Научная статья
УДК 338.246.87:004.8
DOI: 10.25683/VOLBI.2026.75.1607

Aleksey Igorevich Smirnov
Candidate of Economics, Associate Professor,
Associate Professor of the Department
of Economic and financial security,
Siberian Federal University
Krasnoyarsk, Russian Federation;
Deputy General Director
for Security,
Apatit JSC
Cherepovets, Russian Federation
smirnovsfu@mail.ru

Алексей Игоревич Смирнов
канд. экон. наук, доцент,
доцент кафедры
«Экономическая и финансовая безопасность»,
Сибирский федеральный университет
Красноярск, Российская Федерация;
заместитель генерального директора
по режиму (безопасности),
АО «Апатит»
Череповец, Россия
smirnovsfu@mail.ru

Yuriy Aleksandrovich Teterin
Senior Lecturer of the Department
of Economic and financial security,
Siberian Federal University
Krasnoyarsk, Russian Federation;
Deputy Head
of the Unified Competence Center
at the Corporate Economic Security
and Anti-Corruption Department
of the Directorate for Economic Security,
Apatit JSC
Cherepovets, Russian Federation
teterin.yuri@mail.ru

Юрий Александрович Тетерин
старший преподаватель кафедры
«Экономическая и финансовая безопасность»,
Сибирский федеральный университет
Красноярск, Российская Федерация;
заместитель начальника
Единого центра компетенций
Управления корпоративной экономической безопасности
и противодействия коррупции
Дирекции по экономической безопасности,
АО «Апатит»
Череповец, Российская Федерация
teterin.yuri@mail.ru

Aleksandr Yurievich Martynov
Deputy Head
of the Corporate Economic Security
and Anti-Corruption Department
of the Directorate for Economic Security,
Apatit JSC
Cherepovets, Russian Federation
martynovaleksandr@yandex.ru

Александр Юрьевич Мартынов
заместитель начальника
Управления корпоративной экономической безопасности
и противодействия коррупции
Дирекции по экономической безопасности,
АО «Апатит»
Череповец, Российская Федерация
martynovaleksandr@yandex.ru

Irina Rudolfovna Ruiga
Candidate of Economics, Associate Professor,
Head of the Department
of Economic and Financial Security,
Siberian Federal University
Krasnoyarsk, Russian Federation
irina_rouiga@bk.ru

Ирина Рудольфовна Руйга
канд. экон. наук, доцент,
заведующий кафедрой
«Экономическая и финансовая безопасность»,
Сибирский федеральный университет
Красноярск, Российская Федерация
irina_rouiga@bk.ru

КОРПОРАТИВНАЯ ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ: ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ КОМПЛЕКСНОЙ ПРОВЕРКИ КОНТРАГЕНТОВ

5.2.3 — Региональная и отраслевая экономика

Аннотация. *Статья посвящена исследованию направлений и разработке концептуальных рекомендаций по внедрению технологий искусственного интеллекта (ИИ) в процесс проверки контрагентов для повышения уровня корпоративной экономической безопасности. Актуальность исследования обусловлена возрастающей ролью проверки контрагентов как ключевого элемента системы корпоративной экономической безопасности. В условиях роста транзакционных издержек, ужесточения налогового контроля (включая требования к коммерческой осмотрительности) и увеличения объемов закупочной деятельности традиционные сервисы проверки контрагентов (СПАРК, «Контур.Фокус» и др.) демонстрируют ограниченную эффективность, поскольку ориентированы на «абстрактную» оценку благонадежности без привязки к конкретным параметрам договора. Предметом*

исследования выступают технологии искусственного интеллекта; объект исследования — процесс проверки контрагентов в системе корпоративной экономической безопасности. В результате исследования выявлены ключевые нерешенные научно-практические задачи: отсутствие контекстно-зависимых моделей проверки, низкий уровень внедрения искусственного интеллекта в российские сервисы, проблема объяснимости решений искусственного интеллекта (Explainable AI), ограничения информационной безопасности, отсутствие стандартизированных метрик эффективности. Определены наиболее релевантные технологии искусственного интеллекта (машинное обучение, обработка естественного языка, графовые нейронные сети, генеративный искусственный интеллект, компьютерное зрение). Предложен гибридный подход к проектированию специализированного корпоративного сервиса, сочетающий машинное обучение (градиентный бустинг), обработку естественного языка (NLP) и экспертную систему. Сформирована концептуальную модель последовательного внедрения технологий искусственного интеллекта в систему обеспечения корпоративной экономической безопасности промышленного предприятия, включающая три этапа: 1) автоматизация сбора данных и NLP-анализ; 2) предиктивная аналитика и скоринг; 3) управляемый ИИ-ассистент.

Ключевые слова: *корпоративная экономическая безопасность, проверка контрагентов, должная осмотрительность, коммерческая осмотрительность, искусственный интеллект, машинное обучение, обработка естественного языка / NLP, градиентный бустинг, экспертная система, управляемый ИИ-ассистент, генеративный искусственный интеллект, промышленное предприятие*

Для цитирования: Смирнов А. И., Тетерин Ю. А., Мартынов А. Ю., Руйга И. Р. Корпоративная экономическая безопасность: технологии искусственного интеллекта для комплексной проверки контрагентов // Бизнес. Образование. Право. 2026. № 2(75). С. 130—137. DOI: 10.25683/VOLBI.2026.75.1607.

Original article

CORPORATE ECONOMIC SECURITY: ARTIFICIAL INTELLIGENCE TECHNOLOGIES FOR COMPREHENSIVE COUNTERPARTY VERIFICATION

5.2.3 — Regional and sectoral economy

Abstract. *The article is devoted to the study of directions and the development of conceptual recommendations for the implementation of artificial intelligence (AI) technologies in the process of counterparty verification in order to enhance the level of corporate economic security. The relevance of the study is driven by the increasing role of counterparty verification as a key element of the corporate economic security system. In the context of rising transaction costs, stricter tax control (including requirements for commercial prudence), and an increasing volume of procurement activities, traditional counterparty verification services (SPARK, Kontur.Focus, and others) demonstrate limited effectiveness, as they focus on an "abstract" assessment of counterparty reliability without reference to specific contract parameters. The subject of the study is artificial intelligence technologies; the object of the study is the process of counterparty verification within the corporate economic security system. The study identifies key unresolved scientific and practical challenges: the absence of context-dependent verification models, the low level of AI implementation in Russian verification services, the problem of explainability of artificial intelligence solutions (Explainable AI), information security constraints, and the lack of standardized performance metrics. The most relevant AI technologies are identified: machine learning, natural language processing (NLP), graph neural networks (GNNs), generative AI, and computer vision. A hybrid approach to the design of a specialized corporate service is proposed, combining machine learning (gradient boosting), natural language processing (NLP), and an expert system. A conceptual model for the sequential implementation of AI technologies into the corporate economic security system of an industrial enterprise is developed, comprising three stages: (1) automated data collection and NLP analysis; (2) predictive analytics and scoring; (3) governed AI assistant with continuous monitoring.*

Keywords: *corporate economic security, counterparty verification, due diligence, commercial prudence, artificial intelligence, machine learning, natural language processing / NLP, gradient boosting, expert system, governed AI assistant with continuous monitoring, generative artificial intelligence, industrial enterprise*

For citation: Smirnov A. I., Teterin Yu. A., Martynov A. Yu., Ruiga I. R. Corporate economic security: artificial intelligence technologies for comprehensive counterparty verification. *Biznes. Obrazovanie. Pravo = Business. Education. Law*. 2026;2(75):130—137. DOI: 10.25683/VOLBI.2026.75.1607.

Введение

Актуальность. В условиях современных экономических реалий, характеризующихся высокой степенью неопределенности, ростом транзакционных издержек и ужесточением регуляторных требований (включая налоговое регулирование и налоговый контроль, проявление коммерческой осмотрительности), обеспечение корпоративной экономической безопасности хозяйствующих субъектов выступает в качестве приоритетных целей. Особое значение данная проблематика приобретает для представителей крупного промышленного бизнеса, которые в силу масштабов производственных процессов, протяженности кооперационных цепочек, высокой стоимости корпоративных активов наиболее уязвимы для недобросовестных конкурентов.

В этой связи проверка контрагентов представляет собой не просто вспомогательную функцию, а выступает в качестве ключевого элемента системы корпоративной экономической безопасности. Формирование качественной системы оценки благонадежности юридических лиц и индивидуальных предпринимателей позволяет предприятию минимизировать налоговые, регуляторные, правовые

и репутационные риски, а также в дальнейшем принимать обоснованные управленческие решения в рамках функционирования бизнеса.

На сегодняшний день рынок сервисов проверки контрагентов (СПАРК, «Контур.Фокус», «За честный бизнес» и др.) прошел достаточно длительный путь развития. Данные сервисы выступают в качестве эффективных помощников для аналитика, предоставляя доступ к унифицированным данным из различных источников [Федеральная налоговая служба (далее — ФНС), Федеральная служба государственной статистики, Федеральная служба судебных приставов (далее — ФССП), арбитражные суды и пр.]; техническая сервисная поддержка и сопровождение с учетом высокой конкуренции рынка России находится на достаточно высоком уровне. Однако, на сегодняшний день главным конкурентным преимуществом конкретного сервиса становится эффективность его интеграции в корпоративные информационные системы компаний, кроме этого, рассматриваются и дополнительные критерии:

– совместимость с ключевыми системами бизнеса (*ERP*, *CRM*, *SCM*, *BPM* и др.);

– производительность (измеряется в миллионах запросов в сутки / запросах в секунду);

– функционал (поиск компаний по разным признакам, детализация информации, возможность различных выгрузок, отчетов, формирование графов связей, мониторинг изменений и т. д.);

– надежность и стабильность (*SLA* не менее 99,9 %);

– аналитические возможности (например, формирование скорингов или использование данных сервиса в собственных скоринговых моделях бизнеса);

– возможность кастомизации под конкретные задачи бизнеса;

– масштабируемость на бизнес-единицы, бизнес-процессы.

Изученность проблемы. Вопросы обеспечения корпоративной экономической безопасности раскрываются в трудах А. И. Смирнова с соавторами [1; 2]. Аспекты изучения инструментов управления налоговыми рисками, подходов к проверке благонадежности контрагентов и соблюдения коммерческой осмотрительности представлены в исследованиях Л. В. Брянцевой [3], Н. Н. Васильевой [4], А. В. Грачева с соавторами [5], М. Н. Жариковой [6], Ю. А. Тетерина [7], А. А. Бобошко [8]. Исследование возможностей применения технологий искусственного интеллекта (далее — ИИ) в промышленности, в т. ч. для повышения эффективности процессов управления, изложено в работах А. М. Балашова [9], А. В. Зиненко [10—12], А. П. Москалева [13], П. С. Бибикова [14], Н. Г. Андриановой [15].

Анализ научных публикаций по вопросам исследования проверки контрагентов, механизмов обеспечения экономической безопасности, а также функциональных возможностей действующих сервисов, позволяет выявить нерешенную научную задачу: подавляющее большинство существующих решений ориентировано на «абстрактную» проверку контрагента (банкротство, долговая нагрузка, дисквалификация директора), но не на проверку контрагента применительно к конкретному договору, закупке или тендеру.

Более того, как следует из обзора рынка, в России уровень внедрения технологий ИИ в сервисы проверки контрагентов остается крайне низким. Многие сервисы лишь «присматриваются» к ИИ, что объективно препятствует развитию системы корпоративной экономической безопасности в целом. При этом достигнутый высокий уровень интеграции сервисов с корпоративными информационными системами и накопленные массивы исторических данных о принятых решениях создают необходимые предпосылки для активизации деятельности по внедрению ИИ.

Научная новизна исследования состоит в следующем:

1) в развитии теоретических положений экономической безопасности (в т. ч. категории «коммерческая осмотрительность»): авторами обоснована контекстно-зависимая модель оценки благонадежности;

2) в разработке гибридной трехуровневой архитектуры (*ML + NLP + Expert System*) для проверки благонадежности контрагентов, которая в отличие от существующих сервисов обеспечивает не только прогнозирование рисков, но и объяснимость решений для налоговых органов и руководства предприятия.

Указанная актуальность и проблематика предопределили **цель** исследования**,** которая заключается в обосновании направлений и разработке концептуальных рекомендаций по внедрению технологий ИИ в процесс проверки контрагентов для повышения уровня корпоративной экономической безопасности.

Задачи исследования:

1) провести контент-анализ нормативно-правовой документации и материалов судебной практики, а также обзор функциональных возможностей специализированных сервисов по проверке контрагентов;

2) провести эмпирический анализ исследований по вопросам применения технологий ИИ на промышленных предприятиях, в т. ч. для повышения эффективности процессов управления;

3) разработать концептуальные рекомендации по внедрению технологий ИИ в процесс проверки контрагентов для повышения уровня корпоративной экономической безопасности;

4) сформулировать направления для дальнейшего исследования.

Теоретическая значимость исследования заключается в развитии теоретических положений в контексте совершенствования цифровых инструментов проверки благонадежности контрагентов в аспекте повышения уровня корпоративной экономической безопасности. **Практическая значимость** заключается в возможности применения результатов исследования представителями корпоративного сектора при реализации стратегии перехода от вспомогательных инструментов к полноценным автоматизированным системам принятия решений на основе ИИ.

Основная часть

Материалы и методы исследования. В процессе исследования использованы такие общенаучные методы и подходы, как анализ, синтез, сравнение, обобщение, описание, аналогия, системный и субъектно-ориентированный подходы.

Информационная база исследования:

1) нормативные правовые акты, закрепляющие функциональные обязанности проверки контрагентов [Федеральный закон от 7 августа 2021 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»,

Налоговый кодекс РФ (ст. 5.1), Письмо ФНС России от 10 марта 2021 г. № БВ-4-7/3060@ (разъяснение критериев выбора контрагента в целях получения налоговой выгоды, что является принципиально значимым для разработки автоматизированных систем проверки с учетом вариации требований к проверке в зависимости от параметров конкретной сделки)];

2) материалы судебной практики Верховного суда РФ; информационно-аналитические материалы АНО «Цифровая экономика»; официальные сайты специализированных сервисов по проверке контрагентов [СПАРК (Интерфакс), «Контур.Фокус», СБИС («Тензор») и др.].

Контент-анализ нормативно-правовой документации и материалов судебной практики свидетельствует о том, что проверка контрагентов перестает быть исключительно внутренней процедурой службы экономической безопасности компании и приобретает характер юридически значимого действия, влияющего на налоговые последствия и корпоративную ответственность.

Обзор функциональных возможностей специализированных сервисов указывает на отсутствие явных конкурентных преимуществ в виду получения информации из одних и тех же государственных источников и наличие интеграционных возможностей с корпоративными информационными системами; не предусматривается практическая реализация решения проблемы оценки благонадежности контрагента в рамках конкретной закупочной процедуры с заданными параметрами (сумма, сроки, предмет поставки, условия оплаты и пр.). Данное ограничение порождает значительный объем ручного труда аналитиков экономической безопасности, которые вынуждены самостоятельно сопоставлять параметры сделки с рисками контрагента. В условиях промышленного предприятия с объемом проверок более 100 тыс. в год этот «интеллектуальный разрыв» становится критическим фактором, сдерживающим скорость принятия управленческих решений и полноту учета рисков компании.

Эмпирический анализ исследований по вопросам проверки контрагентов на промышленных предприятиях [7; 10; 13; 14] указывает на необходимость формирования концептуального подхода к проектированию специализированной информационно-аналитической системы, учитывающей отраслевую характеристику и специфику, интегрированной с корпоративным ландшафтом.

С точки зрения бизнеса проблема отсутствия автоматизированного решения по проверке контрагентов основанного на ИИ — это очень длительный процесс проверки, что зачастую замедляет многие бизнес-процессы. С точки зрения корпоративной экономической безопасности аналогичная проблема — это невозможность эффективного учета всех факторов при принятии решения о благонадежности контрагента в рамках конкретной закупки, тендера или договора.

Резюмируя выше изложенное, сформулированы следующие нерешенные научно-практические задачи:

1. ***Отсутствие контекстно-зависимых моделей проверки***. Существующие решения оценивают контрагента как такового, а не в привязке к конкретным параметрам договора (сумма, сроки, предмет поставки, условия оплаты, штрафные санкции). Это противоречит требованиям ФНС о дифференцированном подходе к коммерческой осмотрительности (Письмо ФНС России от 10 марта 2021 г. №БВ-4-7/3060@).

2. ***Низкий уровень внедрения ИИ в российских сервисах***. Как следует из обзора рынка, большинство сервисов только рамочно тестирует технологии ИИ, что сдерживает развитие системы корпоративной экономической безопасности в целом.

3. ***Проблема объяснимости (Explainable AI)***. Для принятия юридически значимых решений требуется, чтобы ИИ не просто выдавал результаты оценки, но и производил обоснование (подкрепляя ссылками на конкретные факты и источники данных).

4. ***Безопасность и конфиденциальность***. Промышленные предприятия не могут использовать публичные облачные *LLM* (*OpenAI*, *Anthropic*, *Google*) для обработки данных о контрагентах в силу требований информационной безопасности и Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Требуются решения *on-premise* на российских моделях.

5. ***Отсутствие стандартизированных метрик эффективности***. В актуальных научных исследованиях отсутствует предложение по разработке унифицированной системы показателей для оценки качества ИИ-проверки контрагентов (*precision*, *recall*, *F1-score* применительно к выявлению недобросовестных поставщиков).

С другой стороны, в контексте решения указанных ограничений современное развитие ИИ формирует технологическую основу для их преодоления. Анализ применимых технологий ИИ [7; 12; 13] для задачи проверки контрагента позволил выявить наиболее релевантные:

1) ***машинное обучение*** (*ML*): построение скоринговых моделей, прогнозирование банкротства и дефолта;

2) ***обработка естественного языка*** (*NLP*): извлечение сущностей из судебных решений, анализ тональности новостей, семантический анализ договоров;

3) ***графовые нейронные сети*** (*GNN*): выявление цепочек аффилированности, поиск скрытых связей между компаниями;

4) ***генеративные модели*** (*LLM*): формирование отчетов с рекомендациями, ответы на вопросы аналитика в диалоговом режиме;

5) ***компьютерное зрение*** (*CV*): распознавание сканированной документации, печати, подписи.

Результаты исследования. Определяя современный этап интеграции ИИ в автоматизированные процессы проверки контрагентов как начальный, ключевой задачей представляется определение новых дополнительных требований к сервису по проверке контрагентов с учетом потенциального использования достижений в области ИИ. Главным образом выделим функциональные и технические требования, а также требования к данным.

1. ***Функциональные требования***:

– комплексный автоматизированный сбор и анализ данных из всех доступных источников [в т. ч. использование автоматизированных инструментов *Open Source Intelligence* (*OSINT*) при условии проведения фактчекинга и присвоения уровня доверия к данным], например для определения скрытых связей между формально неаффилированными между собой компаниями, а также для оценки репутационных рисков.

– формирование инструментов прогнозирования банкротства, изменений в финансовом состоянии, неисполнения обязательств контрагентом на основе машинного обучения;

– генерация информативных отчетов с конкретными рекомендациями;

– мониторинг в реальном времени;

– интеграция с большинством корпоративных систем компании для своевременного принятия управленческих решений (блокировка платежей, поставок, допусков и т. д.).

2. ***Технические требования***:

– масштабируемость на отраслевой или национальный уровень (архитектура должна поддерживать рост числа пользователей и объема обрабатываемых данных без потери производительности);

– высокий уровень производительности, отказоустойчивости и информационной безопасности;

– использование передовых технологий (*ML*, *DL*, *NLP*, генеративные модели (в т. ч. *LLM*), компьютерное зрение, системы обнаружения аномалий, автоматизированные системы реагирования на инциденты и т.д.).

3. ***Требования к данным*** (актуальность, достоверность, полнота, унификация и т. д.).

Не менее важны требования к интерфейсу, нормативно-правовые, эксплуатационные и требования, которые в целом следует рассматривать, ориентируясь на лучшие практики рынка.

Концептуальный подход предлагаемого решения выглядит следующим образом:

1. ИИ должен уметь идентифицировать и понимать основания для закупок, условия тендеров, конкурентные листы, тексты договоров как объекты, с которыми он может работать в привязке с параметрами соответствующих контрагентов.

2. ИИ запускает проверку в сервисе, анализирует выявленные риск-факторы, исторические данные о проверках, данные скоринговых моделей. Далее объект, содержащий параметры закупки или договора, используется в качестве ключевого элемента оценки благонадежности. Важно понимать, что контрагент проверяется не абстрактно, а в привязке к конкретным параметрам объекта.

3. ИИ генерирует отчет и направляет заключение на согласование аналитику по экономической безопасности (происходит коммуникация аналитика с ИИ в рамках обучения модели). После согласования в соответствующем основанию порядке ИИ вносит необходимую информацию к корпоративную информационную систему.

Учитывая изложенные функциональные и технические требования, требования к данным, а также концептуальные тезисы предлагаемого решения, полагаем целесообразным представить следующие технологии ИИ с учетом применимости в процедуре проверки контрагента и степени важности (см. табл.).

Технологии искусственного интеллекта для проверки контрагента

Технологии ИИ	Функциональная роль в процедуре проверки	Оценка важности для комплексной проверки
Машинное обучение (*ML*). Градиентный бустинг	Построение итоговой формулы риска, определение весовых значений включенных признаков. Автоматическое агрегирование данных ФНС, ФССП, арбитражных судов (дела), картотеки арбитражных дел (тексты решений), СМИ и социальных сетей (упоминания), корпоративных баз данных компании (история платежей)	Максимальная (ключевая)
Обработка естественного языка (*NLP*)	Расшифровка неструктурированных текстов. Анализ тональности. Идентификация фактов из судебных актов новостных сообщений, социальных сетей (информация, не включенная в табличный формат, важная часть для нечисловых данных)	Выше среднего
Экспертная система	Дополнение юридически значимыми «риск-факторами» и «стоп-факторами»	Средняя
Генеративный ИИ (*LLM*)	Формирование заключения по отчету	Минимальная (формирует удобство для пользователя)
Компьютерное зрение (*CV*)	Распознавание сканированных документов, печатей, подписей	Минимальная (применение только на входе данных)

Таким образом, в силу таких требований, как объяснимость (почему взаимодействие с данным контрагентом исключено) и работа с разнородными данными (цифры, текст, реестры) для проектирования специализированного корпоративного сервиса из представленных в таблице технологий ИИ предлагается гибридное решение на основе комбинации технологий машинного обучения (*ML*) (а именно градиентный бустинг для расчета итогового индекса риска) в совокупности с обработкой естественного языка (*NLP*) для извлечения смысла из неструктурированного текста (судебные решения, СМИ, социальные сети) и элементами экспертных систем для формирования жестких фильтров (черные списки). Указанная комбинация не противоречит функциональному концепту систем «СПАРК-Риски» (Интерфакс), «Контур.Фокус» и скоринговых систем в Сбере/Тинькофф.

Среди ограничений для формирования подобных сервисов можно выделить следующие:

– отсутствие возможности использования моделей лидеров мирового ИИ таких как *OpenAI*, *Anthropic*, *Google* и др.;

– приоритеты информационной безопасности компаний и как следствие стремление многих компаний развернуть «собственный» ИИ в закрытом контуре на «слабых» моделях;

– долгое обучение моделей для эффективного учета контекста, переобучение по причине дискриминирующих результатов, галлюцинаций ИИ;

– зависимость эффективности модели от качества и полноты данных.

Таким образом, сервисы по проверке контрагентов должны быть еще более интегрированными в информационные системы компаний, должны стать интеллектуальными (на основе ИИ) и превратиться из помощника аналитика в систему подготовки проектов обоснованных решений по благонадежности контрагента максимально учитывая требования регуляторов и потребностей бизнеса.

Резюмируя изложенное представляется целесообразным сформировать концептуальную модель последовательного внедрения технологий ИИ в систему обеспечения корпоративной экономической безопасности промышленного предприятия (см. рис.).

I ЭТАП. АВТОМАТИЗАЦИЯ СБОРА ДАННЫХ И NLP-АНАЛИЗ	
Цель: *Замена ручного труда по сбору данных из более чем 10 источников. Получение навыков понимания неструктурированного текста (судебные решения, СМИ, социальные сети)*	
Технология: *NLP (извлечение сущностей, анализ тональности), RAG-агенты*	
Интеграция в ИС: *Внедрение ИИ-модуля в существующую CRM/ERP (например, 1С) и платформу комплаенса*	
Позиции по внедрению	***Ожидаемый эффект***
Автоматизированный сбор данных	Сокращение времени сбора информации
NLP-анализ судебных решений	Ранне выявление риска мошенничества (ст. 159 УК)
RAG-отчет по документам	Ускорение процедуры комплексной проверки (*ускорение Due Diligence на 70 %*)
Интеграция: *Подключение API к внутренней базе контрагентов. При загрузке ИНН система автоматически подтягивает и структурирует данные*	
II ЭТАП. ПРЕДИКТИВНАЯ АНАЛИТИКА И СКОРИНГ	
Цель: *Переход от констатации фактов к процедуре пргнозирования (вероятность банкротства / блокировка счетов)*	
Технологии: *Машинное обучение (градиентный бустинг), Предиктивная аналитика*	
Позиции по внедрению	***Ожидаемый эффект***
Скоринг-модель «Кредитный лимит»	Снижение доли «плохих» долгов
Факторный анализ аффилированности	Защита от сговора и картельных схем
Санкционный комплаенс	Соответствие требованиям Международного права
Интеграция: *Встраивание модели в модуль «Финансовый контроль» ERP (При попытке создать заказ на сумму более 5 млн руб. система требует авторизации по результатам ИИ-скоринга)*	
II ЭТАП. УПРАВЛЯЕМЫЙ ИИ-АССИСТЕНТ	
Цель: *создание «цифрового помощника» для специалиста экономической безопасности, полная автоматизация процесса мониторинга и прогнозирования*	
Технологии: *LLM-агенты с ролью (Role-Based Agents), Low-code платформы*	
Позиции по внедрению	***Ожидаемый эффект***
Гибридный ИИ-ассистент	Экономия времени аналитика
Управляемый ИИ-ассистент (Governed AI)	Исключение утечек данных. Соответствие 152-ФЗ и 115-ФЗ
Continuous Monitoring	Снижение операционных потерь
Интеграция: *Low-code платформа (например, на базе решений GreenData или СберКорус). Возможности для специалистов ДЭБ самостоятельно менять правила проверки без функционала программистов, подстраиваясь под изменения в 54.1 НК РФ*	

Рис. Концептуальную модель последовательного внедрения технологий искусственного интеллекта в систему обеспечения корпоративной экономической безопасности промышленного предприятия

Заключение

Перспектива развития ИИ в сфере проверки контрагентов заключается в постепенном переходе от вспомогательных инструментов к полноценным автоматизированным системам принятия решений, способным учитывать многогранность и специфику каждой сделки.

В ближайшие 2—3 года можно ожидать следующих шагов по развитию:

1. Углубление алгоритмов машинного обучения — переход от расчета общего индекса риска к прогнозированию вероятности конкретных рисков (например, неисполнения обязательств, мошенничества, скрытых аффилированных связей) с детализацией по типам закупок/договоров.

2. Совершенствование *NLP*-технологий — расширение базы неструктурированных данных (включая многоязычные источники, внутренние отчеты компаний, профессиональные форумы) и повышение точности извлечения релевантных сигналов (например, признаков финансовых трудностей, репутационных рисков).

3. Интеграция с блокчейн-технологиями и электронными подписями для автоматического верифицирования легитимности документов и истории контрагентов.

4. Развитие гибридных экспертных систем с возможностью самообучения на основе обратной связи от аналитиков (например, анализ причин отклоненных сделок для корректировки весовых коэффициентов рисков).

5. Создание унифицированных *API* для бесшовной интеграции ИИ-решений с корпоративными *ERP*, *CRM*, системами электронного документооборота.

6. Внедрение объяснимого ИИ (*XAI*) — предоставление аналитикам прозрачных отчетов с обоснованием принятых системой решений (например, топ-5 факторов, повлиявших на оценку благонадежности).

7. Разработка модульных решений для разных отраслей (строительство, *IT*, ритейл), учитывающих специфику контрактных требований и типичных рисков.

8. Синхронизация с государственными реестрами (ФНС, ФССП, ЕГРЮЛ) в режиме реального времени для оперативного выявления изменений в статусе контрагентов.

9. Использование мультимодальных моделей (комбинация текста, таблиц, изображений) для анализа всей доступной информации (например, фото объектов недвижимости, отчетов о производственных мощностях).

10. Этическое и правовое регулирование — разработка стандартов прозрачности, защиты данных и ответственности за решения, принятые ИИ-системами.

Итогом развития станет создание «цифрового аналитика» — интеллектуального помощника, способного на основе многофакторного анализа предлагать оптимальные сценарии взаимодействия с контрагентами, минимизируя риски и оптимизируя транзакционные издержки. Это позволит компаниям перейти на проактивный уровень управления экономическими рисками, опережая потенциальные угрозы за счет предиктивной аналитики и автоматизации рутинных проверок.

Говоря о перспективах и конкретных задачах сегодняшнего дня в аспекте развития ИИ в сфере проверки контрагентов, большим компаниям и их вендорам информационно-аналитических систем следует начинать формировать техническое задание для разработки прототипа ИИ-системы автоматизированной проверки контрагентов с учетом предложенного гибридного подхода.

СПИСОК ИСТОЧНИКОВ

1. Смирнов А. И., Тетерин Ю. А., Руйга И. Р., Мартынов А. Ю. Концепция корпоративной экономической безопасности: базовые положения, механизмы обеспечения и этапы реализации // Финансовый менеджмент. 2025. № 1. С. 185—197.

2. Руйга И. Р., Смирнов А. И., Тетерин Ю. А., Мартынов А. Ю. Концептуальный подход к оценке корпоративной экономической безопасности на основе интеграции методов программирования и машинного обучения // Национальные интересы: приоритеты и безопасность. 2025. Т. 21. № 7. С. 79—99. DOI: 10.24891/hcasfn.

3. Брянцева Л. В., Бичева Е. Е. Налоговые риски в системе обеспечения экономической безопасности // Современная экономика: проблемы и решения. 2024. № 8(176). С. 94—106.

4. Васильева Н. Н., Свинов А. В., Ткачук О. В. Адаптация системы управления рисками на предприятии промышленного типа // Интеллектуальные системы в производстве. 2021. Т. 19. № 3. С. 134—141. DOI: 10.22213/2410-9304-2021-3-134-141.

5. Грачев А. В., Сикорская Л. В., Виноградова Ю. А. Оценка надежности контрагентов как инструмент обеспечения экономической безопасности хозяйствующего субъекта // Известия высших учебных заведений. Серия: Экономика, финансы и управление производством. 2022. № 4(54). С. 44—52.

6. Жарикова М. Н. О некоторых вопросах проявления должной осмотрительности при выборе контрагента // Вестник Челябинского государственного университета. Серия: Право. 2023. Т. 8. № 3. С. 28—33. DOI: 10.47475/2618-8236-2023-8-3-28-33.

7. Тетерин Ю. А. Инструменты мониторинга и прогнозирования в системе коммерческой осмотрительности для минимизации налоговых рисков компании // Интеллектуальная инженерная экономика и Индустрия 6.0 (ИНПРОМ-2025) : сб. тр. Междунар. науч.-практ. конф. : в 2 т. СПб. : ПОЛИТЕХ-ПРЕСС, 2025. Т. 2. С. 157—160.

8. Бобошко А. А., Куприн А. А., Вержбицкая А. В. Сущность коммерческой осмотрительности при проверке надежности контрагента как инструмента экономической безопасности // Экономика и управление народным хозяйством. 2024. № 19(21). С. 91—96.

9. Балашов А. М. Цифровизация и использование искусственного интеллекта в производственных процессах современных предприятий // Теоретическая экономика. 2024. № 11. С. 34—41. DOI: 10.52957/2221-3260-2024-11-34-41.

10. Зиненко А. В. Интегрирование элемента «машина» в организационную систему институционального инвестора // Современные наукоемкие технологии. 2025. № 9. С. 58—62. DOI: 10.17513/snt.40486.

11. Зиненко А. В. Комплексная методология поддержки принятия инвестиционных решений // Модели, системы, сети в экономике, технике, природе и обществе. 2025. № 3. С. 141—152. DOI: 10.21685/2227-8486-2025-3-11.

12. Зиненко А. В., Балабанова Н. В. Компартментная модель оценки финансовых рисков // Современные наукоемкие технологии. Региональное приложение. 2022. № 3(71). С. 27—32.

13. Москалев А. П. Автоматизированные системы мониторинга контрагентов на основе больших данных для снижения бизнес-рисков // Интеллектуальная инженерная экономика и Индустрия 6.0 (ИНПРОМ-2025) : сб. тр. Междунар. науч.-практ. конф. : в 2 т. СПб. : ПОЛИТЕХ-ПРЕСС, 2025. Т. 2. С. 128—132.

14. Бибиков П. С. Цифровые технологии, блокчейн и искусственный интеллект в развитии финансового контроля электроэнергетических корпораций // Вестник евразийской науки. 2025. Т. 17. № s2. URL: https://esj.today/PDF/15FAVN225.pdf.

15. Андрианова Н. Г. Искусственный интеллект в налоговом контроле: проблемы и перспективы правового регулирования // Налоги и налогообложение. 2025. № 3. С. 22—32. DOI: 10.7256/2454-065X.2025.3.74301.

REFERENCES

1. Smirnov A. I., Teterin Yu. A., Ruyga I. R., Martynov A. Yu. The concept of corporate economic security: basic provisions, mechanisms for ensuring and stages of implementation. *Finansovyi menedzhment = Financial management*. 2025;1:185—197. (In Russ.)

2. Ruiga I. R., Smirnov A. I., Teterin Yu. A., Martynov A. Yu. Conceptual framework for assessing corporate economic security through the integration of programming and machine learning techniques. *Natsional`nye interesy: prioritety i bezopasnost` = National Interests: Priorities and Security*. 2025;21(7):79—99. (In Russ.) DOI: 10.24891/hcasfn.

3. Bryantseva L. V., Bicheva E. E. Tax risks in the economic security system. *Sovremennaya ekonomika: problemy i resheniya = Modern economics: problems and solutions*. 2024;8(176):94—106. (In Russ.)

4. Vasilyeva N. N., Svinov A. V., Tkachuk O. V. Adaptation of the Risk Management System in an Industrial-Type Enterprise. *Intellektual`nye sistemy v proizvodstve = Intelligent systems in manufacturing*. 2021;19(3):134—141. (In Russ.) DOI: 10.22213/2410-9304-2021-3-134-141.

5. Grachev A. V., Sikorskaya L. V., Vinogradova Ju. A. Assessment of counterpart reliability as a tool to ensure economic security of an economic subject. *Izvestiya vysshikh uchebnykh zavedenii. Seriya "Ekonomika, finansy i upravlenie proizvodstvom" = News of higher educational institutions. Series "Economy, finance and production management"*. 2022;4(54):44—52. (In Russ.)

6. Zharikova M.N. Some issues of due diligence in choosing a counterparty. *Vestnik Chelyabinskogo gosudarstvennogo universiteta. Seriya: Pravo = Bulletin of Chelyabinsk State University. Series: Law*. 2023;8(3):28—33. (In Russ.) DOI: 10.47475/2618-8236-2023-8-3-28-33.

7. Teterin Yu. A. Monitoring and forecasting tools in the commercial diligence system to minimize the company's tax risks. *Intellektual`naya inzhenernaya ekonomika i Industriya 6.0 (INPROM-2025) = Intelligent Engineering Economics and Industry 6.0 (INPROM-2025). Proceedings of the International scientific and practical conference*. Saint Petersburg, POLYTECH-PRESS, 2025;2:157—160. (In Russ.)

8. Boboshko A. A., Kuprin A. A., Verzhbitskaya A. V. The essence of commercial prudence in verifying the reliability of a counterparty as an instrument of economic security. *Ekonomika i upravlenie narodnym khozyaistvom*. 2024; 19(21):91—96. (In Russ.)

9. Balashov A. M. Digitalization and the use of artificial intelligence in the production processes of modern enterprises. *Teoreticheskaya ekonomika = Theoretical economics*. 2024;11:34—41. (In Russ.) DOI: 10.52957/2221-3260-2024-11-34-41.

10. Zinenko A. V. "Machine" element integration into an institutional investor organizational system. *Sovremennye naukoemkie tekhnologii = Modern high technologies*. 2025;9:58—62. (In Russ.) DOI: 10.17513/snt.40486.

11. Zinenko A. V. Comprehensive methodology of supporting investment decisions. *Modeli, sistemy, seti v ekonomike, tekhnike, prirode i obshchestve = Models, systems, networks in economics, technology, nature and society*. 2025;3:141—152. (In Russ.) DOI: 10.21685/2227-8486-2025-3-11.

12. Zinenko A. V., Balabanova N. V. Compartment model for assessing financial risks. *Sovremennye naukoemkie tekhnologii. Regional`noe prilozhenie = Modern high technologies. Regional application*. 2022;3(71):27—32. (In Russ.)

13. Moskalev A. P. Automated systems for counterparty monitoring based on big data: a key to reducing business risks. *Intellektual`naya inzhenernaya ekonomika i Industriya 6.0 (INPROM-2025) = Intelligent Engineering Economics and Industry 6.0 (INPROM-2025). Proceedings of the International scientific and practical conference*. Saint Petersburg, POLYTECH-PRESS, 2025;2:128—132. (In Russ.)

14. Bibikov P. S. Digital technologies, blockchain and artificial intelligence in the development of financial control of electric power corporations. *Vestnik evraziiskoi nauki = The Eurasian Scientific Journal*. 2025;17(s2). (In Russ.) URL: https://esj.today/PDF/15FAVN225.pdf.

15. Andrianova N. G. Artificial intelligence in tax control: problems and prospects of legal regulation. *Nalogi i nalogooblozhenie = Taxes & taxation*. 2025;3:22—32. (In Russ.) DOI: 10.7256/2454-065X.2025.3.74301

Статья поступила в редакцию 10.03.2026; одобрена после рецензирования 19.04.2026; принята к публикации 20.04.2026.
The article was submitted 10.03.2026; approved after reviewing 19.04.2026; accepted for publication 20.04.2026.