется с эмпирическими данными о росте производительности в сервисных задачах при применении generative AI [19].

6. Заключение

В статье предложен воспроизводимый контур интеграции AI-агентов в бизнес-процессы организации. Он включает 5 архитектурных уровней, 5 специализированных агентных ролей и 6 этапов методического цикла. Научная новизна состоит в соединении событийных журналов, BPMN-моделей, conformance checking, what-if simulation, RAG-рекомендаций и governance-контроля в единой риск-ориентированной архитектуре.

Количественные ориентиры подтверждают актуальность задачи: 88 % организаций уже используют ИИ хотя бы в одной бизнес-функции [17], но только 7 % масштабировали такие решения на уровне предприятия [18]. В сервисном секторе generative AI повышает производительность на 14 % в среднем и на 34 % у менее опытных сотрудников [19]. В авторском расчетном сценарии длительность кейса уменьшается на 17 мин. (с 44 до 27 мин.), трудоемкость аналитика — на 6 мин. (с 10 до 4 мин.), а покрытие отклонений возрастает на 34 п.п. (с 57 до 91 %).

Практическая ценность подхода состоит в том, что решение о внедрении связывается не с декларативным уровнем автоматизации, а с измеримыми параметрами: R_ready, T_case, E_net, R_AI, B_time и K_dev. Наиболее обоснованным является внедрение в повторяемые, регламентированные и хорошо журналируемые процессы, где не менее 80 % кейсов восстанавливаются в единую трассу, критические действия проходят HITL-контроль, а все рекомендации имеют audit trail и ссылки на источники.

Список литературы / References

1. van der Aalst W. M. P. Process Mining: Data Science in Action. 2nd ed. Berlin: Springer, 2016. 467 p. DOI: 10.1007/978-3-662-49851-4.
2. van der Aalst W. M. P. et al. Process Mining Manifesto // Business Process Management Workshops. Lecture Notes in Business Information Processing. 2012. Vol. 99. P. 169–194. DOI: 10.1007/978-3-642-28108-2_19.
3. IEEE Std 1849-2023. IEEE Standard for eXtensible Event Stream (XES) for Achieving Interoperability in Event Logs and Event Streams. IEEE, 2023. DOI: 10.1109/IEEESTD.2023.10267858.
4. Berti A., Koren I., Adams J. N. et al. OCEL (Object-Centric Event Log) 2.0 Specification. arXiv:2403.01975. 2024.
5. Object Management Group. Business Process Model and Notation (BPMN). Version 2.0.2. 2013; ISO/IEC 19510:2013.
6. Dumas M., La Rosa M., Mendling J., Reijers H. A. Fundamentals of Business Process Management. 2nd ed. Berlin: Springer, 2018. 527 p. DOI: 10.1007/978-3-662-56509-4.

7. Weske M. Business Process Management: Concepts, Languages, Architectures. 4th ed. Berlin: Springer, 2024. 455 p. DOI: 10.1007/978-3-662-69518-0.
8. Rosenthal K., Ternes B., Strecker S. Business Process Simulation on Procedural Graphical Process Models // Business & Information Systems Engineering. 2021. Vol. 63. P. 569–602. DOI: 10.1007/s12599-021-00690-3.
9. Banks J., Carson J. S., Nelson B. L., Nicol D. M. Discrete-Event System Simulation. 5th ed. Upper Saddle River: Pearson, 2010. 640 p.
10. Berti A., Kourani H., Hafke H., Li C.-Y., Schuster D. Evaluating Large Language Models in Process Mining: Capabilities, Benchmarks, and Evaluation Strategies // Enterprise, Business-Process and Information Systems Modeling. LNBIP. 2024. Vol. 511. P. 13–21. DOI: 10.1007/978-3-031-61007-3_2.
11. Kirchdorfer L., Blümel R., Kampik T., van der Aa H., Stuckenschmidt H. AgentSimulator: An Agent-based Approach for Data-driven Business Process Simulation. arXiv:2408.08571. 2024.
12. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg: National Institute of Standards and Technology, 2023. DOI: 10.6028/NIST.AI.100-1.
13. Autio C., Schwartz R., Dunietz J., Jain S., Stanley M., Tabassi E., Hall P., Roberts K. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. NIST AI 600-1. Gaithersburg: National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.AI.600-1.
14. ISO/IEC 42001:2023. Information technology — Artificial intelligence — Management system. Geneva: ISO/IEC, 2023.
15. ISO/IEC 23894:2023. Information technology — Artificial intelligence — Guidance on risk management. Geneva: ISO/IEC, 2023.
16. OWASP Foundation. OWASP Top 10 for Large Language Model Applications. Version 2025. Mode of access: https://genai.owasp.org/llm-top-10/. Date of access: 03.05.2026.
17. Singla A., Sukharevsky A., Hall B., Yee L., Chui M. The state of AI in 2025: Agents, innovation, and transformation // McKinsey & Company. 2025. Mode of access: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai. Date of access: 03.05.2026.
18. McKinsey & Company. AI at work but not at scale // Week in Charts. 2025. Mode of access: https://www.mckinsey.com/featured-insights/week-in-charts/ai-at-work-but-not-at-scale. Date of access: 03.05.2026.
19. Brynjolfsson E., Li D., Raymond L. R. Generative AI at Work. NBER Working Paper No. 31161. 2023. DOI: 10.3386/w31161.
20. Пискун Е., Крячев Е., Азизов А. Риск-ориентированная оценка экономической эффективности LLM в сервисном секторе Республики Беларусь // Наука и инновации. 2026. № 3. С. 36–44. DOI: 10.29235/1818-9857-2026-03-36-44.
21. Пискун Е. С., Азизов А. А., Крячев Е. В. Методика оценки финансовых рисков организаций на основе внедрения Isolated Multiagent Arbitration // Цифровая трансформация. 2026. Т. 22, № 6. С. XX–XX.