Финансы и управление
Правильная ссылка на статью:
Ротко А.Г. Анализ цифровых следов и реестровых данных в системе корпоративной безопасности // Финансы и управление. 2025. № 2. DOI: 10.25136/2409-7802.2025.2.74927 EDN: KFSSZP URL: https://nbpublish.com/library_read_article.php?id=74927

Анализ цифровых следов и реестровых данных в системе корпоративной безопасности

Ротко Андрей Геннадьевич

ORCID: 0009-0009-6688-093X

Магистр; Институт проблем безопасности; Национальный исследовательский университет «Высшая школа экономики»

109012, Россия, г. Москва, Таганский р-н, Славянская пл., д. 4 стр. 2

agrotko@edu.hse.ru

Статья из рубрики "Финансовый мониторинг"

DOI:

10.25136/2409-7802.2025.2.74927

EDN:

KFSSZP

Дата направления статьи в редакцию:

21-06-2025

Аннотация: Предметом исследования является система проверки контрагентов на этапе предварительного анализа в целях обеспечения экономической безопасности компании. Объектом исследования выступают процедуры due diligence в корпоративной практике, направленные на выявление рисков взаимодействия с ненадёжными партнёрами. Автор подробно рассматривает такие аспекты темы, как использование цифровых следов, правовых и поведенческих индикаторов в оценке благонадёжности контрагента. Особое внимание уделяется анализу информации из открытых источников, таких как государственные реестры, судебные базы, агрегаторы новостей и платформы коммерческой аналитики. В статье исследуется, как данные из цифровой среды могут быть интегрированы в систему внутреннего контроля. Также рассматриваются механизмы адаптации подхода KYC (Know Your Customer) к российским условиям. Автор выделяет особенности формирования модели ИРЦК (интегральный риск цифрового контрагента), применимой в рамках автоматизированной проверки деловых партнёров. Работа основана на примере конкретного кейса в строительной отрасли, что позволяет

продемонстрировать практическую значимость применяемых методов. В исследовании применяются методы контент-анализа, кейс-стади и сравнительного анализа, а также построена авторская модель оценки риска — ИРЦК. Новизна исследования заключается в разработке прикладной модели интегрального риска цифрового контрагента (ИРЦК), учитывающей юридические, финансовые и поведенческие параметры на основе цифровых источников. Особым вкладом автора в исследование темы является систематизация подходов к анализу цифрового следа контрагента в рамках процедур внутреннего контроля и оценки благонадёжности. Основными выводами проведенного исследования являются подтверждение практической значимости комплексной цифровой оценки при реализации принципа должной осмотрительности, а также возможность интеграции предложенной модели в автоматизированные системы проверки. Результаты исследования демонстрируют, что использование данных из открытых реестров, медиасреды и коммерческих аналитических платформ позволяет сократить субъективность в принятии решений и повысить уровень экономической безопасности компании. Работа может быть полезна специалистам в сфере управления рисками, комплаенса и инвестиционного анализа.

Ключевые слова:

экономическая безопасность, цифровой след, анализ контрагента, должная осмотрительность, система внутреннего контроля, риск-контроль, открытые источники информации, комплаенс-проверка, корпоративная безопасность, оценка благонадёжности

Введение

Корпоративная безопасность как научная и прикладная категория начала формироваться в российской практике в конце 1990-х – начале 2000-х годов под влиянием становления института частной охраны и служб экономической безопасности внутри крупных корпораций [1; 5]. Если на начальных этапах в фокусе внимания находились преимущественно физическая охрана и защита имущественных интересов, то к середине 2010-х годов вектор сместился в сторону комплексного управления рисками, включающего правовые, финансовые, репутационные и информационные угрозы [6; 18].

В отечественной и зарубежной литературе под корпоративной безопасностью традиционно понимается совокупность мер по выявлению, предотвращению и нейтрализации внутренних и внешних угроз, способных нанести ущерб имущественным, кадровым, репутационным и иным интересам хозяйствующего субъекта [1; 9; 18]. В современной трактовке корпоративная безопасность включает в себя оценку контрагентов, мониторинг партнёрской среды, анализ утечек информации, цифровую репутацию, а также мероприятия по внутреннему контролю и соблюдению комплаенс-процедур [4; 6; 17].

Важным направлением деятельности служб корпоративной безопасности является due diligence — практика предварительной оценки благонадёжности и рисков при выборе партнёров [13; 15]. Однако в условиях цифровизации экономики, распространения теневых финансовых схем и использования номинальных структур классические методы проверки становятся всё менее эффективными. На первый план выходит анализ цифровых следов: информационных фрагментов, оставляемых субъектами хозяйственной

деятельности в публичных источниках, цифровых реестрах и информационном пространстве [4; 12].

Современные вызовы требуют включения в арсенал корпоративной безопасности новых источников информации, таких как базы данных арбитражной и уголовной практики, сведения из Федресурса и ЕГРЮЛ, информация о банкротствах, аффилированности, публичных контрактах, а также сигналы из СМИ, социальных сетей и специализированных каналов в мессенджерах [13; 19]. Возникает задача не только доступа к этим источникам, но и их системного анализа, формализации критериев интерпретации и оценки рисков [3; 19].

Анализ степени разработанности темы показывает, что вопросы организации due diligence и комплаенс-процедур рассматривались в трудах таких авторов, как В. В. Астанин, М. М. Панарина, А. В. Страдымов и др.[9; 18; 24]. Особое внимание уделяется юридическим и организационным аспектам проверки контрагентов, применению системного подхода к выявлению рисков, а также построению антикоррупционной экспертизы [17; 24]. Зарубежные исследователи S. Biegelman, T. Fox, M. Pieth акцентируют внимание на цифровом комплаенсе, принципе прослеживаемости и анализе цифрового поведения компании [20; 21; 22].

В то же время, несмотря на активное развитие нормативно-методических основ due diligence, остаются нерешёнными вопросы интеграции цифровых следов в процесс оценки контрагентов. Не представлено достаточное количество эмпирических исследований, где цифровая активность и информация из электронных реестров использовались бы в комплексе для принятия решений в корпоративной безопасности [4; 13; 15].

Таким образом, предметом настоящего исследования выступает система инструментов анализа цифровых и реестровых данных, применимых в рамках корпоративной проверки контрагентов. Целью работы является обоснование методического подхода, позволяющего на основе анализа цифрового следа формировать целостную оценку рисков, ассоциированных с конкретным хозяйствующим субъектом.

В ходе исследования использованы методы контент-анализа, case-study и сравнительной оценки на основе материалов публичных источников и кейсов из корпоративной практики. Гипотеза исследования заключается в том, что комплексный анализ цифровых следов и реестровых данных позволяет выявить ранее недоступные риски и существенно повысить эффективность due diligence-процедур.

Статья включает четыре основных раздела. В разделе «Методы» изложены методологические основания исследования, источники данных и принципы построения модели цифрового риска. Раздел «Результаты» содержит эмпирический анализ цифровых профилей контрагентов, рассчитанные значения интегрального показателя риска и визуализацию сравнений. В разделе «Обсуждение» представлены интерпретация полученных данных, выявленные ограничения и перспективы практического применения предложенной модели. Заключительный раздел включает обобщающие выводы, а также направления дальнейших исследований и возможные векторы развития предложенного подхода.

Основная часть

Методы

Настоящее исследование опирается на комплексный методический подход, объединяющий элементы контент-анализа, сравнительного анализа, кейс-стади и анализа цифрового поведения хозяйствующих субъектов [4; 12; 19]. Основной акцент сделан на изучении открытых данных, образующих так называемый цифровой след юридического лица, а также официальных сведений, содержащихся в государственных и коммерческих реестрах [13; 4; 6].

Материалы исследования сформированы на основе анализа: Государственных реестров юридических лиц и индивидуальных предпринимателей (ЕГРЮЛ, ЕГРИП)[25]; Информационной системы сообщений о банкротстве (Федресурс)[26]; Единой информационной системы в сфере закупок (zakupki.gov.ru) [27]; Судебных решений из ГАС «Правосудие» и КАД «Арбитр»[28]; Платформ коммерческой аналитики (СПАРК, Контур.Фокус, RuData, Zachestnybiznes)[29]; Публичных упоминаний в СМИ и Telegram-каналах, доступных через агрегаторы новостей и поисковые системы (Yandex.News, Google Alerts, TgStat)[30]. Данные за 2022–2024 гг. были структурированы в аналитические профили по каждой исследуемой организации и проверены на полноту, достоверность и повторяемость [12].

В рамках исследования применялся комплекс методов, направленных на интерпретацию цифровых следов контрагентов и их сопоставление с формализованными юридическими данными.

Контент-анализ. Для обработки цифровых следов использовался как ручной, так и автоматизированный анализ текстовых упоминаний с акцентом на выявление маркеров риска. К таким маркерам относились: наличие негативных публикаций в СМИ и социальных сетях, участие компании или её представителей в процедурах банкротства, аффилированность с субъектами, находящимися под санкциями или в статусе фигурантов уголовных дел, а также аномальная цифровая активность (включая всплески упоминаний, удаление страниц, резкие изменения информационного фона) [4; 13; 19].

Кейс-анализ (case study). Проведено сопоставление трёх эмпирических кейсов (организации А, Б и В), в отношении которых были реализованы процедуры проверки с применением как классических источников (реестры, судебные базы), так и цифровых инструментов. Сравнение позволило продемонстрировать информативность и предикативность цифровых следов в контексте раннего выявления репутационных и юридических рисков [15].

Сравнительный анализ. Применялся для сопоставления параметров цифрового поведения с данными официальных реестров. Отдельное внимание уделялось расхождениям между заявленной и фактической деловой активностью: например, отсутствием судебных упоминаний в ЕГРЮЛ при наличии арбитражных споров в ГАС «Правосудие» [13; 16].

Элементы экспертной оценки. Для интерпретации совокупных признаков цифрового поведения использовалась внутренняя шкала оценки, применяемая в Компании Х, включающая восемь ключевых критериев: частотность негативных упоминаний, юридическая история, наличие в реестрах недобросовестных поставщиков, участие в банкротных процедурах, аффилированность, реакция медиа, частота смены учредителей и руководства, признаки низкой цифровой прозрачности [2; 9; 18].

В рамках исследования был разработан интегральный показатель цифрового риска (ИРЦК), представляющий собой взвешенную сумму значений по ряду ключевых критериев. Методика основана на полуструктурированной шкале оценки, разработанной на основе практического опыта в области корпоративной безопасности и обобщения типовых кейсов из строительного сектора [6; 9].

Весовые коэффициенты критериев определены экспертным путём с учётом частоты и значимости проявлений признаков риска в ранее верифицированных инцидентах [3; 18].

Значимость каждого критерия задавалась в виде весового коэффициента, отражающего его вклад в итоговую оценку. Распределение весов было сформировано на основе эмпирического анализа частотности и последствия проявления признаков риска по ранее изученным кейсам [2; 3].

Расчёт ИРЦК осуществлялся по следующей формуле:

$$\text{ИРЦК} = \sum_{i=1}^{n} \omega_i \times x_i$$

где: Wi— вес критерия

xi— значение по шкале xi∈{0;0,5;1}

n — общее количество критериев

Применяемая шкала интерпретации значений ИРЦК:

- 0.0–0.3 — низкий уровень риска;
- 0.3–0.6 — средний риск (требует дополнительной проверки);
- 0.6–1.0 — высокий уровень риска, указывающий на необходимость отказа от взаимодействия либо ручной верификации.

Исследование ограничено числом эмпирических кейсов (n = 3), что не позволяет экстраполировать результаты на всю совокупность строительных организаций без дополнительных проверок [2]. Отбор кейсов осуществлялся целенаправленно и не предполагает репрезентативную выборку, однако позволяет выявить характерные паттерны цифрового риска на уровне типовых ситуаций [15].

Кроме того, в рамках настоящего анализа не учитывались платные или закрытые источники информации, включая банковские скоринговые модели, внутренние аналитические системы и отчёты коммерческих структур, специализирующихся на проверках благонадёжности, что, по мнению ряда исследователей, значительно расширяет контур достоверной оценки [13; 20]. Это может ограничивать полноту профиля и сужать границы применимости предложенной модели в сегментах с повышенной информационной доступностью [4; 13].

Также оценка производилась на основе полуструктурированной интервальной шкалы, основанной на экспертных допущениях. Несмотря на высокую практическую релевантность и подтверждение в прикладных исследованиях [3; 6], шкала требует дальнейшей статистической валидации и отраслевой адаптации, особенно при использовании в автоматизированных системах оценки рисков [3; 19].

Результаты

В целях эмпирической апробации разработанной методики были сформированы цифровые профили трёх строительных компаний — условно обозначенных как А, Б и В. Каждая из них была оценена по восьми ключевым критериям цифрового риска, согласно установленным весовым коэффициентам и интервальной шкале оценки [3; 9; 18]. Ниже представлен пример расчёта интегрального показателя цифрового риска (ИРЦК) для компании А (см. таблицу 1), соответствующего методике, разработанной с опорой на практику корпоративного мониторинга в сфере обеспечения экономической безопасности [2; 6].

Таблица 1. Пример расчёта ИРЦК: компания А

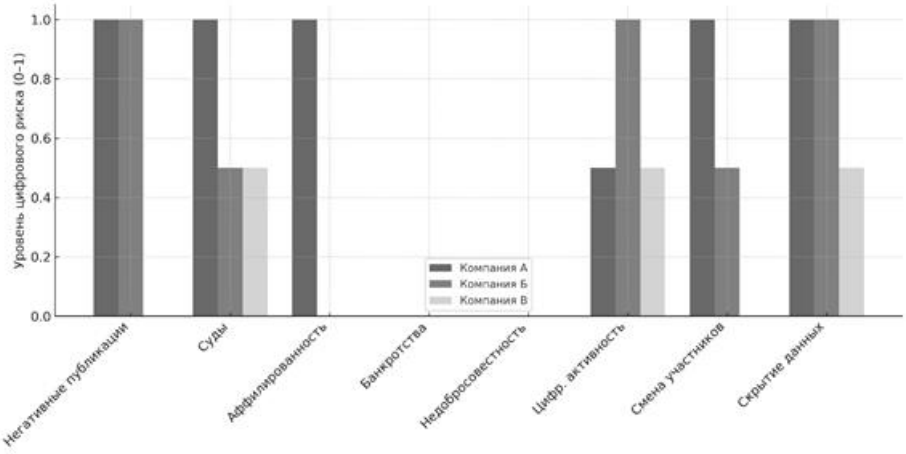
№	Критерий оценки	Вес (wi)	Оценка (xi)	wi × xi
1	Негативные публикации	0.15	1.0	0.15
2	Судебные разбирательства	0.15	1.0	0.15
3	Аффилированность	0.20	1.0	0.20
4	Участие в банкротствах	0.10	0.0	0.00
5	Недобросовестность	0.10	0.0	0.00
6	Аномальная цифровая активность	0.10	0.5	0.05
7	Смена учредителей и руководства	0.10	1.0	0.10
8	Слабая цифровая представленность / сайт	0.10	1.0	0.10
	Итоговый ИРЦК	1.00	—	0.75

Источник: составлено автором на основе данных кейс-анализа.

Таким образом, интегральный цифровой риск компании А составляет 0.75, что, согласно принятой шкале интерпретации [6; 18], соответствует высокому рисковому профилю. Это указывает на необходимость проведения углублённой верификации и анализа обстоятельств формирования негативного цифрового следа [13].

Аналогичные расчёты были произведены для компаний Б (ИРЦК = 0.475) и В (ИРЦК = 0.20), что позволило визуализировать рисковые профили по ключевым цифровым критериям (см. рис. 1).

- Компания Б демонстрирует средний уровень риска, обусловленный информационными аномалиями (всплески цифровой активности, упоминания в Telegram-каналах), при отсутствии формальных юридических нарушений [4; 19].
- Компания В, несмотря на отсутствие критических признаков, характеризуется низкой цифровой прозрачностью (ограниченное количество открытых данных, отсутствие публичной отчётности), что отражается в низком значении ИРЦК — типичном для добросовестных субъектов МСП в строительстве [15].



Источник: составлено автором на основе эмпирических данных исследования.

Рис. 1. Сравнение цифрового риска строительных компаний А, Б и В по ключевым критериям.

Анализ трёх эмпирических кейсов продемонстрировал различия в структуре цифрового следа при сопоставимых или контрастных уровнях итогового риска:

- **Компания А** характеризуется насыщенным цифровым фоном (упоминания, судебные споры, смена участников), при этом отсутствуют формальные признаки банкротства или связи с санкционными фигурантами. Тем не менее, совокупность факторов формирует устойчивый профиль высокого риска [13].
- **Компания Б** менее выражена в цифровом пространстве, но демонстрирует признаки участия в судебных процессах, слабую цифровую прозрачность и регистрацию по юридически аномальным адресам, что требует мониторинга и возможной ручной проверки [16].
- **Компания В** показывает профиль стабильного субъекта с низким уровнем риска: отсутствуют негативные сигналы, цифровой след сдержанный, структура стабильна [15; 6].

Сравнительный анализ подтверждает аналитическую пригодность предложенной модели и её чувствительность к различным проявлениям цифрового и структурного риска в корпоративной среде [3; 9]. Использование разрозненных показателей без системной агрегации может привести к искажению оценки, особенно в случаях с формально «чистыми» субъектами, обладающими скрытыми рисками. Применение модели ИРЦК позволяет формализовать процесс цифровой проверки и обоснованно сегментировать контрагентов по уровням риска [12; 17].

Обсуждение

Полученные в ходе исследования данные подтверждают высокую аналитическую значимость цифрового следа как индикатора благонадёжности контрагента. На примере трёх эмпирических кейсов (компании А, Б и В) показано, что объединение формально-юридических источников (Федресурс, ЕГРЮЛ, судебные базы) с цифровыми репутационными сигналами (СМИ, агрегаторы, Telegram-каналы и пр.) обеспечивает более полное и дифференцированное представление о рисковом профиле хозяйствующих субъектов [4; 13; 19].

Разработанный интегральный показатель цифрового риска (ИРЦК) продемонстрировал чувствительность к различным типам угроз — от репутационных до структурно-организационных [3; 9]. Примечательно, что компании с различной структурой цифрового поведения могут демонстрировать сопоставимый уровень агрегированного риска, что подчёркивает необходимость не только количественной оценки, но и содержательной интерпретации полученных результатов [15; 16].

В ходе анализа цифрового следа были зафиксированы типовые аномалии и индикаторы неблагонадёжности, в том числе:

- сокрытие существенной информации при формальной юридической «чистоте» контрагента;
- нестандартные цифровые паттерны (всплески активности, удаление контента), предшествующие корпоративным конфликтам;
- репутационное давление в медиапространстве, сопровождающее судебные процессы и банкротства [4; 13].

Таким образом, цифровой анализ усиливает традиционные процедуры due diligence и может рассматриваться как инструмент раннего предупреждения о рисках [17; 20].

Выдвинутая в начале исследования гипотеза о том, что анализ цифровых следов и реестровых данных позволяет повысить достоверность оценки контрагентов в системе корпоративной безопасности, получила эмпирическое подтверждение. Интеграция гетерогенных источников информации — как структурированных (реестры, базы данных), так и неструктурированных (открытые публикации, цифровые сигналы) — значительно расширяет возможности аналитика по выявлению нетипичных, скрытых и потенциально рисковых субъектов делового оборота [13; 19].

Модель ИРЦК позволяет не только формализовать процесс оценки цифрового поведения, но и обеспечить воспроизводимость процедур в рамках стандартов внутреннего контроля и корпоративного комплаенса, особенно в отраслях с высокой регуляторной нагрузкой (финансовый сектор, ТЭК, государственные закупки и др.) [18; 21].

Предложенная модель цифровой оценки рисков может быть интегрирована:

- в процедуры внутреннего контроля и корпоративного комплаенса [17; 21];
- в автоматизированные системы проверки (в том числе на базе концепции KYC (Know Your Customer — «Знай своего клиента») и risk-based подходов) [3; 20];
- в инструменты первичной и углублённой аналитики контрагентов [4; 18];
- в архитектуру корпоративной информационной безопасности как подсистему цифрового мониторинга [6; 19].

Наибольшую практическую значимость методика может иметь в секторах с повышенной чувствительностью к непрозрачным или токсичным субъектам: лизинговом, инвестиционном, страховом бизнесе, а также в проектах с государственным участием [13; 17]. Применение цифрового анализа позволяет снизить репутационные, правовые и имущественные риски, повысив устойчивость бизнес-процессов и уровень корпоративной ответственности [4; 6].

Для сопоставления предложенного подхода с международной практикой оценки деловых

партнёров целесообразно рассмотреть зарубежные модели digital KYC и digital compliance (цифровое обеспечение соответствия нормативным требованиям). В странах с развитой финансовой инфраструктурой (США, Великобритания, Сингапур) процедуры цифровой верификации опираются на стандартизированные источники, автоматизированную обработку публичных данных и скоринговые модели на базе алгоритмов машинного обучения. Компании используют интеграции с государственными и частными реестрами через API, а также осуществляют мониторинг цифровых рисков в режиме реального времени, включая поведенческие паттерны и аномалии в онлайн-активности [20; 21; 22].

В ряде юрисдикций применяется концепция perpetual KYC (постоянное KYC), предполагающая непрерывный мониторинг цифровой активности клиентов и контрагентов. Такие решения используют потоковую обработку данных из новостных агрегаторов, корпоративных отчётов, социальных сетей и цифровой репутации. Сравнение с российской практикой показывает, что несмотря на наличие сопоставимых источников (Федресурс, ЕГРЮЛ, ГАС «Правосудие»), уровень автоматизации и системной интеграции в отечественных компаниях пока остаётся ограниченным.

Предложенная в статье модель ИРЦК концептуально близка к зарубежным инструментам digital compliance, однако адаптирована к российским источникам информации и нормативно-правовой среде. Это создаёт потенциал как для внутреннего применения, так и трансграничной адаптации модели с учётом международных стандартов регулирования и оценки рисков — таких как FATF (Межправительственная группа разработки финансовых мер борьбы с отмыванием денег), AMLD (Антиотмывочная директива ЕС) и OFAC (Управление по контролю за иностранными активами Минфина США).

Несмотря на подтверждённую практическую применимость предложенной методики, исследование имеет ряд содержательных ограничений.

Во-первых, численность эмпирической выборки составляет три кейса, что не позволяет утверждать о статистической устойчивости выявленных закономерностей. Представленные кейсы демонстрируют типовые профили риска, однако выборка не является репрезентативной с точки зрения отраслевого и регионального охвата [2; 15].

Во-вторых, используемая модель оценки цифрового следа основана на интервальной шкале, полученной на основе экспертной калибровки и эмпирического анализа. Несмотря на более высокую гибкость по сравнению с бинарным подходом, она всё ещё не прошла формальную статистическую валидацию и не адаптирована к отраслевым спецификам в полном объёме [3; 6; 18].

Предложенная шкала оценки цифрового следа контрагента является авторским инструментом, разработанным на основе практического опыта специалистов в области корпоративной безопасности [9]. Распределение весов по критериям риска носит качественный характер и требует дополнительного подтверждения на более широкой выборке [2; 3].

Тем не менее, дальнейшее развитие методики видится в направлении количественной верификации весов с применением аналитических процедур — таких как метод анализа иерархий (AHP), регрессионное моделирование или байесовская классификация. Это позволит повысить объективность модели и расширить её применимость в различных

секторах [19; 22].

Кроме того, интервальная шкала может быть дополнена вероятностной компонентой, учитывающей не только наличие и выраженность признаков, но и их частотность и контекстуальную значимость в конкретной цифровой среде [4; 20].

- С учётом полученных результатов и выявленных ограничений, дальнейшее развитие заявленной научной темы представляется перспективным по следующим направлениям:
- Разработка программных решений на базе предложенной модели, включая создание автоматизированного скрипта или API-инструмента для расчёта ИРЦК с использованием открытых источников данных и агрегаторов реестровой информации. Потребность в интеграции цифрового анализа в корпоративную практику подчёркивается в исследованиях, посвящённых OSINT-инструментам и аналитическим платформам [19].
- Интеграция оценки цифрового следа в архитектуру корпоративных информационных систем, прежде всего ERP- и CRM-платформ, что позволит использовать модель ИРЦК в режиме предварительной фильтрации и текущего мониторинга контрагентов. Такая автоматизация соответствует трендам в области цифровой трансформации систем внутреннего контроля и оценки контрагентов [3; 18].
- Адаптация методики к отраслевой специфике с целью повышения точности и релевантности оценки, включая создание модифицированных шкал риска для финансовых организаций, участников государственного заказа, логистических компаний и проектно-подрядных структур. Отраслевая калибровка модели позволит учесть особенности цифровой активности, типичные для разных сегментов бизнеса [15; 6].
- Расширение модели за счёт цифровых поведенческих индикаторов, таких как стилистика публичной коммуникации, динамика публикационной активности, реактивность в цифровой среде, — с их последующим включением в составные индексы деловой репутации и финансовой устойчивости контрагента. Подобные подходы всё чаще применяются в международной практике оценки рисков и формирования комплаенс-инфраструктуры [20; 21].
- Реализация указанных направлений позволит повысить точность и воспроизводимость оценки, а также сформировать предпосылки для создания стандартизированных инструментов цифрового комплаенса в корпоративной практике [17; 21; 22].

Выводы

В результате проведённого исследования подтверждена гипотеза о том, что комплексный анализ цифровых следов и официальных реестровых данных позволяет существенно повысить эффективность процедур due diligence и служит действенным инструментом обеспечения корпоративной безопасности [4; 13; 17]. Объединение цифровых и юридически значимых источников информации обеспечивает многомерную оценку благонадёжности контрагента и позволяет выявлять скрытые риски, недоступные при использовании только классических методов проверки [6; 19].

Разработанный индекс цифрового риска контрагента (ИРЦК), основанный на шкале из восьми ключевых критериев, продемонстрировал применимость в прикладных задачах корпоративной аналитики [3; 9]. Модель показала чувствительность к различным типам угроз — репутационным, юридическим и организационным, — и может быть адаптирована для применения в различных отраслях и секторах экономики [15; 18].

Предложенный подход также обладает высоким потенциалом к интеграции в системы внутреннего контроля, комплаенса и цифровой безопасности [17; 21].

Практическая значимость результатов заключается в возможности их внедрения в регулярные процедуры проверки контрагентов, а также в автоматизированные системы поддержки управленческих решений [20; 21]. Методология применима в финансовом секторе, в лизинговых и страховых компаниях, в закупочной деятельности и в процессе предварительной инвестиционной оценки [13; 6]. Использование ИРЦК позволяет не только формализовать оценку, но и повысить прозрачность и воспроизводимость аналитических выводов [9].

В перспективе дальнейших исследований видится развитие методики в направлении статистической валидации шкалы, расширения выборки кейсов, перехода от бинарной к интервальной системе шкалирования рисков, а также построения программных решений, позволяющих реализовать анализ цифрового следа в полуавтоматическом режиме [3; 19]. Дополнительным направлением может стать адаптация модели к зарубежным юрисдикциям и стандартизация её использования в рамках корпоративных политик безопасности и управления рисками [22; 21].

Библиография

1. Безопасность предпринимательской деятельности: учебник для вузов / В. Л. Шульц [и др.] ; под ред. В. Л. Шульца. – 3-е изд., перераб. и доп. – М. : Юрайт, 2025. – 563 с. EDN: WWHFYN.
2. Шира Т., Салыга К., Дерий В., Приходько И., Шимкив С. Развитие корпоративной безопасности в контексте противодействия угрозам ведения бизнеса // Бизнес: теория и практика. – 2021. – Т. 22, № 1. – С. 211-221. – DOI: 10.3846/btp.2021.13396.
3. Na O., Park L. W., Yu H., Kim Y., Chang H. The rating model of corporate information for economic security activities // Security Journal. – 2019. – DOI: 10.1057/s41284-019-00171-z. EDN: IWDFWY.
4. Лезина Т. А., Хорошева Т. А., Коростелева А. В. Цифровой след как инструмент оценки компетенций: кейс компании "Газпром нефть" // ПроНефть. – 2021. – Т. 6, № 2. – С. 91-98. – DOI: 10.51890/2587-7399-2021-6-2-91-98. EDN: LZUHMO.
5. Зайнуллин С. Б. Корпоративная безопасность: учеб. пособие. – М. : РУДН, 2023. – 131 с. – ISBN 978-5-209-11755-1. EDN: EBUNDQ.
6. Панарина М. М. Основы корпоративной безопасности предприятия: монография. – М. : Ruscience, 2021. – 107 с. – ISBN 978-5-4365-6130-1.
7. Сиганьков А. А. Обеспечение финансово-экономической корпоративной безопасности: учеб.-метод. пособие. – М. : МИРЭА, 2024.
8. Михайлова У. В., Афанасьева М. В. Безопасность корпоративной инфраструктуры: практикум. – Магнитогорск : МГТУ им. Г. И. Носова, 2021. EDN: XYWXWV.
9. Стратымов А. В., Лебедев С. А. Финансовые расследования как системообразующий базис обеспечения экономической безопасности компании: монография. – Красноярск : СФУ, 2024. – 301 с.
10. Анискин Ю. П. Факторный анализ экономических показателей и оценка деловой активности компании: учеб.-метод. практикум. – М. : Ваш формат, 2025. – 200 с.
11. Криворотов В. В., Калина А. В., Ерыпалов С. Е., Левшенюк Р. В. Исследование и оценка конкурентоспособности компаний различной отраслевой направленности: монография. – М. : ЮНИТИ-ДАНА, 2023. – 363 с.
12. Иванов В. Ю. Тактическая операция "Осмотр электронно-цифровых следов":

монография. – Екатеринбург : УЮИ МВД России, 2023.
13. Гурбанов А. А. Современные особенности проверки добросовестности делового партнера // Отходы и ресурсы. – 2022. – Т. 9, № 4. – URL: https://resources.today/PDF/17ECOR422.pdf – DOI: 10.15862/17ECOR422. EDN: QPIONU.
14. Зотиков Н. З. Контрагент – надежный партнер или источник налогового риска // Вестник Евразийской науки. – 2021. – Т. 13, № 1. – URL: https://esj.today/PDF/30ECVN121.pdf. EDN: RHGVWY.
15. Позднякова Т. С. Анализ методов проверки контрагентов с целью обеспечения экономической безопасности АО "Арнест" // Вестник Евразийской науки. – 2021. – Т. 13, № 6. – URL: https://esj.today/PDF/77ECVN621.pdf. EDN: WSXOPM.
16. Бондарчук Н. В., Дорофеев Е. С. Проверка сведений о контрагентах как инструмент внутреннего контроля договорных отношений организации // МИРЭА – РТУ. – 2023. – DOI: 10.28995/2782-2222-2023-3-25-34. EDN: XZIXQA.
17. Попондопуло В. Ф., Петров Д. А. Комплаенс как система управления рисками в сфере предпринимательства // В кн.: Антимонопольный комплаенс как эффективный инструмент профилактики нарушений. – М. : Юрист, 2019. – С. 15-32. EDN: QQMPEN.
18. Панарина М. М. Корпоративная безопасность. Управление рисками и комплаенс в эпоху цифровизации: учеб. пособие. – 3-е изд. – М. : Юрайт, 2025. – 181 с. – ISBN 978-5-534-17777-0. – URL: https://urait.ru/bcode/559219 (дата обращения: 21.06.2025).
19. Мищиряков И. В., Шевелев А. Д., Макарчук Д. В. Исследование инструментов и методов для сбора и анализа открытой информации в сети Интернет (OSINT) // Вестник науки. – 2024. – Т. 3, № 6 (75). – С. 1414-1423. EDN: GHZWRM.
20. Biegelman M. T., Biegelman D. R. Building a World-Class Compliance Program: Best Practices and Strategies for Success. – Wiley, 2008. – 320 p. – ISBN 978-0-470-27840-6.
21. Fox T. The Compliance Handbook: A Guide to Operationalizing Your Compliance Program. – LexisNexis, 2021.
22. Pieth M. Duty to Report Suspicion? Risk for Personal Liability (Aiding and Abetting?) // In: Meier A., Oetiker C. (eds). Arbitration and Crime. – Alphen aan den Rijn : Wolters Kluwer, 2021. – P. 83-88.
23. Agrawal A., Gans J., Goldfarb A. From prediction to transformation // Harvard Business Review. – 2022. – Nov./Dec. – P. 100-109.
24. Астанин В. В. Корпоративный антикоррупционный комплаенс: проблемы и ресурсы практического обеспечения // Российская юстиция. – 2017. – № 10. – С. 5-8. EDN: ZHFCEL.
25. Единый государственный реестр юридических лиц (ЕГРЮЛ) и индивидуальных предпринимателей (ЕГРИП). Официальный сайт ФНС России. – URL: https://egrul.nalog.ru/ (дата обращения: 21.06.2025).
26. Единый федеральный реестр сведений о банкротстве (Федресурс). – URL: https://fedresurs.ru/ (дата обращения: 21.06.2025).
27. Единая информационная система в сфере закупок. – URL: https://zakupki.gov.ru/ (дата обращения: 21.06.2025).
28. Государственная автоматизированная система "Правосудие". – URL: https://sudrf.ru/ (дата обращения: 21.06.2025); Картотека арбитражных дел (КАД "Арбитр"). – URL: https://kad.arbitr.ru/ (дата обращения: 21.06.2025).
29. СПАРК-Интерфакс. – URL: https://spark-interfax.ru/ (дата обращения: 21.06.2025); Контур.Фокус. – URL: https://focus.kontur.ru/ (дата обращения: 21.06.2025); RuData. – URL: https://rudata.ru/ (дата обращения: 21.06.2025); ЗаЧестныйБизнес. – URL: https://zachestnyibiznes.ru/ (дата обращения: 21.06.2025).
30. Yandex.News. – URL: https://news.yandex.ru/ (дата обращения: 21.06.2025); Google Alerts. – URL: https://www.google.ru/alerts (дата обращения: 21.06.2025); TgStat. – URL:

https://tgstat.ru/ (дата обращения: 21.06.2025).

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования в рецензируемой статье выступает система инструментов анализа цифровых и реестровых данных, применимых в рамках корпоративной проверки контрагентов.
Методология исследования базируется на применении методов контент-анализа, case-study и сравнительной оценки материалов публичных источников и кейсов из корпоративной практики.
Актуальность работы авторы связывают с необходимостью обеспечения экономической безопасности внутри крупных корпораций и противодействия угрозам в условиях цифровизации экономики, когда распространение теневых финансовых схем снижает эффективность классических методов проверки благонадёжности партнёров, и на первый план выходит анализ цифровых следов: информационных фрагментов, оставляемых субъектами хозяйственной деятельности в публичных источниках, цифровых реестрах и информационном пространстве.
Научная новизна исследования состоит в обосновании методического подхода, позволяющего на основе анализа цифрового следа формировать целостную оценку рисков, ассоциированных с конкретным хозяйствующим субъектом.
Структурно в публикации выделены следующие разделы: Введение, Основная часть, включающая 3 подраздела: Методы, Результаты, Обсуждение, а также Выводы и Библиография.
В статье говорится о необходимости использования таких новых источников информации, как базы данных арбитражной и уголовной практики, сведения из Федресурса и ЕГРЮЛ, информация о банкротствах, об аффилированности, публичных контрактах, а также сигналы из СМИ, социальных сетей и специализированных каналов в мессенджерах для обеспечения корпоративной безопасности. Авторами разработан интегральный показатель цифрового риска, представляющий собой взвешенную сумму значений по ряду ключевых критериев, в публикации приведены формула расчета и пример вычисления этого показателя; проведено сравнение цифрового риска двух строительных компаний по ключевым критериям.
Библиографический список включает 30 источников – учебные и научные публикации по теме статьи на русском и иностранных языках в российских и международных журналах, а также интернет-источники, на которые в тексте имеются адресные ссылки, подтверждающие наличие апелляции к оппонентам.
К достоинствам работы можно отнести наличие четких формулировок цели исследования, научной новизны и практической значимости полученных результатов, использование графических способов подачи материала, изложение перспективе дальнейших исследований.
Из недостатков следует отметить, что из раздела «Библиография» следует исключить учебные издания (см. пп. 1, 5, 7, 8, 10 в списке литературы) и интернет-источники (пп. 25-30), расположив их в тексте статьи в скобках, наряду с прочими комментариями и примечаниями авторов, как это предусмотрено принятыми редакцией Правилами оформления списка литературы.
Рецензируемый материал соответствует направлению журнала «Финансы и управление», может вызвать интерес у читателей, рекомендуется к опубликованию после внесения

корректив в оформление библиографии.