π-Economy. 2026, Том 19, № 1. С. 62–79.
π-Economy. 2026, Vol. 19, No. 1. Pp. 62–79.

Научная статья
УДК 005.334:004.8
DOI: https://doi.org/10.18721/JE.19103
EDN: https://elibrary/TQYIFT

ИДЕНТИФИКАЦИЯ И ПРИКЛАДНАЯ ИНТЕРПРЕТАЦИЯ НОВЫХ ПРИЗНАКОВ КЛАССИФИКАЦИИ КОМПЛАЕНС-РИСКОВ В СРЕДЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

И.В. Петрученя ✉

Сибирский федеральный университет, Красноярск, Российская Федерация

✉ petrucheny@gmail.com

Аннотация. В условиях цифровой трансформации комплаенс-среды не только появляются и развиваются новые актуальные инструменты для комплаенса, но и формируется новая категория «техногенных» рисков, для управления которыми традиционные, статичные методы систематизации и группировки малопригодны. Целью данного исследования являются выявление новых видов комплаенс-рисков в условиях применения искусственного интеллекта (ИИ) и разработка усовершенствованной классификации, а также верификация прикладной значимости результатов исследования посредством оценки их влияния на минимизацию потенциальных потерь организаций. В основу работы положен теоретико-методологический подход, включающий комплекс теоретико-аналитических методов, таких как сравнительно-правовой анализ, контент-анализ нормативных документов и научных публикаций, формально-логическое моделирование, позволившее структурировать проведенные исследования. Сравнительный анализ существующих научных разработок по данной проблеме в отечественной и зарубежной литературе выявил ограниченную их применимость к рискам, порождаемым применением ИИ и больших данных. Научная новизна исследования заключается в разработке теоретико-методологического подхода к совершенствованию классификации комплаенс-рисков, основанного на выявлении и систематизации новых специфических видов угроз, порождаемых фундаментальными свойствами систем ИИ (автономностью, изменчивостью, масштабируемостью), включая латентную дискриминацию и программные искажения фактических данных; а также на онтологическом обосновании признаков классификации специфических видов комплаенс-рисков, что позволило расширить предметное поле цифрового комплаенса и обеспечить повышение коэффициента охвата идентифицируемых рисков с 42% (в базовых моделях) до 90% (в авторской модели). Для подтверждения прикладной состоятельности теоретико-методологических положений предложенной классификации автором сформирован инструментально-расчетный блок исследования, направленный на верификацию прогнозной эффективности предлагаемых мер. Данный аспект новизны заключается в разработке методики количественной оценки эффективности предлагаемых решений, включающей обоснование коэффициента сравнительной эффективности, позволяющего математически верифицировать превосходство авторского подхода над традиционными статичными моделями; выведение модифицированной формулы, обеспечивающей конвертацию качественных признаков рисков в измеримые количественные показатели экономической выгоды организации. Предложенная в данной статье классификация комплаенс-рисков может служить теоретическим фундаментом для создания предиктивных моделей комплаенс-мониторинга, проактивной адаптации нормативно-правового поля, разработки предиктивных, превентивных систем контроля, цифровых профилей комплаенс-рисков и автоматизации оценки ответственности субъектов.

Ключевые слова: классификация рисков, комплаенс-риски, цифровой комплаенс, набор критериев, риски, искусственный интеллект, большие данные, регуляторная среда, компании

Для цитирования: Петрученя И.В. (2026) Идентификация и прикладная интерпретация новых признаков классификации комплаенс-рисков в среде искусственного интеллекта. π-Economy, 19 (1), 62–79. DOI: https://doi.org/10.18721/JE.19103

Research article
DOI: https://doi.org/10.18721/JE.19103

IDENTIFICATION AND PRACTICAL INTERPRETATION OF NEW FEATURES FOR CLASSIFYING COMPLIANCE RISKS IN AN ARTIFICIAL INTELLIGENCE ENVIRONMENT

I.V. Petrucheny ✉

Siberian Federal University, Krasnoyarsk, Russian Federation

✉ petrucheny@gmail.com

Abstract. In the context of the digital transformation of the compliance environment, not only are new relevant compliance tools emerging and developing, but a new category of "technogenic" risks is also being formed, for which traditional, static methods of systematization and grouping are of little use. The goal of this study is to identify new types of compliance risks from the use of artificial intelligence (AI) and to develop an improved classification, as well as to verify the practical significance of the research results by assessing their impact on minimizing potential losses for organizations. The work is based on a theoretical and methodological approach, incorporating a range of theoretical and analytical methods, such as systems and comparative legal analysis, content analysis of regulatory documents and scientific publications and formal logic modeling, which allowed for the structuring of the research. A comparative analysis of existing scientific studies on this topic in domestic and foreign literature revealed their limited applicability to the risks posed by AI and Big Data. The scientific novelty of the research lies in the development of a theoretical and methodological approach to improving the classification of compliance risks, based on the identification and systematization of new specific types of threats generated by the fundamental properties of AI systems (autonomy, variability, scalability), including latent discrimination and algorithmic distortion of factual data; as well as on the ontological substantiation of the classification criteria for specific types of compliance risks, which has expanded the scope of digital compliance and increased the risk coverage ratio from 42% (in basic models) to 90% (in the author's model). To confirm the practical validity of the theoretical and methodological principles of the proposed classification, the author developed an instrumental and computational block aimed at verifying the predictive effectiveness of the proposed measures. This novelty aspect lies in the development of a methodology for quantitatively assessing the effectiveness of the proposed solutions, including the substantiation of a comparative effectiveness coefficient, allowing for mathematical verification of the superiority of the author's approach over traditional static models; and the derivation of a proprietary formula for determining prevented potential damage, ensuring the conversion of qualitative risk indicators into measurable quantitative indicators of the organization's economic benefit. The classification of compliance risks proposed in this article can serve as a theoretical foundation for the creation of predictive compliance monitoring models, proactive adaptation of the regulatory framework, development of predictive, preventive control systems, digital compliance risk profiles and the automation of entity liability assessment.

Keywords: risk classification, compliance risks, digital compliance, set of criteria, risks, artificial intelligence, big data, regulatory environment, companies

Citation: Petrucheny I.V. (2026) Identification and practical interpretation of new features for classifying compliance risks in an artificial intelligence environment. π-Economy, 19 (1), 62–79. DOI: https://doi.org/10.18721/JE.19103

Введение

Актуальность исследования

Актуальность исследования обусловлена рядом критических факторов, влияющих как на бизнес-среду компаний, так и на правовое поле. Прежде всего, это связано с экспоненциальным ростом применения технологий искусственного интеллекта (ИИ, англ. *Artificial Intelligence*, *AI*) и больших данных (БД, англ. *Big Data*) в корпоративном секторе, что находит подтверждение в актуальных мировых статистических данных. Так, согласно [1], полученные данные свидетельствуют о росте инвестиций в разработку больших языковых моделей, а количество инцидентов, связанных с эксплуатацией систем ИИ, только за 2024 г. увеличилось на 56,4%, достигнув исторического максимума. Данная динамика, в совокупности с вступлением в силу положений Регламента ЕС[1] в августе 2026 г., формирует новую регуляторную реальность, требующую пересмотра традиционных подходов к комплаенс-контролю.

Во-первых, широкое использование продуктов информационных технологий (ИТ, англ. *Information Technology*, *IT*), ИИ и облачных сервисов для оптимизации различных процессов, принятия управленческих решений и анализа рынка приводит к возникновению новых, ранее не существовавших рисков. Действующие классификации (антикоррупционные, противодействующие отмыванию денег, антимонопольные), разработанные для традиционных бизнес-процессов, носят, как правило, ретроспективный, «догоняющий» характер и слабо адаптируются к новым вызовам и угрозам.

Во-вторых, динамичность регуляторной среды объясняется ужесточением и усложнением действующего законодательства (Общий регламент по защите данных, российские законы о персональных данных, этические кодексы в области ИИ). Несоответствие законодательству и нормативным актам влечет за собой серьезные штрафы и санкции. Актуализация систематизации и типологии комплаенс-рисков помогает бизнесу заранее их классифицировать и защищаться от правонарушений.

В-третьих, многие области ИИ недостаточно или нечетко урегулированы действующим законодательством и нормативными актами. Это ситуация правовой неопределенности, когда невозможно однозначно определить, является ли то или иное действие или применение технологии законным, незаконным или допустимым (например, отсутствие четких стандартов ответственности и др.). Пересмотр признаков классификации рисков помогает выявить эти пробелы, а также позволяет разработать внутренние политики в компаниях для минимизации этих рисков.

В-четвертых, нарушения комплаенса в области использования продуктов ИТ, ИИ наносят серьезный репутационный ущерб, что в стратегической перспективе может подорвать операционную устойчивость компании и привести к ее банкротству или поглощению.

В-пятых, усовершенствованная градация рисков – это фундаментальная основа для разработки автоматизированных комплаенс-систем, использующих ИИ для мониторинга и контроля за соблюдением регуляторных требований и норм[2] [2].

Принципиальным аспектом актуальности работы является необходимость верификации прикладной значимости предлагаемых классификационных решений. В условиях жесткого

[1] EUR-Lex: Access to European Union law (2024) *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)*. [online] Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng [Accessed 10.01.2026].

[2] PwC (2025) *Global AI Jobs Barometer*. [online] Available at: https://www.pwc.com/gx/en/news-room/press-releases/2024/pwc-2025-global-digital-trust-insights.html [Accessed 17.11.2025]; RUBEZH (2025) *О Компании «РУБЕЖ»*. [online] Available at: https://rubezh.ru/about [Accessed 15.10.2025]. (in Russian); Deloitte. [online] Available at: https://www2.deloitte.com/kz/ru/pages/risk/articles/2020/3LOD.html [Accessed 04.11.2025]. (in Russian); Полянина А. (2025) *Цифровая экономика: как специалисты понимают этот термин*. [online] Available at: https://ria.ru/20170616/1496663946.html [Accessed 04.10.2025]. (in Russian); ISO (2025) *Новый стандарт ISO 31000 способствует упрощению системы менеджмента рисков*. [online] Available at: https://www.iso.org/ru/news/ref2263.html [Accessed 09.10.2025]. (in Russian); РБ.РУ. [online] Available at: https://rb.ru/longread/digital-twin/ [Accessed 21.10.2025]. (in Russian).

регулирования процессов внедрения систем ИИ разработка инструментов подтверждения экономической эффективности мер контроля становится обязательным условием обеспечения устойчивости организаций.

При отсутствии доказательной базы и инструментов количественной оценки организации не могут объективно обосновать инвестиции в систему цифрового комплаенса. Таким образом, актуальность исследования также определяется необходимостью создания верифицированного методического инструментария, позволяющего подтвердить эффективность предлагаемых мер через предотвращение потенциального ущерба.

Литературный обзор

В России проблема цифрового комплаенса и рисков, связанных с ИИ и большими данными (ИИ/БД), активно исследуется в рамках юридических и экономических наук. Эти исследования часто носят междисциплинарный характер и фокусируются на адаптации российского законодательства и практик к глобальным технологическим вызовам.

В большинстве проанализированных работ исследователи сходятся во мнении, что этап активного внедрения ИИ/БД требует смены фокуса со статичных отраслевых классификаций в пользу динамических, кросс-функциональных и технологически ориентированных моделей. Вместе с тем сравнительный анализ выявил, что при единстве взглядов на природу цифровых угроз сохраняется существенный методологический разрыв в инструментарии их оценки.

Для систематизации существующей теоретической базы по рассматриваемой проблеме автором выделены три ключевых подхода к классификации комплаенс-рисков, разграниченных по признаку доминирующего вектора идентификации угроз: консалтинговый и регуляторный (вектор – внешняя нормативная среда и санкции); академический зарубежный (вектор – техническая онтология и природа ИИ); отечественный правовой (вектор – организационно-процедурное обеспечение).

1. *Консалтинговый и регуляторный подход*

Основной акцент в данном блоке исследований (работы PwC, международные стандарты ISO, рекомендации Базельского комитета)[3] [1, 2] смещен на обеспечение операционной устойчивости и имплементацию внешних регуляторных требований. Классификации в этом подходе ориентированы на защиту бизнес-процессов от финансовых потерь и штрафных санкций. В условиях наступления нормативной полноты Регламента ЕС данный подход является основополагающим для имплементации систем комплаенс-контроля. Однако, несмотря на высокую практическую значимость, классификации PwC зачастую носят декларативный характер и «пропускают» глубокие технические риски, фокусируясь преимущественно на правовых последствиях, а не на технической причине их возникновения.

2. *Академический зарубежный подход*

В работах зарубежных авторов [3, 4] заложена методологическая база онтологического анализа систем ИИ. Исследователи сходятся в том, что период масштабного внедрения ИИ/БД (согласно трендам 2025–2026 гг.) требует отказа от статичных классификаций в пользу динамических моделей. В своих работах авторы исследуют автономность и изменчивость алгоритмов как первоисточники угроз, которые невозможно описать традиционными юридическими терминами. В настоящей статье адаптирована и развита концепция онтологического обоснования дескрипторов рисков, что позволило автору перейти к идентификации новых видов угроз, не охваченных существующими практико-ориентированными классификациями.

3. *Отечественный правовой подход*

Отечественная научная школа, представленная работами М.А. Панариной и ряда других исследователей [5–13], характеризуется глубокой проработкой правовых и организационных аспектов комплаенса. В рамках данного подхода всесторонне регламентируются механизмы

[3] Там же.

распределения юридической ответственности, детально описываются правовые риски субъектов управления, а также вопросы документационного обеспечения и формирования корпоративной комплаенс-культуры. Однако, несмотря на детальную нормативную проработку, в данных классификациях сохраняется дефицит инструментов для работы с технической онтологией ИИ/БД, что затрудняет идентификацию латентных технологических угроз.

Резюмируя результаты критического анализа, следует констатировать наличие выраженного методологического разрыва между теоретическим пониманием технических свойств ИИ (академический подход) и практическими инструментами правовой регламентации ответственности (отечественный и консалтинговый подходы). Выявленный разрыв заключается в отсутствии интегрированных дескрипторов, способных трансформировать онтологические характеристики цифровых систем (автономность, изменчивость) в измеримые параметры комплаенс-контроля. Традиционные классификации ориентированы на идентификацию реализованных инцидентов, в то время как работа с ИИ требует превентивного контроля и предупреждения специфических угроз, таких как недостоверность данных и скрытая «предвзятость алгоритмов».

Таким образом, потребность в преодолении выявленного методологического разрыва диктует необходимость разработки интегрированного классификационного подхода, объединяющего техническую онтологию систем ИИ с инструментарием количественной оценки предотвращенного ущерба.

Цель исследования – выявление новых видов комплаенс-рисков в условиях применения ИИ и разработка усовершенствованной классификации, а также верификация прикладной значимости полученных результатов исследования посредством оценки их влияния на минимизацию потенциальных потерь организаций.

Объектом исследования являются комплаенс-риски организаций, возникающие в условиях внедрения технологий ИИ/БД.

Предмет исследования – новые виды и признаки классификации комплаенс-рисков в условиях применения ИИ, а также инструментарий оценки влияния их идентификации на минимизацию потенциальных потерь организаций.

Для достижения поставленной цели были сформулированы конкретные задачи:

1) провести критический анализ существующих классификаций комплаенс-рисков ИИ (по материалам работ отечественных и зарубежных авторов);

2) идентифицировать и систематизировать новые специфические признаки комплаенс-рисков, обусловленные фундаментальными свойствами цифровых систем;

3) разработать усовершенствованную классификацию комплаенс-рисков, адаптированную к условиям применения технологий ИИ/БД;

4) провести апробацию разработанной классификации на эмпирических данных и обосновать экономическую эффективность ее интеграции в систему комплаенс-контроля для минимизации потенциальных потерь организаций.

Методы и материалы

Для достижения цели исследования автором был применен комплекс теоретико-аналитических методов, включающий такие, как сравнительно-правовой анализ, контент-анализ нормативных документов и научных публикаций, формально-логическое моделирование, позволившее структурировать проведенные исследования.

Критерием отбора методов послужила потребность в системном анализе сущностных характеристик новых рисков, их соотнесении с действующим нормативным полем и построении непротиворечивой таксономии.

Реализация указанных методов в рамках работы осуществлялась следующим образом:

• *Формально-логическое моделирование* применено для построения иерархической структуры усовершенствованной классификации и верификации ее совместимости с актуальными регуляторными требованиями.

• *Методы нормативного моделирования* послужили основой для разработки инструментально-расчетного компонента и верификации классификации на соответствие актуальным регуляторным требованиям.

• *Контент-анализ и сравнительно-правовой метод* использованы для исследования текстовых массивов и отчетов международных организаций (Stanford AI Index 2025, PwC), что позволило идентифицировать латентные тенденции в восприятии рисков со стороны профессионального сообщества.

• *Ретроспективный анализ и метод экспертных оценок* послужили основой для апробации разработанной классификации. Ретроспективный анализ данных об инцидентах ИИ за 2024–2025 гг. позволил получить эмпирические данные для расчета коэффициента охвата рисков (англ. Risk Coverage Ratio, RCR).

Синергия примененных методов позволила автору разработать научно обоснованный и верифицированный инструментарий для управления новым классом правовых и регуляторных вызовов, возникающих в условиях широкого применения систем ИИ.

Результаты и обсуждение

Изучение влияния технологий ИИ/БД на конфигурацию и «наполняемость» комплаенс-рисков позволяет сделать вывод, что эти технологии не просто «добавляют» новые риски, а фундаментально трансформируют всю систему управления комплаенсом (рис. 1).

Современные технологии ИИ/БД кардинально усиливают возможности по управлению традиционными комплаенс-рисками (табл. 1).

Таблица 1. Влияние ИИ/БД на управление комплаенс рисками
Table 1. Impact of AI / Big Data on compliance risk management

Область применения	Влияние ИИ/БД
Противодействие отмыванию денег и финансированию терроризма	*Сдвиг от ретроспективного анализа к проактивному выявлению*. Традиционные системы основаны на статических правилах и дают много ложных срабатываний. ИИ, анализируя огромные объемы данных, выявляет скрытые схемы и аномалии, которые не поддаются формализации установленными правилами.
«Знай своего клиента» / Due Diligence	*Автоматизация и углубление проверок*. ИИ может в режиме, близком к реальному времени, сканировать тысячи источников данных по клиенту или контрагенту, выявляя скрытые связи и потенциальные репутационные риски.
Мошенничество	*Мгновенное обнаружение мошеннических операций*. Модели машинного обучения анализируют поведение пользователя и в реальном времени блокируют подозрительные действия.
Торговый надзор	*Выявление инсайдерской торговли и манипулирования рынком*. ИИ может анализировать торговые данные, новостные потоки и активность в социальных сетях, чтобы обнаруживать возможные манипуляции или использование инсайдерской информации.
Управление операционными рисками	*Предсказание сбоев*. Анализируя данные с датчиков оборудования, метрики эффективности, ИИ может предсказать вероятность технического сбоя или операционной ошибки, позволяя устранить проблему до ее возникновения.
Регуляторная отчетность	*Автоматизация*. Обработка естественного языка (англ. Natural Language Processing, NLP) может использоваться для автоматического анализа новых регуляторных требований, для частичного заполнения отчетных форм, снижая нагрузку на сотрудников и, как следствие, риск человеческой ошибки.

Источник: составлено автором на основе [5, 8, 9, 14–17].

Источник: составлено автором.

Рис. 1. Влияние технологий ИИ/БД на функцию комплаенса

Fig. 1. Impact of AI / Big Data technologies on the compliance function

Парадоксальным образом эти же технологии формируют кардинально новый класс комплаенс-рисков в сфере конфиденциальности, этики, «прозрачности», что требует реновации комплаенс-инструментария и перехода от реактивных практик к технологичным системным решениям, противостоящим масштабируемым угрозам нового поколения[4] [15–19].

В отечественной научной и практической среде, как правило, анализ и изучение новых цифровых явлений, в том числе технологий ИИ/БД, начинаются не одновременно с их появлением на мировом рынке, а после того, как они уже получили распространение или когда на них уже отреагировали зарубежные регуляторы. Это, в конечном счете, выступает первопричиной возникновения обозначенных выше проблем[5] [20–22].

Для достижения поставленной цели исследования автором были сформулированы новые признаки классификации комплаенс-рисков, возникающих в результате применения ИИ/БД. Выделенные классификационные признаки «вытекают» из фундаментальных свойств цифровых систем – их автономности, изменчивости, масштабируемости и способности создавать новые реальности[6] [7, 8]:

1. *Природа субъекта риска и его правового статуса*

Традиционные классификации комплаенс-рисков базируются на субъектно-ориентированном подходе, в рамках которого источником ответственности всегда признается физическое или юридическое лицо. Однако появление автономных ИИ-агентов, способных самостоятельно инициировать рисковые события, создает ситуацию, не предусмотренную действующим законодательством. Введение этого классификационного признака позволяет идентифицировать этот правовой пробел и обосновать необходимость разработки специальных механизмов регулирования для случаев, когда источником риска выступает ИИ, а не человек или организация.

2. *Степень прозрачности и интерпретируемости функционирования систем ИИ*

Включение данного признака в классификацию обосновано тем, что он является фундаментом для обеспечения подотчетности систем ИИ. Данный признак позволяет систематизировать комплаенс-риски по критерию «Возможности понимания и аудита логики работы ИИ», что является серьезной проблемой для современного правового регулирования и комплаенса. С технической точки зрения этот признак позволяет выявлять скрытые ошибки и предвзятость

[4] ПЛМ Урал. [online] Available at: http://www.plmural.ru/resheniya-dlya-cifrovogo-proizvodstva/preimuschestva-sovmestnogo-ispolzovaniyaplm-i-mes-sistem [Accessed 05.11.2025]. (in Russian).

[5] Deloitte (2017) Стресс-тестирование: лучшие практики. [online] Available at: https://www2.deloitte.com/content/dam/Deloitte/kz/Documents/risk/Стресстестирование_лучшие%20практики [Accessed 17.11.2025]. (in Russian); Елисеева Ю. (2022) Как технологии изменили сферу комплаенс [online] Available at: https://trends.rbc.ru/trends/innovation/5db0538a9a79474c280764e2 [Accessed 19.02.2022]. (in Russian).

[6] EUR-Lex: Access to European Union law (2024) *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)*. [online] Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng [Accessed 10.01.2026].

модели, которые невозможно отследить в традиционном коде. С регуляторной и юридической позиций он обеспечивает проверяемость (аудируемость) решений, позволяя организации доказывать их законность и этичность перед надзорными органами. Выделение этого классификационного признака позволит предприятиям соответствовать современным международным и формирующимся национальным регуляторным трендам, требующим от компаний обеспечения определенного уровня прозрачности автоматизированных систем принятия решений.

3. *Характер и качество данных, используемых в системах ИИ*

Современные регуляторы цифрового комплаенса (например, в рамках Регламента ЕС) смещают фокус контроля с традиционного аудита программного кода на оценку качества и репрезентативности данных. Если в классических системах ИТ риски преимущественно детерминированы человеческим фактором или ошибками программирования, то в системах ИИ именно данные становятся основным источником комплаенс-угроз. Применение этого признака в классификации позволяет внедрить инновационный для предприятий вид контроля – аудит чистоты и этичности данных, что обеспечивает минимизацию рисков, недоступную при использовании традиционных методов. Также предложенный признак позволит классификации быть проактивной и фокусироваться на новых, специфических признаках, которые не учитываются в традиционных классификациях.

На основе указанных признаков можно выделить следующие новые виды комплаенс-рисков (табл. 2).

Распределение нескольких видов рисков в рамках одного критерия позволяет провести более глубокий анализ и создать детализированную «систему координат» для управления рисками[7] [11–22].

Для верификации выдвинутой гипотезы об актуализации существующих классификаций комплаенс-рисков в условиях применения технологий ИИ/БД, а также для оценки практической реализуемости предложенных признаков использовался комплексный подход. Методологическую основу составил синтез двух ключевых методов: ретроспективного анализа инцидентов и метода экспертных оценок. На их базе был произведен аналитический расчет эффективности идентификации специфических комплаенс-рисков и полноты охвата угроз в условиях применения систем ИИ.

В качестве эмпирической базы использованы данные отчета [1], зафиксировавшего рекордный рост инцидентов ИИ до 233 случаев (+ 56,4% в 2024 г. к 2025-му).

Автором была сформирована репрезентативная панель из 50 инцидентов 2024–2025 гг., отобранных методом случайной выборки из базы AI Incident Database[8] (табл. 3). Анализ 50 кейсов показал, что стандартные модели комплаенса (фокусирующиеся на защите данных и кибербезопасности) эффективны только в тех случаях, где причина нарушения очевидна и формализована.

В результате анализа установлено, что стандартные (базовые) модели классификации рисков (ориентированные преимущественно на защиту данных и лицензионную чистоту) смогли бы предотвратить или идентифицировать лишь 21 (12 + 9) случай из 50 (что составляет 42%). Оставшиеся 58% инцидентов (29 случаев) были связаны с факторами, которые в базовых моделях классифицируются как форс-мажор или технический сбой, но в рамках предложенной классификации имеют четкие признаки: алгоритмическое смещение, неопределенность правосубъектности агента или латентная дискриминация.

[7] ПЛМ Урал. [online] Available at: http://www.plmural.ru/resheniya-dlya-cifrovogo-proizvodstva/preimuschestva-sovmestnogo-ispolzovaniyaplm-i-mes-sistem [Accessed 05.11.2025]. (in Russian); Deloitte (2017) Стресс-тестирование: лучшие практики. [online] Available at: https://www2.deloitte.com/content/dam/Deloitte/kz/Documents/risk/Стресстестирование_лучшие%20практики [Accessed 17.11.2025]. (in Russian); Елисеева Ю. (2022) Как технологии изменили сферу комплаенс [online] Available at: https://trends.rbc.ru/trends/innovation/5dнb0538a9a79474c280764e2 [Accessed 19.02.2022]. (in Russian).

[8] AI Incident Database (2026) Responsible AI Collaborative. [online] Available at: https://incidentdatabase.ai [Accessed 15.01.2026].

Таблица 2. Новизна и практическая значимость скорректированной классификации комплаенс-рисков
Table 2. Novelty and practical significance of the adjusted classification of compliance risks

Признак классификации	В чем новизна подхода?	Разновидность риска	Обоснование комплаенс риска	Что конкретно это дает организации?
1. Природа субъекта риска и его правового статуса	Появляется возможность систематизации рисков, возникающих из ключевого несоответствия между фактической агентностью систем ИИ (способностью к действиям как субъекта) и их юридическим статусом «не-субъекта» в правовом поле.	Риск неконтролируемого поведения системы	Риск возникновения негативных последствий, вызванных действиями системы ИИ, не предусмотренных ее разработчиками и являющихся следствием ее функциональной автономии и непредсказуемости	• *Внедрение процессов MLOps* – позволяет автоматически отслеживать изменения данных онлайн, сокращать «серую зону» правовой неопределенности, а также создавать конкурентное преимущество, внедряя более безопасные и надежные ИИ-решения; • *Экономия ресурсов* – проактивное переобучение модели дешевле, чем возможные финансовые потери от штрафов и судебных исков; • *Обоснование для регулятора* – организация демонстрирует проактивный и ответственный подход к управлению ИИ.
		Риск отсутствия (неопределенности) правосубъектности ИИ-агента	Риск отсутствия (неопределенности) правосубъектности, т.е. риск возникновения нормативно-правовых пробелов, разногласий, невозможности возложения ответственности в ситуациях причинения вреда системой ИИ, исходя из правового статуса этой системы – «не-субъекта»	
2. Степень прозрачности и интерпретируемости (объяснимости) функционирования систем ИИ	Сдвиг от проверяемой логики к управлению объяснимостью. Появление «новых рисков» подтверждает необходимость модернизации архитектуры комплаенс-системы, включающей в себя не только правовой надзор, но и технологические инструменты для обеспечения прозрачности и интерпретируемости ИИ.	Риск нарушения «права на объяснение»	Риск потерь вследствие неспособности организации выполнить законодательно закрепленное требование субъекта данных или регулятора предоставить содержательное объяснение автоматически принятого в его отношении решения, что ведет к прямым правовым санкциям.	• *Внедрение Explainable AI (XAI)* – позволяет генерировать объяснимые причины для каждого решения ИИ для клиентов и регулятора, выполняя требование «права на объяснение»; • *Снижение репутационных рисков* – возможность доказать, что решение, даже неочевидное для человека, было статистически обоснованным и недискриминационным; • *Эффективный внутренний аудит* – аудиторы получают инструменты для проверки моделей на «смещение», даже не понимая всей их внутренней механики.
		Риск латентной дискриминации	Риск потерь вследствие того, что ИИ использует для принятия решений трудно доказуемые, неочевидные для человека корреляции и прокси-признаки, которые могут привести к нарушению антидискриминационного законодательства.	

Окончание таблицы 2

Признак классификации	В чем новизна подхода?	Разновидность риска	Обоснование комплаенс риска	Что конкретно это дает организации?
3. Характер и качество данных, используемых в системах ИИ	«Источник нарушения» (источник комплаенс-риска) смещается с процесса (алгоритма) на данные. Сформирована новая категория комплаенс-рисков, «возникающих» из-за фундаментальных недостатков информационного ресурса (данных), на котором базируется работа систем ИИ, а не из-за человеческих ошибок или ошибок программирования	Риск алгоритмического нарушения правил, политик комплаенса	Риск несоответствия деятельности организации установленным внутренним или внешним нормативным требованиям, возникающим в результате автономного принятия решений ИИ (по причине ошибок в данных, неполноты инструкций или др.)	• *Приоритизация рисков* – позволяет выделить те ИИ-решения, сбой в которых приведет к наибольшему ущербу, и направить на них ресурсы контроля; • *Создание планов аварийного реагирования* – разработка «красных флагов» и процедур экстренного отключения систем ИИ для минимизации ущерба при обнаружении массового нарушения; • *Проактивная этическая и правовая экспертиза* – организация заранее оценивает, не может ли масштабируемое решение модели привести к негативным социальным последствиям или обвинениям в манипуляции.
		Риск системной предвзятости	Риск возникновения потерь (штрафов) вследствие систематического и масштабируемого негативного отношения алгоритма ИИ к определенным социальным группам, сформированного на базе нерепрезентативных, неполных или данных на этапе обучения или работы системы.	
		Риск формирования цифрового профиля и манипуляции	Риск использования больших данных для создания детализированных психологических или поведенческих профилей с целью последующего манипулирования поведением пользователей в обход их информированного согласия, нарушающего принципы автономии и этики.	

Источник: составлено автором.

Таблица 3. Валидация классификации: эффективность идентификации комплаенс-угроз и анализ слепых зон базовой модели
Table 3. Classification validation: effectiveness of compliance threat identification and analysis of blind spots in the basic model

Категория инцидента	Количество случаев (из 50)	Идентифицируемость базовой моделью	Причина «пропуска» риска базовой моделью
Утечки данных и кибервзломы	12	Да (100%)	Традиционные ИТ-протоколы контроля доступа
Нарушение лицензий / IP	9	Да (100%)	Стандартный юридический аудит контрактов
Алгоритмическое смещение / Дискриминация	14	Нет (0%)	Базовая модель не видит «внутреннюю логику» черного ящика
Фактологические искажения и ошибки генерации	10	Нет (0%)	Риски интерпретируются как технический сбой, а не как комплаенс-нарушение
Неопределенность статуса ИИ-агента	5	Нет (0%)	Отсутствие правовых норм ответственности за автономные действия

Источник: составлено автором.

Для верификации сформулированной в исследовании гипотезы каждый инцидент из панели (50 инцидентов) был подвергнут встречному анализу:

– возможность его идентификации по базовой модели (традиционные признаки: право собственности, защита персональных данных);

– возможность его идентификации по авторской модели (новые признаки: алгоритмическое смещение, правосубъектность агента, латентная дискриминация).

Результаты сопоставления базовой и представляемой моделей классификации представлены в табл. 4.

Таблица 4. Сравнительный анализ охвата инцидентов базовой и авторской классификациями
Table 4. Comparative analysis of incident coverage by the basic and author's classifications

Группа инцидентов (n = 50)	Покрываются базовой классификацией	Покрываются авторской классификацией	Причина разрыва (Gap)
Число выявленных рисков (*Rid*)	21	45	Несоответствие технической онтологии ИИ правовым нормам
Коэффициент охвата рисков (*RCR*)	42%	90%	–

Источник: составлено автором.

Полученные результаты свидетельствуют о том, что применение предлагаемого подхода к классификации комплаенс-рисков позволяет компенсировать методологический дефицит традиционных подходов. Это достигается за счет охвата 58% инцидентов, имеющих специфическую онтологию комплаенс-рисков, присущую исключительно технологиям ИИ/БД.

Для верификации прикладной значимости был рассчитан относительный коэффициент сравнительной эффективности (прироста результативности на базе авторской модели классификации):

$$K_{eff} = RCR_{author} / RCR_{base} = 90/42(\%) \sim 2{,}14. \quad (1)$$

Это означает, что внедрение предложенных признаков классификации в систему внутреннего контроля предприятия позволяет в 2,14 раза повысить вероятность обнаружения специфических цифровых рисков на этапе проектирования комплаенс-системы.

Эффективность применения предложенных классификационных признаков (как инструментов раннего выявления и структурирования специфических ИИ-рисков) также подтверждается через расчет предотвращенного потенциального ущерба согласно формуле:

$$L_{saved} = \sum (P_i \times C_i) \times RCR_{author}, \quad (2)$$

где P_i – вероятность наступления i-го риска; C_i – средняя стоимость репутационных потерь и штрафных санкций (например, на основе средних штрафов 2025 г.); RCR_{author} – коэффициент охвата рисков, который показывает, какую долю из всех возможных ИИ-инцидентов «видит» предложенная классификация (90% – 0,9 против 0,42 у базовых моделей).

Для практической верификации предложенной формулы и оценки реализуемости результатов на предприятии необходимо декомпозировать ее параметры через актуальные показатели 2025–2026 гг.

В данном контексте эффективность применения предложенного классификационного подхода определяется как разница между предотвращенным ущербом и затратами на имплементацию классификации в систему комплаенс-контроля организации.

Затраты на внедрение классификации I_{imp} (как интеллектуальные инвестиции) носят характер операционных расходов на совершенствование бизнес-процессов. Оценка операционных затрат O_pEx на имплементацию авторской классификации проведена на основе ресурсного подхода применительно к типовому промышленному предприятию (уровня ПАО).

Суммарная трудоемкость внедрения для одной «высоко рисковой» системы ИИ составляет 264 чел./ч и включает следующие этапы:

1) адаптация методологии (160 чел./ч) – актуализация реестра рисков и локальных нормативных актов;

2) технологический аудит алгоритмов (80 чел./ч) – проверка моделей на предмет «латентной дискриминации» специалистами Data Science;

3) обучение персонала (24 чел./ч) – целевой инструктаж ответственных за эксплуатацию систем ИИ.

Исходя из среднерыночной стоимости человеко-часа экспертов в сфере LegalTech и ИИ в 2025 г. (около 6 тыс. руб./ч с учетом налоговой нагрузки), *совокупные инвестиции в адаптацию системы комплаенса* I_{imp} составят около 1,58 млн руб. (разовая инвестиция в создание предиктивного барьера против специфических цифровых угроз).

Оценка потенциального ущерба C_i для промышленного предприятия формируется на основе двух ключевых векторов риска:

1. *Регуляторный риск*

В соответствии с положениями Регламента ЕС за использование высоко рисковых систем ИИ без процедур обеспечения прозрачности и аудита данных предусмотрены серьезные штрафные санкции. Для крупных организаций они могут достигать 1–3% годового оборота (но

не менее 10–30 млн руб. для РФ)[9]. С учетом масштаба ПАО (для примера) минимальный порог риска оценивается в 30 млн руб.

2. *Операционный и репутационный риск*

Включает прямые убытки от некорректной работы алгоритма (брак продукции, сбои в логистике, простои линий). По данным ретроспективного анализа рыночных кейсов, зафиксированных в Stanford AI Index 2025, средние потери от одного инцидента в промышленном секторе составляют 5–150 млн руб. Для расчетов используем среднее значение 70 млн руб.

Следовательно, суммарный ожидаемый ущерб C_{total} *без применения предложенного инструментария* составит 100 (30 + 70) млн руб. в течение одного года (с учетом вероятности наступления инцидента $P = 0{,}16$, согласно статистике Stanford AI Index 2025 для индустриального сектора).

Аппроксимация рисков с помощью коэффициента RCR_{author} (коэффициент охвата рисков, рассмотренный выше), отражающего расширение спектра идентификации рисков (с 42% до 90%), позволяет рассчитать прогнозную эффективность внедрения рассматриваемой модели классификации:

$$L_{saved} = \sum \left(P_i \times C_i \right) \times RCR_{author} = 100 \text{ млн руб.} \times 0{,}16 \times 0{,}9 = 14{,}4 \text{ млн руб.}$$

В денежном выражении это соответствует предотвращению потерь в размере 14,4 млн руб. ежегодно на одну внедренную систему ИИ, что в 9,1 раз (14,4/1,58) превышает инвестиции в имплементацию модифицированной модели (1,58 млн руб.).

Таким образом, процедура классификации комплаенс-рисков трансформируется из теоретического перечня признаков в прикладной управленческий регламент, позволяющий минимизировать математическое ожидание ущерба в области стратегического планирования, демонстрируя высокую окупаемость комплаенс-инновации.

Аллокация предложенных классификационных признаков в области цифрового комплаенса позволит переводить абстрактные угрозы на язык конкретных, управляемых рисков. Это предоставит компаниям возможность перейти от неопределенности к построению целенаправленной, эффективной и превентивной системы защиты, делающей инновации более устойчивыми.

Заключение

По результатам проведенного исследования получены следующие результаты.

1. Критический анализ существующих научных подходов зарубежных и отечественных авторов к классификации комплаенс-рисков позволил:

– *Выявить системный пробел*

Определено, что традиционные и большинство современных классификаций не учитывают технологическую природу технологий ИИ/БД как главного источника новых комплаенс-угроз, так как построены на отраслевом (для налогового или банковского секторов) или процедурном (коррупционный и санкционный риски) принципах;

– *Обосновать новизну исследования*

Анализ литературных источников показал, что предлагаемые подходы к классификации комплаенс-рисков либо ретроспективны и сфокусированы на последствиях, а не на специфических особенностях технологий ИИ/БД, либо фрагментарно описывают отдельные риски, порождаемые ими. Это подтвердило необходимость введения новых системообразующих признаков, таких как «Природа субъекта риска и его правового статуса», «Степень прозрачности и

[9] EUR-Lex: Access to European Union law (2024) *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)*. [online] Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng [Accessed 10.01.2026].

интерпретируемости функционирования систем ИИ», «Характер и качество данных, используемых в системах ИИ».

– *Учесть в классификации новые системные качества комплаенс-рисков*

Выделены такие сущностные черты, как масштабируемость нарушений, объяснимость и прозрачность решений, спорность субъекта нарушения как следствия технологических особенностей ИИ.

Исследование подтвердило, что технологии ИИ/БД не просто способствуют появлению новых видов рисков, а качественно изменяют саму структуру и «наполняемость» комплаенс-рисков.

2. Идентификация и описание новых специфических признаков цифровых комплаенс-рисков позволила:

– *Унифицировать понятийный аппарат*

Предложенные смысловые характеристики обеспечивают единое понимание «наполняемости» цифровых комплаенс-рисков среди разработчиков, юристов и регуляторов.

– *Систематизировать в единую логическую схему разнородные явления*

На основе выделенных общих атрибутов систематизируются в единую логическую схему такие разнородные проявления, как алгоритмическое смещение, латентная дискриминация, эмерджентное поведение систем.

– *Заложить основу для прогнозирования и предикативного управления комплаенс рисками*

Классификация формирует основу для предиктивного управления рисками и обеспечивает тем самым повышение устойчивости предприятий в условиях цифровой трансформации.

3. Проведенная верификация рассматриваемой гипотезы на примере эмпирических данных подтвердила преимущество предложенного в данной статье подхода. Результаты компаративного анализа выборки инцидентов подтверждают выдвинутую научную гипотезу и позволяют:

– *Доказать методологическую эффективность*

Использование предложенной классификации рисков расширяет охват выявляемых комплаенс рисков до 90% (против 42% у базовых моделей), что демонстрирует повышение эффективности идентификации угроз в 2,14 раза.

– *Устранить научный и практический пробел*

Полученные данные свидетельствуют о том, что предложенные признаки устраняют методологический дефицит в комплаенс-контроле, который ранее оставался вне периметра традиционных подходов.

Применение классификационных признаков позволяет:

– четко разграничить зоны ответственности и избежать штрафов за неверную юридическую квалификацию действий ИИ («*Природа субъекта риска и его правового статуса*»);

– исключить риск «черного ящика», предотвращая санкции регуляторов за непроверяемые решения («*Степень прозрачности и интерпретируемости функционирования систем ИИ*»);

– минимизировать риски дискриминации и системных ошибок, вызванных низким качеством обучающих выборок («*Характер и качество данных, используемых в системах ИИ*»).

– *Предоставить экономическое обоснование*

Проведенный расчет подтверждает, что инвестиции в имплементацию представленной модели (1,58 млн руб.) многократно окупаются за счет предотвращения потенциального ущерба (14,4 млн руб. ежегодно).

В итоге предложенная актуализированная классификация комплаенс-рисков, возникающих в результате применения технологий ИИ/БД, – это практический инструмент для повышения устойчивости бизнеса, позволяющий компаниям быстрее и безопаснее внедрять инновации.

Направления дальнейших исследований

В качестве основных направлений дальнейших исследований можно определить такие, как:

– *Верификация и количественная оценка выявленных признаков рисков*

Разработка метрик для измерения степени интерпретируемости, уровня прозрачности и масштаба распределения ответственности в конкретных системах ИИ.

– *Исследование возможностей автоматизации комплаенс-контроля за цифровыми рисками*

Разработка прототипов систем ИИ для мониторинга «наполняемости» комплаенс рисков, автоматического тестирования на «изменчивость».

– *Исследование специфики комплаенс-рисков для новых классов систем ИИ* (*генеративных моделей, систем искусственного общего интеллекта*).

Прогнозирование новых признаков рисков на основе развития технологий.

СПИСОК ИСТОЧНИКОВ

1. Maslej N., Fattorini L., Perrault R., Gil Y. et al. (2025) *Artificial Intelligence Index Report 2025*. arXiv:2504.07139, 1–456. DOI: https://doi.org/10.48550/arXiv.2504.07139

2. Trikoz E., Guliaeva E., Belyaev K. (2020) Russian experience of using digital technologies and legal risks of AI. *E3S Web of Conferences*, 224, art. no. 03005. DOI: https://doi.org/10.1051/e3sconf/202022403005

3. Ogedengbe D., Jejeniwa T., Fiemotongha J.E. (2023) Enhancing Compliance Risk Identification Through Data-Driven Control Self-Assessments and Surveillance Models. *Shodhshauryam, International Scientific Refereed Research Journal*, 6 (4), 224–248. DOI: https://doi.org/10.32628/SHISRRJ

4. Smuha N.A., Yeung K. (2024) The European Union's AI Act: beyond motherhood and apple pie? In: *The Cambridge Handbook on the Law, Ethics and Policy of Artificial Intelligence* (ed. N.A. Smuha), Cambridge University Press, 228–258.

5. Панарина М.М. (2025) Цифровой комплаенс как эффективный способ минимизации информационных рисков. *Журнал российского права*, 29 (1), 141–154. DOI: https://doi.org/10.61205/S160565900031984-6

6. Николаенков С.В. (2024) Комплаенс-риски эксплуатации ИТ-продуктов. *Стратегические решения и риск-менеджмент*, 15 (4), 360–367. DOI: https://doi.org/10.17747/2618-947X-2024-4-360-367

7. Алгалиева Г.С., Шалкарбек А. (2024) Искусственный интеллект как фактор трансформации в PR, маркетинге и медиапространстве. *Российская школа связей с общественностью*, 33, 10–27. DOI: https://doi.org/10.24412/2949-2513-2023-33-10-27

8. Володенков, С.В., Федорченко С.Н., Печенкин Н.М. (2024) Риски, угрозы и вызовы внедрения искусственного интеллекта и нейросетевых алгоритмов в современную систему социально-политических коммуникаций: по материалам экспертного исследования. *Вестник Российского университета дружбы народов. Серия: Политология*, 26 (2), 406–424. DOI: https://doi.org/10.22363/2313-1438-2024-26-2-406-424

9. Качалов Р.М., Слепцова Ю.А. (2023) Феномен риска в условиях применения алгоритмов искусственного интеллекта. *Вестник Волгоградского государственного университета. Экономика*, 25 (4), 5–16. DOI: https://doi.org/10.15688/ek.jvolsu.2023.4.1

10. Сущева Н.В. (2024) Институциональные аспекты использования искусственного интеллекта в высшем образовании и науке: роль и значение комплаенса. *Экономика и управление*, 30 (8), 905–913. DOI: https://doi.org/10.35854/1998-1627-2024-8-905-913

11. Ланская Д.В., Башук М.А., Алексанина В.А. (2024) Комплаенс: сущность и механизм имплементации в сферу управления документацией корпорации. *Вестник Академии знаний*, 3 (62), 816–823.

12. Румянцева А.Ю., Безгачева О.Л., Церкасевич Л.В. (2024) Продвижение комплаенс-контроля в банковскую сферу России. *Фундаментальные исследования*, 5, 73–77. DOI: https://doi.org/10.17513/fr.43616

13. Башкирова О.В. (2023) Классификация рисков системы цифровой идентификации граждан (на основе иностранного опыта). *Проблемы анализа риска*, 20 (1), 64–77. DOI: https://doi.org/10.32686/1812-5220-2023-20-1-64-77

14. Гаибов Г.С.О. (2022) Раскрытие информации о системе управления рисками в финансовой отчетности кредитных организаций в условиях формирования цифровых экосистем. *РИСК: Ресурсы, Информация, Снабжение, Конкуренция*, 4, 151–155. DOI: https://doi.org/10.56584/1560-8816-2022-4-151-155

15. Гаибов Г.С., Курныкина О.В. (2023) Влияние современных тенденций в банковском секторе Российской Федерации на раскрытие информации о рисках в финансовой отчетности. *Human Progress*, 9 (2), art. no. 5. DOI: https://doi.org/10.34709/IM.192.5

16. Краснослободцев А.И., Хэлльстром А.К., Хэлльстром Д.А. (2022) Исследование трансформации банковского сектора России в условиях цифровизации. *Финансовая экономика*, 3, 231–234.

17. Васильцова Н.Т., Флегонтов В.И. (2018) Новые требования к раскрытию информации в IFRS 9. *Актуальные проблемы социально-экономического развития России*, 3, 97–102.

18. Крепышева А.М., Сергиевская А.А., Сторчевой М.А. (2020) Определение и измерение риска в комплаенс-менеджменте. *Стратегические решения и риск-менеджмент*, 11 (2), 150–159. DOI: https://doi.org/10.17747/2618-947X-2020-2-150-159

19. Боровкова В.А., Люкевич И.Н., Акылбекова Н.И. (2022) Методика оценки целесообразности внедрения на предприятиях программного обеспечения риск-менеджмента. *π-Economy*, 15 (6), 128–145. DOI: https://doi.org/10.18721/JE.15609

20. Калмыкова С.В., Кобышева М.С., Сергеев Д.А. (2019) Цифровой комплаенс как фактор развития экономики региона. *Российский экономический интернет-журнал*, 4, art. no. 66.

21. Головин С.В., Луценко М.С., Шендрикова О.О. (2021) Вопросы организации комплаенс-контроля в условиях цифровой экономики. *Вестник Воронежского государственного университета. Серия: Экономика и управление*, 2, 5–26. DOI: https://doi.org/10.17308/econ.2021.2/3457

22. Хачатурян М.В. (2021) Особенности управления рисками цифровой трансформации бизнес-процессов организации в условиях пандемии. *Креативная экономика*, 15 (1), 45–58. DOI: https://doi.org/10.18334/ce.15.1.111515

23. Банк России (2024) *Обзор основных типов компьютерных атак в финансовой сфере в 2024 году*. [online] Available at: https://www.cbr.ru/collection/collection/file/55129/attack_2024.pdf [Accessed 17.11.2025]. (in Russian)

REFERENCES

1. Maslej N., Fattorini L., Perrault R., Gil Y. et al. (2025) *Artificial Intelligence Index Report 2025*. arXiv:2504.07139, 1–456. DOI: https://doi.org/10.48550/arXiv.2504.07139

2. Trikoz E., Guliaeva E., Belyaev K. (2020) Russian experience of using digital technologies and legal risks of AI. *E3S Web of Conferences*, 224, art. no. 03005. DOI: https://doi.org/10.1051/e3sconf/202022403005

3. Ogedengbe D., Jejeniwa T., Fiemotongha J.E. (2023) Enhancing Compliance Risk Identification Through Data-Driven Control Self-Assessments and Surveillance Models. *Shodhshauryam, International Scientific Refereed Research Journal*, 6 (4), 224–248. DOI: https://doi.org/10.32628/SHISRRJ

4. Smuha N.A., Yeung K. (2025) The European Union's AI Act: beyond motherhood and apple pie? In: *The Cambridge Handbook on the Law, Ethics and Policy of Artificial Intelligence* (ed. N.A. Smuha), Cambridge (UK): Cambridge University Press, 228–258.

5. Panarina M.M. (2025) Digital Compliance as an Effective Means to Minimize Information Risks. *Journal of Russian Law*, 29 (1), 141–154. DOI: https://doi.org/10.61205/S160565900031984-6

6. Nikolaenko V.S. (2024) Compliance-risks in the operation of IT products. *Strategic decisions and risk management*, 15 (4), 360–367. DOI: https://doi.org/10.17747/2618-947X-2024-4-360-367

7. Algaliyeva G.S., Shalkarbek A. (2024) Artificial intelligence as a factor of PR, marketing and media space transformation. *Russian School of Public Relations*, 33, 10–27. DOI: https://doi.org/10.24412/2949-2513-2023-33-10-27

8. Volodenkov S.V., Fedorchenko S.N., Pechenkin N.M. (2024) Risks, threats, and challenges of introducing artificial intelligence and neural network algorithms into the contemporary system of socio-political communications: The results of expert study. *RUDN Journal of Political Science*, 26 (2), 406–424. DOI: https://doi.org/10.22363/2313-1438-2024-26-2-406-424

9. Kachalov R.M., Sleptsova Yu.A. (2023) The Phenomenon of Risk Under the Application of Artificial Intelligence Algorithms. *Journal of Volgograd State University. Economics*, 25 (4), 5–16. DOI: https://doi.org/10.15688/ek.jvolsu.2023.4.1

10. Sushcheva N.V. (2024) Institutional aspects of the use of artificial intelligence in higher education and science: The role and importance of compliance. *Economics and Management*, 30 (8), 905–913. DOI: https://doi.org/10.35854/1998-1627-2024-8-905-913

11. Lanskaya D.V., Bashuk M.A., Aleksanina B.A. (2024) Compliance: the essence and mechanism of implementation in the field of corporate documentation management. *Bulletin of the Academy of Knowledge*, 3 (62), 816–823.

12. Rumyantseva A.Yu., Bezgacheva O.L., Tserkasevich L.V. (2024) Compliance control promotion in the banking sector of Russia. *Fundamental Research*, 5, 73–77. DOI: https://doi.org/10.17513/fr.43616

13. Bashkirova O.V. (2023) Digital identification system's risk classification (based on foreign experience). *Issues of Risk Analysis*, 20 (1), 64–77. DOI: https://doi.org/10.32686/1812-5220-2023-20-1-64-77

14. Gayibov G.S.O. (2022) Disclosure of information on the risk management system in the financial statements of credit institutions in the context of the formation of digital ecosystems. *RISK: Resources, Information, Supply, Competition*, 4, 151–155. DOI: https://doi.org/10.56584/1560-8816-2022-4-151-155

15. Gayibov G., Kurnykina O. (2023) Impact of modern trends in the banking sector of the Russian federation on risk disclosures in financial statement. *Human Progress*, 9 (2), art. no. 5. DOI: https://doi.org/10.34709/IM.192.5

16. Krasnoslabodcev A.I., Hellstrom A.K., Hellstrom D.A. (2022) Study of the transformation of the banking sector of Russia under the conditions of digitalization. *Financial Economy*, 3, 231–234.

17. Vasil'tsova N.T., Flegontov V.I. (2018) Novye trebovaniia k raskrytiiu informatsii v IFRS 9 [New disclosure requirements in the Unified Federal Register]. *Aktual'nye problemy sotsial'no-ekonomicheskogo razvitiia Rossii* [*Current issues of socio-economic development in Russia*], 3, 97–102.

18. Krepysheva A.M., Sergievskaya A.A., Storchevoy M.A. (2020) Definition and measurement of risk in compliance management. *Strategic decisions and risk management*, 11 (2), 150–159. DOI: https://doi.org/10.17747/2618-947X-2020-2-150-159

19. Borovkova V.A., Lyukevich I.N., Akylbekova N.I. (2022) Methodology for assessing the feasibility of implementing risk management software at enterprises. *π-Economy*, 15 (6), 128–145. DOI: https://doi.org/10.18721/JE.15609

20. Kalmykova S.V., Kobysheva M.S., Sergeev D.A. (2019) Digital compliance as a factor in the development of the regional economy. *Russian economic online journal*, 4, art. no. 66.

21. Golovin S.V., Lutsenko M.S., Shendrikova O.O. (2021) Organising compliance controls in the context of the digital economy. *Eurasian Journal of Economics and Management*, 2, 5–26. DOI: https://doi.org/10.17308/econ.2021.2/3457

22. Khachaturyan M.V. (2021) Risk management of business processes' digital transformation in the conditions of a pandemic. *Creative Economy*, 15 (1), 45–58. DOI: https://doi.org/10.18334/ce.15.1.111515

23. Bank Rossii [Bank of Russia] (2024) *Obzor osnovnykh tipov komp'iuternykh atak v finansovoi sfere v 2024 godu* [*An overview of the main types of cyber-attacks in the financial sector in 2024*]. [online] Available at: https://www.cbr.ru/collection/collection/file/55129/attack_2024.pdf [Accessed 17.11.2025]. (in Russian)

СВЕДЕНИЯ ОБ АВТОРЕ / INFORMATION ABOUT AUTHOR

ПЕТРУЧЕНЯ Ирина Владимировна
E-mail: petrucheny@gmail.com
Irina V. PETRUCHENY
E-mail: petrucheny@gmail.com

Поступила: 02.12.2025; Одобрена: 13.02.2026; Принята: 13.02.2026.
Submitted: 02.12.2025; Approved: 13.02.2026; Accepted: 13.02.2026.