

ОРИГИНАЛЬНАЯ СТАТЬЯ



DOI: 10.26794/2408-9303-2026-13-2-69-79
УДК 657.6;65.012.7(045)
JEL G30

Трансформация внутреннего аудита в эпоху искусственного интеллекта

М.Н. Семиколенова^а, И.Н. Санникова^б

^а Национальный исследовательский университет «МЭИ», Москва, Российская Федерация;

^б Алтайский государственный университет, Барнаул, Российская Федерация

АННОТАЦИЯ

Современное развитие технологий искусственного интеллекта (ИИ) ставит организации перед дилеммой: с одной стороны, повышение эффективности и оперативности бизнес-процессов за счет внедрения новых инструментов, с другой — угроза возникновения стратегических рисков в результате их применения. Баланс существующих возможностей и рисков способна обеспечить грамотно организованная и выстроенная система внутреннего аудита ИИ-моделей. **Цель** настоящего исследования состоит в раскрытии ключевых преобразований, с которыми сталкивается внутренний аудит в условиях развития и внедрения ИИ-технологий в операционную деятельность компаний. Основными **методами** работы стали обобщение, сравнение, оценка, библиометрический, сетевой, кластерный и контент-анализ. Комплексное использование названных инструментов позволило выявить основные тренды, проблемные области и лучшие практики в сфере аудита ИИ. **Результатом исследования** явилась разработка ключевых этапов внутреннего аудита моделей ИИ (интегрированных в бизнес-процессы компании) с учетом специфики использования последних, задач по обеспечению регуляторных и корпоративных требований к их внедрению и возникающих при этом рисков. Предложенный алгоритм охватывает полный жизненный цикл ИИ-моделей — от проверки качества входящих данных и корректности работы на этапе внедрения до мониторинга результатов применения (а именно — их конфиденциальности, точности и надежности), а также соответствия нормативным, этическим требованиям в ходе эксплуатации. Результаты исследования являются полезными для специалистов подразделений внутреннего аудита экономических субъектов, разрабатывающих корпоративные стандарты и регламенты аудита внутренних бизнес-процессов. **Ключевые слова:** внутренний аудит; искусственный интеллект; информационная безопасность; корпоративные риски; ИТ-аудит

Для цитирования: Семиколенова М.Н., Санникова И.Н. Трансформация внутреннего аудита в эпоху искусственного интеллекта. *Учет. Анализ. Аудит = Accounting. Analysis. Auditing.* 2026;13(2):69-79. DOI: 10.26794/2408-9303-2026-13-2-69-79

ORIGINAL PAPER

Transformation of Internal Audit in the Era of Artificial Intelligence

M.N. Semikolenova^a, I.N. Sannikova^b

^a National Research University "MPEI", Moscow, Russian Federation;

^b Altai State University, Barnaul, Russian Federation

ABSTRACT

The current development of artificial intelligence technologies presents organisations with a dilemma: on the one hand, improving the efficiency and effectiveness of business processes through the introduction of new tools, and on the other hand, significantly transformation of strategic risks as a result of their application. A well-organised and structured internal audit system for AI models can balance these opportunities and risks. **The objective** of this study is to identify the key transformations facing internal audit in the framework of AI technologies development and implementation in companies' operations. **The key methods** of research include system analysis, generalisation, comparison, evaluation, bibliometric analysis, network, cluster, and content analysis. The integrated use of these methods allowed us to identify key trends, problem areas, and best practices in AI auditing. **The findings resulted** in the development of key stages for the internal audit of AI models integrated into companies' business processes, taking into account the specifics of implementation of the latter, the challenges of ensuring regulatory and corporate requirements for their usage of these models. The proposed internal audit algorithm covers the entire lifecycle of AI models: from checking the quality of incoming data and algorithm validity during implementation to monitoring application results and ensuring compliance

© Семиколенова М.Н., Санникова И.Н., 2026

with regulatory and ethical requirements during operation. This ensures the required level of information security, confidentiality, accuracy, and reliability of the obtained results. The research results are useful for specialists in internal audit departments of economic entities engaged in developing corporate standards and regulations for auditing internal business processes.

Keywords: internal audit; artificial intelligence; information security; corporate risks; IT audit

For citation: Semikolenova M.N., Sannikova I.N. Transformation of internal audit in the era of artificial intelligence. *Uchet. Analiz. Audit = Accounting. Analysis. Auditing*. 2026;13(2):69-79. DOI: 10.26794/2408-9303-2026-13-2-69-79

ВВЕДЕНИЕ

В последние годы ключевым мировым трендом является прогрессивное развитие технологий искусственного интеллекта (ИИ) во многих сферах деятельности, в том числе в области организационно-управленческих задач менеджмента, анализа больших данных, прогнозирования, контроля мошеннических операций и т.д. Ведущие цифровые экономики борются за мировое лидерство в индустрии ИИ. В США в 2019 г. был опубликован национальный стратегический план исследований и разработок, который фокусируется на важнейших вопросах, связанных с использованием ИИ, и направлен на поддержание лидирующих позиций США за счет национальных инвестиций¹. В Европейском союзе (ЕС) в 2018 г. был создан аналогичный концептуальный документ — «Искусственный интеллект для Европы»², направленный на выработку скоординированного подхода к принципам применения ИИ во всех отраслях экономики и обеспечение высоких конкурентных позиций в его разработке и использовании. Китай, в свою очередь, приоритетное внимание уделяет генеративному ИИ в качестве одной из основных проблемных областей цифровой экономики [1].

Россия также не осталась безучастной к формированию глобального рынка ИИ и разработала Национальную стратегию развития искусственного интеллекта до 2030 г.³, ставя в качестве первоочередных задач создание и внедрение ИИ-технологий в наиболее значимых отраслях. Согласно глобальному индексу искусственного интеллекта (The Global AI Index), наша страна занимает 31 место в мире по уровню инноваций, инвестиций и развития ИИ⁴.

Оценка экспертов свидетельствует о том, что объем отечественного рынка искусственного интеллекта в 2023 г. составил 650 млрд руб., и Россия переходит к фазе активной реализации проектов с его участием в бизнес-процессах предприятий.

Внедрение моделей машинного обучения, технологий блокчейна и ИИ, с одной стороны, приводит к революционным преобразованиям в операционной деятельности компаний, создавая новые возможности и способствуя повышению эффективности, а с другой — порождает целый комплекс политических, этических, технических и социальных рисков. В связи с этим внутренний аудит (ВА) становится критически важным элементом корпоративного управления современной организации.

Технологии ИИ не только являются новым вызовом для системы внутреннего аудита компании, но и предоставляют широкие возможности для решения его задач, повышения эффективности и оперативности осуществляемых аудиторских процедур.

МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ

В рамках настоящего исследования предлагается системный и комплексный подход к изучению влияния ИИ на методику внутреннего аудита, состоящий из нескольких этапов. На первом с помощью библиометрического, контентного, сетевого анализа международных и российских наукометрических баз исследований рассматривались современные проблемы, связанные с применением ИИ в разных отраслях экономики; выявлялись предпосылки трансформации системы ВА в условиях развития и внедрения ИИ. Полученные результаты позволили выделить основные кластеры научных изысканий в области аудита информационных систем и ИИ-моделей.

Второй этап работы был посвящен изучению современного развития внутреннего аудита ИИ в России и в мире. На основе результатов исследований, проведенных Институтом внутренних аудиторов (ИВА)⁵, путем обобщения, группировки, графического метода выделены основные риски, связанные с применением

¹ The national artificial intelligence research and development strategic plan: 2019. URL: <https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf>

² Communication from the commission to the european parliament, the european council, the council, the european economic and social committee and the committee of the regions Artificial Intelligence for Europe. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>

³ URL: <http://www.kremlin.ru/acts/bank/44731/page/1>

⁴ URL: <http://www.tortoisemedia.com/data/global-ai>

⁵ URL: <https://www.investopedia.com/terms/i/institute-of-internal-auditors.asp>

ем ИИ (в том числе для реализации функций системы ВА), и определены ключевые области трансформации этой системы в рамках внедрения ИИ-моделей в бизнес-процессы компаний.

Задача третьего этапа состояла в разработке адаптированной программы внутреннего аудита моделей ИИ, интегрированных в хозяйственную деятельность предприятия, что было реализовано посредством использования общенаучных методов индукции и дедукции, синтеза и анализа, сравнения и оценки.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Библиометрический анализ научных исследований в области аудита ИИ-моделей

Источником библиометрического анализа стали базы данных Openalex⁶, Scopus⁷, РИНЦ⁸. Результаты анализа публикационной активности по проблеме аудита внедренных компаниями инструментов ИИ свидетельствуют о ее постоянном приросте (начиная с 2010 г.), что, безусловно, связано с развитием и совершенствованием данных технологий для реализации различных управленческих функций организаций (рис. 1).

Наиболее значимыми темами публикаций в открытой базе научной литературы Openalex являются этика и социальные последствия использования ИИ,

безопасность технологий блокчейна, искусственный интеллект в здравоохранении и образовании, космической науке, анализе больших данных и бизнес-аналитике. При этом одним из самых распространенных ключевых слов, касающихся ИИ, стало понятие «аудит». Таким образом, большинство ученых связывают внедрение инструментов искусственного интеллекта именно с необходимостью их аудита.

Сетевой анализ научных трудов, имеющих отношение к методике внутреннего аудита информационных систем, задействующих ИИ на разных стадиях сбора, группировки и обработки данных, проводился с помощью инструментов Vosviewer⁹. Источником информации для анализа явилась выборка из 1091 научных и обзорных статей, опубликованных в период с 2010 по 2025 г. и размещенных в Openalex. Контент-анализ показал использование авторами выбранных публикаций 55 086 ключевых слов, которые были разделены на соответствующие кластеры с целью установления взаимосвязи между ними. Применение метода «fullcounting» позволило сформировать библиометрическую карту публикаций с отображением ключевых терминов в предметной области «Аудит информационных систем и ИИ», употребляемых исследователями не менее 50 раз (рис. 2). Исходя из представленных данных, можно выделить три кластера: «Ограничительные рамки», «Оценка» и «Управление бизнесом».

⁶ URL: <https://openalex.org>

⁷ URL: <https://www.sciencedirect.com>

⁸ URL: <https://elibrary.ru>

⁹ URL: <https://www.vosviewer.com/>

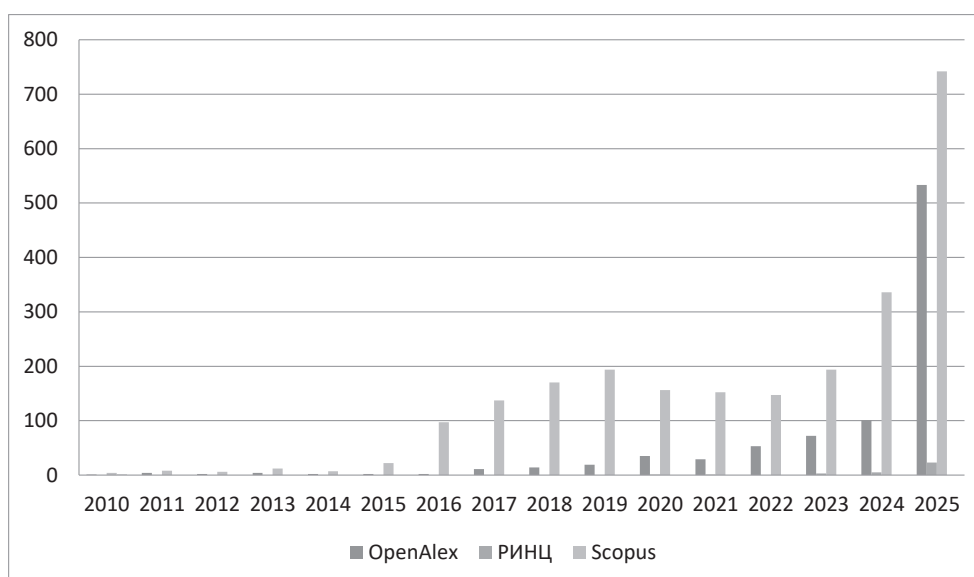


Рис. 1 / Fig. 1. Количество публикаций предметной области «Аудит информационных систем и ИИ» / Number of Publications in the Subject Area "Audit of Information Systems and AI"

Источник/ Source: составлено авторами / compiled by the authors

Особенностью первого является формирование нормативных правил применения технологий ИИ в информационных системах компаний. Данное направление исследований подразумевает необходимость как законодательного регулирования вопросов использования ИИ, так и изучения архитектуры внедряемых технологий, набора ее компонентов с целью получения достоверных, согласованных, подтвержденных результатов [2–4].

Второй кластер — «Оценка» — включает темы исследований, направленных на разработку оценочных инструментов, обеспечивающих эффективность применения ИИ менеджментом организации. Совокупность определенных критериев оценки регламентирует требования как к формированию набора необходимых управленческих данных, так и к алгоритмам их обработки, классификации и анализа, включая общие этические нормы применения и корпоративные принципы управления [5–8].

В рамках третьего кластера раскрываются возможности, перспективы и ограничения современных информационных технологий [9–14].

Следует отметить, что тематика названных кластеров тесно связана с понятием аудита, что подтверждает важность ВА и контроля технологий

ИИ, задействованных в управленческих и информационных системах предприятий.

Нужно отметить, что исследовательский интерес к методологии и практике применения ИИ в академических кругах постоянно возрастает, и пик публикационной активности приходится на последние три анализируемых года. В этот период меняется фокус научных трудов: от изучения эффекта от внедрения прогрессивных технологий в системе менеджмента организации в 2023 г. к определению нормативно-правовых рамок их применения в 2024 г. и разработке архитектуры, регламентов, контрольных процедур, исключению аномалий и ошибок в 2025 г. (рис. 3).

Таким образом, мировая наука и практика демонстрируют динамичное развитие технологий анализа данных, искусственного интеллекта и их внедрение в операционную деятельность компаний разных видов деятельности, что делает особо актуальным создание адаптированной методики внутреннего аудита.

Исследование текущего состояния и направлений развития внутреннего аудита: влияние ИИ-технологий

Инновации, внедрение которых обусловлено объективными причинами, в последнее время оказывают заметное влияние на систему внутреннего

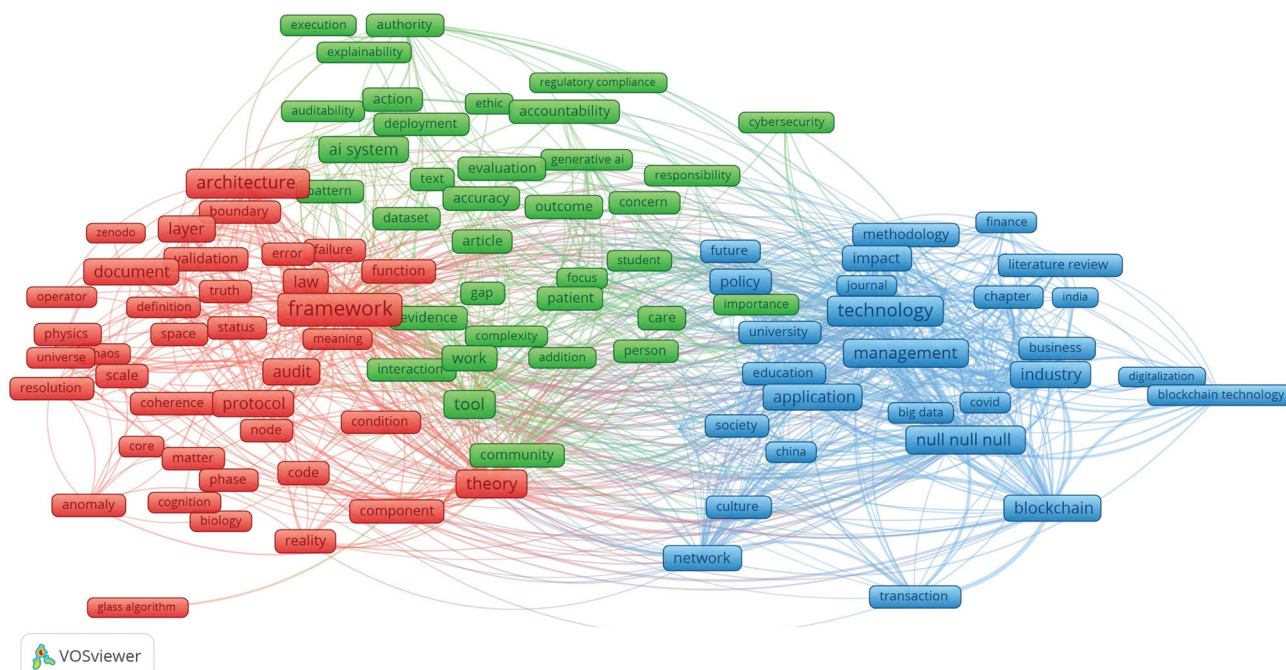


Рис. 2 / Fig.2. Библиометрическая карта публикаций в предметной области «Аудит информационных систем и ИИ» за период 2010–2025 гг. / Bibliometric Map of Publications in the Subject Area “Audit of Information Systems and AI» for the Period 2010–2025

Источники / Source: составлено авторами с помощью Openalex; инструментарий: VOSviewer; метод: Keyword / compiled by the authors based on Openalex: tools: VOSviewer: method: Keyword.

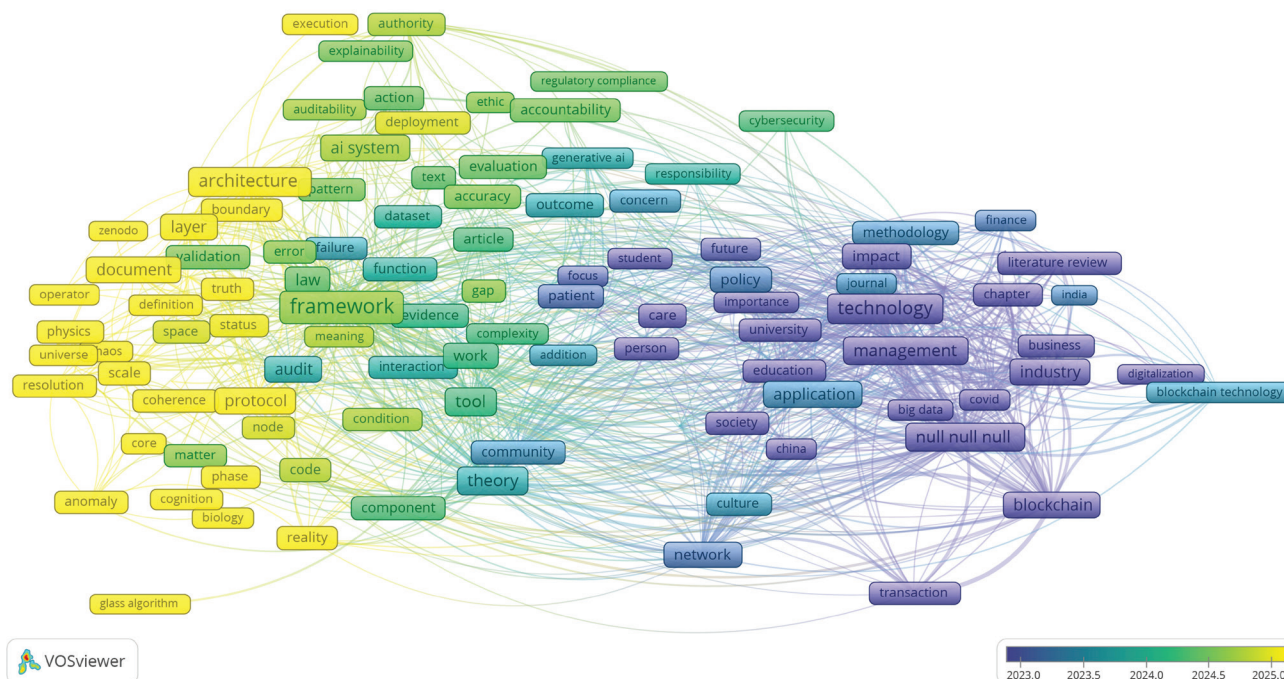


Рис. 3 / Fig. 3. Библиометрическая карта публикаций в предметной области «Аудит информационных систем и ИИ» с группировкой по периодам публикации / Bibliometric Map of Publications in the Subject Area “Audit of Information Systems and AI” Grouped by Publication Periods

Источник/ Source: составлено авторами / compiled by the authors.

аудита. Наиболее существенные преобразования коснулись, на наш взгляд, четырех основных элементов (рис. 4). Прежде всего, это технологии аудита, дополненные возможностями анализа данных с помощью ИИ в части их сбора и обработки, выявления аномалий и трендов при оценке рисков и анализе финансовых потоков. Кроме того, реализация моделей искусственного интеллекта в целях

достижения общекорпоративных целей меняет ключевые направления ВА в сторону аудита как внедрения новых информационных систем и программного обеспечения, так и информационной безопасности, и требует повышения технологических навыков специалистов.

На сегодняшний день уровень автоматизации процессов управления рисками и внутреннего

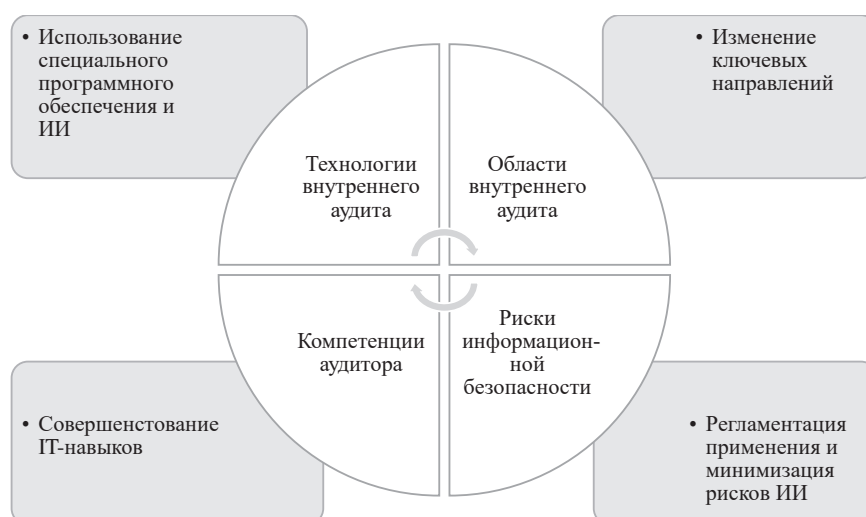


Рис. 4 / Fig. 4. Трансформация внутреннего аудита под влиянием ИИ-технологий / Transformation of Internal Audit under the Influence of AI Technologies

Источник / Source: составлено авторами / compiled by the authors.

контроля предприятий нельзя назвать высоким. По результатам исследования, проведенного в августе 2025 г. аудиторской компанией Kept (в партнерстве с ПАО «Интер РАО») ¹⁰, только 66% опрошенных компаний имеют в наличии ИТ-системы, позволяющие собирать, хранить, обрабатывать информацию и поддерживать процессы по управлению рисками и внутреннему контролю. У 22% функционал ИТ-системы распространяется только на документирование контрольных процедур. Наиболее автоматизированной является система внутреннего контроля (СВК) участвующих в опросе организаций, хотя ее технический уровень не удовлетворяет современным требованиям: только у 37% компаний СВК интегрирована с системой управления рисками, и они образуют единую информационную базу.

В качестве наиболее распространенных технологических решений в системе внутреннего аудита по итогам изучения текущего состояния и тенденций ее развития в России в 2025 г. ¹¹ называют инструменты: анализа данных (кроме Excel) (70%), визуализации данных (48%), ИИ (34%) и GRC ¹² (30%). По оценке руководителей служб ВА, в ближайшие два года приоритетными для внедрения станут технологии ИИ (47%), RPA (программные роботы для выполнения аудиторских процедур) (47%), процессная аналитика (Processmining) (43%) и GRC (41%). Основными целями использования ИИ для целей ВА в настоящее время выступают: анализ информации (34%), формирование рабочей программы аудита (29%), написание кодов для выгрузки, обработки и сопоставления данных в целях эффективного проведения аудиторских процедур (25%).

Думается, что в будущем профессию внутреннего аудитора ждут серьезные (и даже революционные) преобразования, вызванные ускоряющимися техни-

ческими достижениями, продолжающимися глобальными кризисами и возникающими корпоративными рисками. Основываясь на выводах исследования «Внутренний аудит: видение 2035» ¹³, проведенного Институтом внутренних аудиторов, можно предположить, что трансформация коснется таких сфер ВА, как методы и технологии аудиторской проверки, подготовка кадров, повышение авторитета профессии. Участники исследования (6506 респондентов из 155 стран мира и 7 различных регионов) наиболее значимым фактором, способным оказать существенное влияние на систему внутреннего аудита, назвали использование новых технологий, поскольку:

- они позволят аудиторам управлять растущими объемами сложных и неоднородных данных;
- для их применения внутренним аудиторам будет необходимо непрерывно повышать свои технологические навыки;
- применение новых технологий даст возможность достичь более глубокого понимания внутренних и внешних процессов бизнес-среды;
- инновации позволят противостоять дезинформации и манипуляции данными — главным глобальным рискам для ВА;
- благодаря новым технологиям начальные этапы внутреннего аудита могут быть автоматизированы.

Тем не менее большинство компаний только начинают изучать возможности ИИ и пока не применяют его доступный функционал в рамках внутреннего аудита. По оценкам участников исследования, ИИ в настоящее время внедрен на продвинутом уровне только в 7% функций ВА ¹⁴.

Существенные преобразования коснутся не только технологий, но и ключевых областей внутреннего аудита (рис. 5). Ракурс смещается в сторону ИТ, стратегического управления, взаимоотношений со стейкхолдерами, снижения затрат, кибербезопасности и ESG-устойчивости.

Безусловно, внедрение ИИ повлечет за собой проблемы для служб ВА как за счет расширения областей уже известных корпоративных рисков, так и появления дополнительных — внутренних и внешних, связанных с использованием ИИ третьими лицами.

По данным института внутренних аудиторов РФ, руководители служб ВА российских компа-

¹⁰ Исследование текущего состояния и тенденций развития внутреннего аудита в России. URL: https://kept.ru/news/tekushchee-sostoyanie-i-tendentsii-razvitiya-vnutrennego-audita-v-rossii/?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru

¹¹ Уровень автоматизации процессов управления рисками и внутреннего контроля. URL: <https://kept.ru/news/uroven-avtomatizatsii-protseessov-upravleniya-riskami-i-vnutrennego-kontrolya/>

¹² GRC (Governance, Risk and Compliance) — это класс программных продуктов, включающий инструменты анализа деятельности предприятия и внутренних бизнес-процессов.

¹³ Внутренний аудит: видение 2035. URL: <https://ia-vision2035.org/>

¹⁴ Внутренний аудит: видение 2035. URL: <https://ia-vision2035.org/>

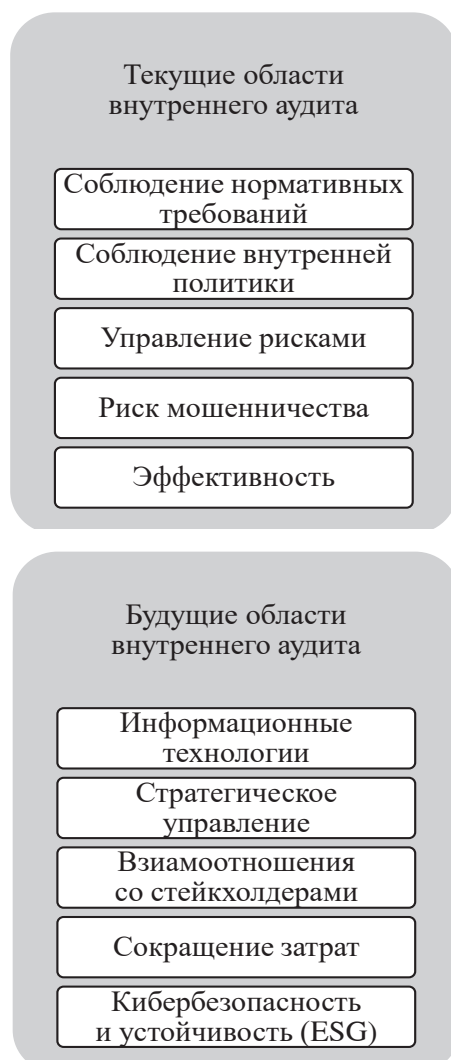


Рис. 5 / Fig. 5. Текущие и будущие ключевые области внутреннего аудита по данным «Vision 2035»/ Current and Future Key Areas of Internal Audit According to “Vision 2035”

Источник/ Source: составлено авторами / compiled by the authors.

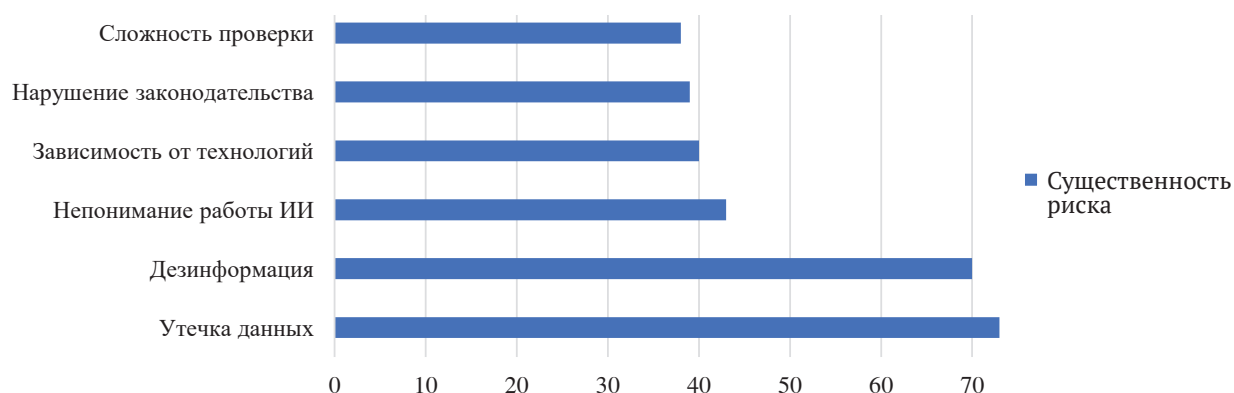


Рис. 6 / Fig. 6. Наиболее значимые риски использования генеративного ИИ по оценке внутренних аудиторов РФ / The Most Significant Risks of Using Generative AI, According to Russian Internal Auditors

Источник/ Source: составлено авторами / compiled by the authors.

ний¹⁵ в 2025 г. назвали наиболее значимыми рисками применения общедоступного ИИ нарушение конфиденциальности данных; галлюцинирование и создание дезинформации; некорректное использование ИИ; избыточную зависимость от технологий и отсутствие критического анализа (рис. 6). Самыми перспективными направлениями минимизации рисков признаны: повышение ИТ-компетенций сотрудников; разработка стандартов и регламентов использования ИИ; верификация данных; контроль и внутренний аудит.

Следовательно, перед компаниями, осуществляющими внедрение инструментов ИИ в операционную деятельность, стоит ключевая цель — создание системы ВА, обеспечивающей эффективное применение доступного функционала инструментов ИИ и минимизирующей риски его использования. Основными задачами такой системы, с нашей точки зрения, являются непрерывный мониторинг рисков, контроль входных данных и архитектуры ИИ, анализ моделей ИИ, контроль их внедрения и отслеживание дальнейшего использования.

Трансформация методики внутреннего аудита бизнес-процессов компании при внедрении ИИ-моделей

Одним из наиболее востребованных для организации ВА в части оценки системы внутреннего контроля предприятия является руководство «Применение структуры и принципов COSO для внедрения

¹⁵ Результаты опроса Ассоциации «Институт внутренних аудиторов»: риски использования общедоступного ИИ. URL: https://www.iiar-ru.ru/upload/inner-auditor/articles/2025_04_07%20ИИ_опрос%20ИТОГ.pdf



Рис. 7 / Fig. 7. Структура системы внутреннего контроля COSO при внедрении и масштабировании ИИ /
Structure of the COSO Internal Control System During the Implementation and Scaling of AI

Источник/ Source: составлено авторами / compiled by the authors.

Таблица 1 / Table 1

**Элементы программы внутреннего аудита моделей ИИ, внедренных в бизнес-процессы компании /
Elements of an Internal Audit Program for AI Models Implemented in a Company's Business Processes**

Объект аудита / Audit Object	Задача внутреннего аудита / Internal Audit Task
Модель управления рисками	Обзор организационной структуры и модели управления; создание механизмов контроля для выявления моделей ИИ, которые прямо или косвенно могут оказывать влияние на финансовую и нефинансовую информацию
Архитектура данных и ИТ-системы	Разработка политики резервного копирования; проверка соответствия политике кибербезопасности; разработка стандартов защиты данных
Качество данных	Определение и документирование процесса считывания входных данных; тестирование их качества; контроль источников и хранилища данных
Оценка эффективности ИИ	Мониторинг производительности используемых систем ИИ в соответствии с бизнес-целями; разработка документированной процедуры интерпретации результатов; организация процесса обратного тестирования
Фактор «черного ящика»	Анализ чувствительности модели к колебаниям входных данных; обеспечение достаточности данных; мониторинг обучающих данных; оценка наличия возможных предубеждений ИИ
Человеческий фактор и алгоритмическая предвзятость	Предотвращение незаконного или преступного использования результатов работы систем ИИ или их использования в нарушение внешнего регулирования или внутренней бизнес-политики

Источник/ Source: составлено авторами / compiled by the authors.

и масштабирования искусственного интеллекта»¹⁶. Предлагаемая модель включает контрольные процедуры по пяти ключевым компонентам: контрольная среда, оценка рисков, контрольные мероприятия, обучение и коммуникация, надзор и оценка (рис. 7).

Большой практический интерес представляет разработанная институтом внутренних аудиторов Испании программа внутреннего аудита моделей

ИИ¹⁷, внедренная в бизнес-процессы компаний, служащая руководством по оценке структур внутреннего контроля и созданная для обеспечения управления рисками, которым подвергаются внедряемые и используемые системы искусственного интеллекта. Разработчики выделяют шесть ключевых областей внутреннего контроля и связанные с ними аудиторские процедуры: модель управле-

¹⁶ Applying the COSO framework and principles to help implement and scale artificial intelligence. URL: https://www.coso.org/files/ugd/3059fc_e17fdcd298924d4ca4df1a4b453b4135.pdf

¹⁷ Internal Audit of Artificial Intelligence Applied to Business Processes. URL: <https://www.theiia.org/en/content/articles/affiliate-content/internal-audit-of-artificial-intelligence-applied-to-business-processes/>

Таблица 2 / Table 2

**Предлагаемые этапы внутреннего аудита моделей ИИ, интегрированных в бизнес-процессы компании /
Proposed Stages of Internal Audit of AI Models Integrated into Companies' Business Processes**

Задачи службы внутреннего аудита / Tasks of the internal audit service	Методы аудита / Audit methods	Рабочие документы аудитора / Auditor's working papers
Этап 1: Планирование внутреннего аудита		
Инвентаризация внедренных инструментов ИИ; предварительная оценка рисков для каждого инструмента; определение размера аудиторской выборки; формирование аудиторской группы	Опросы и анкетирование владельцев бизнес-процессов и ИТ-департамента; анализ документации (технические задания, отчеты о внедрении, политики)	Акт инвентаризации ИИ-инструментов; матрица (карта) предварительной оценки ИИ-рисков; программа и план внутреннего аудита
Этап 2: Сбор аудиторских доказательств		
Проверка полноты, достоверности и релевантности входящих данных; оценка информационной безопасности; контроль за соблюдением конфиденциальности; оценка корректности алгоритма и объяснимости результатов моделей ИИ; мониторинг параметров внедренных моделей ИИ; проверка наличия и соблюдения внутренних корпоративных политик в области ИИ и этики	Интервью с разработчиками, владельцами продуктов, юристами, специалистами по информационной безопасности; выборочная проверка документации: технических паспортов моделей ИИ, протоколов тестирования; наблюдение за процессом внедрения; тестирование средств контроля; инспектирование; анализ отчетов мониторинга; бенчмаркинг с лучшими практиками	Протоколы интервью; результаты тестирования; рабочие матрицы аудиторского риска; отчет об объеме выборки; аналитические отчеты
Этап 3: Анализ, отчетность и представление результатов		
Обобщение и ранжирование выявленных недостатков и отклонений; оценка потенциального воздействия и вероятности рисков; формулирование практических рекомендаций по устранению недостатков; подготовка итогового отчета; презентация результатов аудита	Структурирование ошибок по категориям рисков; оценка существенности отклонений; согласование фактов с руководством проверяемых подразделений	Итоговый отчет; презентация; матрица выявленных отклонений и рекомендаций
Этап 4: Мониторинг выполнения корректирующих действий		
Получение от менеджмента плана корректирующих действий; регулярный мониторинг его выполнения; проведение выборочной верификации фактического устранения недостатков; информирование руководства о статусе выполнения	Анализ отчетности ответственных менеджеров; запрос доказательств выполнения; выборочная повторная проверка критичных нарушений и ошибок	План корректирующих действий; журнал мониторинга выполнения плана; справка о результатах верификации

Источник / Source: составлено авторами / compiled by the authors.

ния системами искусственного интеллекта; архитектура данных и ИТ-системы; качество данных; оценка эффективности; фактор «черного ящика» в системах безопасности ИИ; человеческий фактор и алгоритмическая предвзятость (табл. 1).

Таким образом, основная цель ВА моделей ИИ состоит в независимой и объективной оценке рисков, контроля, эффективности и соответствия нормативным требованиям внедренных в компании инструментов ИИ на всех стадиях жизненного цикла данных ресурсов. С нашей точки зрения, подход к внутреннему аудиту используемых моделей ИИ предполагает реализацию нескольких последовательных и взаимосвязанных этапов, на каждом из которых задействуются соответствующие методы аудиторской проверки и порядок формирования отчетных документов (табл. 2).

ВЫВОДЫ

Внутренний аудит является деятельностью, требующей постоянного совершенствования применяемых методов и подходов для обеспечения эффективного управления рисками и повышения результативности функционирования организации. Очевидно, что

в обозримой перспективе стремительное внедрение в бизнес-процессы предприятий прогрессивных информационных и автоматизированных технологий на основе ИИ расширит область ВА и поставит новые задачи по обеспечению надежности данных и информационной безопасности. При разработке методик внутреннего аудита в отношении ИИ-технологий, интегрированных в операционную деятельность, компании берут за основу результаты научных исследований и практические рекомендации профессиональных сообществ.

Такие модели, с нашей точки зрения, должны предполагать риск-ориентированный подход к ВА, направленный на мониторинг, контроль и управление возникающими рисками на всех стадиях внедрения ИИ: сбор и управление данными, разработка алгоритма ИИ, внедрение и эксплуатация технологий, контроль соответствия. Таким образом, в ближайшей перспективе можно предположить увеличение исследовательского интереса к области применения проактивного внутреннего аудита, анализу соответствия применяемых методов и технологий успешности развития компаний, деловой активности и предпринимательской уверенности.

REFERENCES / СПИСОК ИСТОЧНИКОВ

1. Ye. X., Yan Yu., Li J., Jiang B. Privacy and personal data risk governance for generative artificial intelligence: A Chinese perspective. *Telecommunications Policy*. 2024;48:102851. URL: <https://www.sciencedirect.com/science/article/pii/S0308596124001484> DOI: 10.1016/j.telpol.2024.102851
2. Toth Z., Blut M. Ethical compass: The need for Corporate Digital Responsibility in the use of artificial intelligence in financial services. *Organizational Dynamics*. 2024;53:101041. URL: <https://www.sciencedirect.com/science/article/pii/S0090261624000147> DOI: 10.1016/j.orgdyn.2024.101041
3. Zhang C., Zhu W., Dai J., Wu Y., Chen Xg. Ethical impact of artificial intelligence in managerial accounting. *International Journal of Accounting Information Systems*. 2023;49:100619. URL: <https://www.sciencedirect.com/science/article/pii/S1467089523000118> DOI: /10.1016/j.accinf.2023.100619
4. Kazim E., Denny D., Koshiyama A. AI auditing and impact assessment: According to the UK information commissioner's office. *AI and Ethics*. 2021;1:301-310. DOI:10.1007/s43681-021-00039-2
5. Tan J., Chang S., Zheng Y., Chan K. Effects of artificial intelligence in the modern business: Client artificial intelligence application and audit quality. *International Review of Financial Analysis*. 2025;104:104271. URL: <https://www.sciencedirect.com/science/article/pii/S1057521925003588> DOI: 10.1016/j.irfa.2025.104271
6. Yang J., Amrollahi A., Marrone M. Harnessing the potential of artificial intelligence: Affordances, constraints, and strategic implications for professional services. *Journal of Strategic Information Systems*. 2024;33:101864. URL: <https://www.sciencedirect.com/science/article/pii/S0963868724000465> DOI: 10.1016/j.jsis.2024.101864
7. Metzger M.I., O'Reilly S., Bhaird C. Generative artificial intelligence augmenting SME financial management. *Technovation*. 2025;147:103313. URL: <https://www.sciencedirect.com/science/article/pii/S0166497225001452> DOI: 10.1016/j.technovation.2025.103313
8. Трофимов И.А. Способ выявления рисков нарушения информационной безопасности и уязвимостей процессов обработки, хранения и передачи информации в информационных системах. *Вестник науки и образования*. 2025;10-1(165):23-31.
Trofimov I.A. A method for identifying information security risks and vulnerabilities in information processing, storage, and transmission in information systems. *Vestnik nauki i obrazovaniya = Science and Education Bulletin*. 2025;10-1(165):23-31. (In Russ.).

9. Zou M., Yang Y. Unveiling the impact of artificial intelligence on corporate misconduct, the perspective of information asymmetry. *Technological Forecasting & Social Change*. 2026;225:124506. URL: <https://www.sciencedirect.com/science/article/pii/S0040162525005372> DOI: 10.1016/j.techfore.2025.124506
10. Pisoni G., Moloney M. Responsible AI-based business process management and improvement. *Digital Society*. 2024;323. DOI:10.1007/s44206-024-00105-2
11. Wu T-H., Huang S. Y., Chiu A., Yen D. C. IT governance and IT controls: Analysis from an internal auditing perspective. *International Journal of Accounting Information Systems*. 2024;52:100663. URL: <https://www.sciencedirect.com/science/article/pii/S1467089523000556> DOI: 10.1016/j.accinf.2023.100663
12. Кизилов А.Н., Чернышева Ю.Г. Особенности аудита регенеративного бизнеса и возможности искусственного интеллекта при его проведении. *Фундаментальные исследования*. 2025;7:24-29. DOI: 10.17513/fr.43870
Kizilov A. N., Chernysheva YU.G. Features of regenerative business audit and the potential of artificial intelligence in its implementation. *Fundamental'nye issledovaniya = Fundamental research*. 2025;7:24-29. (In Russ.). DOI: 10.17513/fr.43870
13. Дмитриева С.В. Внедрение регулярного аудита как фактор повышения эффективности деятельности предприятия в условиях цифровой трансформации. *Экономика и управление: проблемы и решения*. 2025;12(5):72-79. DOI: 10.36871/ek.up.p.r.2025.05.12.007
Dmitrieva S. V. Implementing regular audits as a factor in increasing the efficiency of enterprise operations in the context of digital transformation. *Ehkonomika i upravlenie: problemy i resheniya = Economics and Management: Problems and Solutions*. 2025;12(5):72-79. (In Russ.). DOI: 10.36871/ek.up.p.r.2025.05.12.007
14. Chambers R. 5 Key trends in AI-enabled fraud schemes internal auditors must watch in 2025. URL: <https://www.richardchambers.com/5-key-trends-in-ai-enabled-fraud-schemes-internal-auditors-must-watch-in-2025/>

ИНФОРМАЦИЯ ОБ АВТОРАХ / ABOUT THE AUTHORS

Марина Николаевна Семиколонова — кандидат экономических наук, доцент кафедры экономики в энергетике и промышленности, Национальный исследовательский университет «МЭИ», Москва, Российская Федерация

Marina N. Semikolenova — Cand. Sci. (Econ.), Assoc. Prof., Department of Economics in Power Engineering and Industry, National Research University "Moscow Power Engineering Institute", Moscow, Russian Federation <https://orcid.org/0000-0002-0209-0957>

Автор для корреспонденции / Corresponding author:
semikolenovamn@mpei.ru

Инна Николаевна Санникова — доктор экономических наук, профессор, профессор кафедры экономической безопасности, учета, анализа и аудита, Алтайский государственный университет, Барнаул, Российская Федерация

Inna N. Sannikova — Dr. Sci. (Econ.), Prof., Prof. of the Department of Economic Security, Accounting, Analysis and Audit, Altai State University, Barnaul, Russian Federation
<https://orcid.org/0000-0001-5457-6812>
sannikova00@mail.ru

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.
Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

Статья поступила 18.02.2026; после рецензирования 28.02.2026; принята к публикации 02.04.2026.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article was received on 18.02.2026; revised on 28.02.2026 and accepted for publication on 02.04.2026.
The authors read and approved the final version of the manuscript.