Международный научно-исследовательский журнал
«Прогрессивная экономика»
№ 7 / 2026 https://progressive-economy.ru/vypusk_1/matematicheskaya-model-obyasnimogo-risk-ranzhirovaniya-operaczij-malogo-predpriyatiya-dlya-rannego-vyyavleniya-priznakov-moshennichestva/
Научная статья / Original article
Шифр научной специальности ВАК: 5.2.3
УДК 330.4:657.6:005.334
DOI: 10.54861/27131211_2026_7_169

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОБЪЯСНИМОГО РИСК-РАНЖИРОВАНИЯ ОПЕРАЦИЙ МАЛОГО ПРЕДПРИЯТИЯ ДЛЯ РАННЕГО ВЫЯВЛЕНИЯ ПРИЗНАКОВ МОШЕННИЧЕСТВА

Шумилин А.А., *бакалавр, Российский экономический университет имени Г.В. Плеханова, Москва, Россия*
115054, г. Москва, Стремянный переулок, д. 36
ORCID: https://orcid.org/0009-0005-0809-4456

Ладогина А.Ю., *доцент, Российский экономический университет имени Г.В. Плеханова, Москва, Россия*
115054, г. Москва, Стремянный переулок, д. 36
ORCID: https://orcid.org/0000-0003-2890-6739

Нефедов Ю.В., *доцент, Российский экономический университет имени Г.В. Плеханова, Москва, Россия*
115054, г. Москва, Стремянный переулок, д. 36
ORCID: https://orcid.org/0000-0002-9772-2629

Аннотация. Цель исследования – разработать и апробировать математическую модель объяснимого риск-ранжирования операций малого предприятия для раннего выявления признаков мошенничества при ограниченности контрольных ресурсов и отсутствии размеченной базы инцидентов. В статье на основе теоретико-эмпирического анализа предложена математическая модель объяснимого риск-ранжирования операций малого предприятия для раннего выявления признаков мошенничества в условиях ограниченности контрольных ресурсов и отсутствия размеченной базы подтверждённых инцидентов. Научная новизна полученных результатов заключается в разработке математической модели объяснимого риск-ранжирования операций малого предприятия, объединяющей регламентные нарушения, робастные статистические отклонения и аномальные процессные сочетания признаков в единую оценку приоритета проверки. На основе интеграции теоретических подходов предложена гибридная модель, объединяющая регламентные правила, робастный риск-скоринг и метод Isolation Forest в единую оценку

приоритета проверки. Апробация модели выполнена на открытом объектно-центрическом журнале событий Procure-To-Payment в формате OCEL 2.0. Сделан вывод о том, что модель может использоваться как инструмент формирования объяснимой очереди риск-проверки, не подменяющий экспертную оценку и не трактующий аномалию как доказанный факт мошенничества.

Ключевые слова: малое предприятие, корпоративное мошенничество, риск-ранжирование, математическая модель, внутренний контроль, process mining, объектно-центрический журнал событий, анализ аномалий.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Шумилин А.А., Ладогина А.Ю., Нефедов Ю.В. Математическая модель объяснимого риск-ранжирования операций малого предприятия для раннего выявления признаков мошенничества // Прогрессивная экономика. 2026. № 7. С. 169–189. https://doi.org/10.54861/27131211_2026_7_169.

Статья поступила в редакцию: 26.05.2026 г. Одобрена после рецензирования: 09.07.2026 г. Принята к публикации: 14.07.2026 г.

MATHEMATICAL MODEL FOR EXPLAINABLE RISK RANKING OF SMALL ENTERPRISE OPERATIONS FOR THE EARLY DETECTION OF FRAUD INDICATORS

Shumilin A.A., *Bachelor, Plekhanov Russian University of Economics, Moscow, Russia*
115054, Moscow, Stremyanny Lane, 36
ORCID: https://orcid.org/0009-0005-0809-4456

Ladogina A.Y., *Associate Professor, Plekhanov Russian University of Economics, Moscow, Russia*
115054, Moscow, Stremyanny Lane, 36
ORCID: https://orcid.org/0000-0003-2890-6739

Nefedov Yu.V., *Associate Professor, Plekhanov Russian University of Economics, Moscow, Russia*
115054, Moscow, Stremyanny Lane, 36
ORCID: https://orcid.org/0000-0002-9772-2629

Abstract. The purpose of the study is to develop and test a mathematical model of explicable risk ranking of small business operations for early detection of signs of fraud with limited control resources and the absence of a marked incident database. Based on theoretical and empirical analysis, the article proposes a mathematical model of explicable risk ranking of small business operations for early detection of signs of fraud in conditions of limited control resources and the absence of a marked database of confirmed incidents. The scientific novelty of the results

obtained lies in the development of a mathematical model of explicable risk-ranking of small business operations, combining regulatory violations, robust statistical deviations and abnormal process combinations of features into a single assessment of the priority of verification. Based on the integration of theoretical approaches, a hybrid model is proposed that combines regulatory rules, robust risk scoring and the Isolation Forest method into a single assessment of the verification priority. The model was tested on an open object-centric Procure-To-Payment event log in OCEL 2.0 format. It is concluded that the model can be used as a tool for forming an explicable risk check queue that does not replace expert assessment and does not treat an anomaly as a proven fact of fraud.

Keywords: small enterprise, corporate fraud, risk ranking, mathematical model, internal control, process mining, object-centric event log, anomaly detection.

JEL classification: M42, C63, C38.

Conflict of interest. The authors declare that there is no Conflict of Interests.

For citation: Shumilin A.A., Ladogina A.Yu., Nefedov Yu.V. (2026). Matematicheskaya model' ob"yasnimogo risk-ranzhirovaniya operatsii malogo predpriyatiya dlya rannego vyyavleniya priznakov moshennichestva [Mathematical model for explainable risk ranking of small enterprise operations for the early detection of fraud indicators]. Progressivnaya ekonomika [Progressive Economy], 7, 169–189. https://doi.org/10.54861/27131211_2026_7_169. (In Russ., abstract in Eng.)

The article was submitted to the editorial office: 26/05/2026. Approved after review: 09/07/2026. Accepted for publication: 14/07/2026.

Введение

Современный этап цифровизации хозяйственной деятельности характеризуется ростом объема учетных данных, электронных согласований и транзакционных событий, фиксируемых в бухгалтерских, ERP-, CRM- и иных информационных системах. Процесс цифровизации сопровождается изменением подходов к внутреннему контролю: контрольные процедуры все чаще должны опираться не только на последующую проверку документов, но и на анализ фактического хода бизнес-процессов, поведения участников процесса и данных внутренних информационных систем [4; 7; 16]. При этом для закупочно-платежных операций особое значение приобретает учет связей между несколькими объектами процесса – заявкой, заказом, счетом, поступлением и платежом [11; 12]. Необходимо учитывать регламентные требования, качество признакового описания, исторический контекст операции, а также возможность применения process mining для анализа отклонений от нормативного процесса и методов анализа аномалий для выявления нетипичных действий [9; 10; 14; 16].

Особую значимость в этом контексте приобретает задача раннего выявления признаков мошенничества в малом бизнесе. Малые предприятия, как правило, располагают ограниченными финансовыми, кадровыми и организационными ресурсами, а система внутреннего контроля в них требует

адаптации к менее формализованным процедурам, совмещению функций и высокой роли руководителя [3; 6]. При этом риск мошеннических действий сохраняет высокую практическую значимость: профессиональное мошенничество приводит к существенным потерям организаций, а внутренние злоупотребления могут выражаться в присвоении активов, коррупционных действиях, искажении отчетности, сговоре с контрагентами, хищении имущества и иных нарушениях [1; 2; 8].

Актуальность исследования обусловлена несколькими факторами. Во-первых, малые предприятия часто не располагают достаточными ресурсами и экспертизой для внедрения сложных антифрод-процедур [15], а отсутствие репрезентативной базы подтвержденных fraud-инцидентов затрудняет применение классических моделей машинного обучения с учителем [14]. Во-вторых, использование только формальных red flag-признаков без учета процессного контекста повышает риск ложных срабатываний, поскольку сам по себе red flag является лишь индикатором необычного поведения, а не доказательством мошенничества [9]. В-третьих, для практического применения требуется не автоматическое установление факта мошенничества, а объяснимое риск-ранжирование операций, позволяющее сформировать очередь экспертной проверки и показать причины повышения риск-приоритета [18; 21]. Цель исследования – разработать и апробировать математическую модель объяснимого риск-ранжирования операций малого предприятия для раннего выявления признаков мошенничества при ограниченности контрольных ресурсов и отсутствии размеченной базы инцидентов.

Обзор литературы

Теоретическое осмысление проблемы раннего выявления признаков мошенничества опирается на несколько групп исследований. В отечественных работах внутренний контроль рассматривается как инструмент предупреждения корпоративного мошенничества и выявления искажений в учетной информации [1; 2; 5], а для малого бизнеса подчеркивается необходимость адаптации контрольных процедур к ограниченным ресурсам и менее формализованной организационной структуре [3; 6]. Связь контроля с процессной аналитикой раскрывается в исследованиях process mining, где анализ фактического хода бизнес-процессов рассматривается как инструмент мониторинга, выявления отклонений и сопоставления наблюдаемого поведения с моделью процесса [4; 7].

Зарубежные источники показывают, что профессиональное мошенничество остается значимым источником потерь организаций [8], а применение red flag-подхода без учета процессного контекста может приводить к значительному числу ложноположительных срабатываний [9]. Поэтому современные исследования акцентируют внимание на подготовке данных, исторических агрегатах и признаках нетипичного поведения [10], а

также на анализе связанных объектов закупочно-платежного процесса [11–13]. Методологическую основу составляют работы по анализу аномалий [14], fraud-рискам и employee fraud в малом бизнесе [15; 20], непрерывному аудиту и применению process mining в контрольных процедурах [16]. Значимы исследования аномалий в журналах бизнес-процессов [17], объяснимого выявления аномалий [18], метода Isolation Forest [19] и explainable occupational fraud detection [21]. Вместе с тем недостаточно раскрыт вопрос модели, применимой для малого предприятия, не требующей размеченной базы fraud-инцидентов и формирующей не бинарный вывод о мошенничестве, а объяснимую очередь риск-проверки.

Материалы и методы

Теоретико-методологическая база исследования сформирована на пересечении трех групп источников: работ по внутреннему контролю и предупреждению корпоративного мошенничества, исследований по process mining и объектно-центрическим журналам событий, а также публикаций по статистическому выявлению аномалий. Внутренний контроль рассматривается как исходная управленческая рамка, поскольку он задает регламенты, контрольные процедуры, разграничение полномочий, проверку документов и мониторинг подозрительной активности [1; 2; 5]. Для малого предприятия важно, что контроль не может строиться по модели крупной компании: его организация должна учитывать масштаб деятельности, сложность организационной структуры, финансовую состоятельность, человеческий фактор и соотношение затрат и выгод от контрольных процедур [3; 6]. Поэтому хозяйственная операция трактуется не как изолированная бухгалтерская запись, а как элемент бизнес-процесса, по которому можно сформировать проверяемый набор риск-признаков.

Второй методический блок связан с процессной аналитикой. В работах по fraud detection подчеркивается, что классический red flag-подход часто порождает ложные срабатывания, если признаки рассматриваются вне фактического маршрута операции [9]. Исследования по data engineering для антифрода показывают, что качество признакового описания и учет исторического контекста являются не менее важными, чем выбор алгоритма [10]. В связи с этим анализируется не только наличие формального нарушения, но и фактический маршрут операции: последовательность действий, временные характеристики этапов и участие субъектов процесса, фиксируемые в журнале событий [4; 7; 16].

Эмпирическую базу исследования составил открытый объектно-центрический журнал событий Procure-To-Payment (P2P) в формате OCEL 2.0 [13]. Выбор данного набора данных обусловлен тем, что реальные ERP-данные малого бизнеса с разметкой мошеннических инцидентов, как правило, недоступны из-за коммерческой тайны, персональных данных и риска раскрытия внутренних контрольных процедур. P2P-датасет воспроизводит

закупочно-платежный процесс от возникновения потребности в закупке до исполнения платежа и построен на реалистичных SAP-транзакциях. Журнал содержит 14 671 событие, 9 543 объекта, 10 типов событий и 7 типов объектов. В нем отражены записи о создании и согласовании заявки на закупку, запросе и получении коммерческого предложения, создании и согласовании заказа, поступлении товаров, регистрации счета, трехсторонней сверке заказа, поступления и счета, а также исполнении платежа. В набор включены специальные поведенческие сценарии: maverick buying, duplicate payments и lengthy approval process [13].

Использование формата OCEL 2.0 имеет самостоятельное методическое значение. В традиционном case-centric журнале событие обычно привязано к одному идентификатору случая, тогда как закупочно-платежная операция одновременно связана с несколькими объектами: заявкой, заказом, счетом, поступлением, платежом, материалом, поставщиком или иным участником процесса. Объектно-центрический формат позволяет сохранять связи «событие – объект» и «объект – объект», фиксировать временные метки, типы действий и атрибуты объектов без искусственного сведения процесса к одному идентификатору случая [11; 12; 13]. Это важно для выявления ситуаций, которые не выглядят рискованными в отдельной записи, но становятся подозрительными при анализе цепочки связанных событий.

Методика исследования включала несколько последовательных этапов. На первом этапе был выполнен теоретико-эмпирический анализ источников и выделены группы риск-сигналов, применимые к малому предприятию: регламентные нарушения, статистические отклонения, аномальные сочетания признаков и процессные несоответствия. На втором этапе данные журнала были приведены к единому аналитическому представлению: для событий учитывались время, тип действия, участник, связанный объект, статус, числовой параметр, а также связи с предшествующими и последующими событиями. На третьем этапе операция формализовалась как объект риск-анализа, включающий транзакционные, процессные, временные и историко-агрегированные признаки: сумму и тип операции, число связанных документов, ручные корректировки, изменение реквизитов, прохождение обязательных этапов, длительность маршрута, активность пользователя и отклонение от типичного профиля сотрудника, контрагента или временного окна.

На аналитическом уровне применялись системный анализ, сравнительный анализ источников, формализация признаков, методы робастной статистической обработки, объектно-центрический process mining и методы выявления аномалий без учителя. Такой выбор связан с тем, что в условиях малого предприятия часто ограничены ресурсы и экспертиза для построения сложной антифрод-системы [15], а для обучения классического бинарного классификатора требуется точная и репрезентативная разметка

нормальных и аномальных случаев, получение которой в задачах выявления аномалий является существенной проблемой [14]. Поэтому результат исследования интерпретируется не как автоматическое установление факта мошенничества, а как формирование объяснимой очереди операций для экспертной проверки. Для оценки применимости подхода использовались критерии воспроизводимости обработки журнала, полноты восстановления процессного контекста, трассируемости причин риск-срабатывания и соответствия выявляемых признаков сценариям P2P-датасета. Объяснимость результата обеспечивается тем, что каждая операция должна сопровождаться указанием группы риск-факторов: нарушенное правило, статистическое отклонение, нетипичная комбинация признаков или процессное отклонение. Для внутреннего контроля малого предприятия такая интерпретация принципиальна, поскольку проверяющий должен понимать, почему операция была отнесена к REVIEW или INCIDENT, и какие документы, действия или участников процесса необходимо проверить в первую очередь [18; 21].

Результаты и обсуждение

Систематизация исследованных источников показывает, что внутреннее мошенничество следует рассматривать не только как юридический факт, устанавливаемый по итогам расследования, но и как управленческий риск, проявляющийся в отклонениях хозяйственных операций, нарушении контрольных процедур и нетипичном поведении участников бизнес-процесса. В исследовании Е.И. Афанасовой подчеркивается, что риску мошеннических действий подвержены предприятия разного масштаба, при этом собственники часто концентрируются на внешних угрозах и недооценивают внутренние источники потерь: сговор сотрудника с контрагентом, хищение имущества, утечку информации, завышение расходов или обход установленных процедур [1]. В международной терминологии такие действия относятся к occupational fraud – использованию служебного положения для личного обогащения через намеренное злоупотребление ресурсами или активами организации [8].

В работе Е.И. Афанасовой приводятся результаты опросов, согласно которым более половины компаний России и СНГ в 2019–2020 гг. сталкивались с фактами корпоративного мошенничества, а доля российских респондентов, сообщавших о таких случаях, по данным PwC, выросла с 48 % в 2016 г. до 66 % в 2018 г. [1]. Более поздние международные оценки ACFE также показывают устойчивую значимость проблемы: по данным Occupational Fraud 2026: A Report to the Nations, организации ежегодно теряют около 5 % выручки из-за профессионального мошенничества, медианный ущерб по одному случаю составил 104 тыс. долл., средний ущерб – 1,457 млн долл., а типичный случай длился около 12 месяцев до выявления [8]. Там же указано, что 20 % кейсов превышали 1 млн долл. ущерба, а 43 % случаев были выявлены через сообщения информаторов.

С точки зрения внутреннего контроля принципиально важно, что мошенничество редко проявляется как одно очевидное нарушение. Чаще оно складывается из цепочки внешне допустимых действий: создание заявки вне стандартного маршрута, ускоренное согласование счета, ручная корректировка реквизитов, повторная оплата, дробление суммы, проведение операции в нетипичное время или использование доступа сотрудника для обхода процедуры. Воюцкая, Коське и Мишучкова выделяют две базовые группы мошенничества в бухгалтерском учете: преднамеренное искажение финансовых данных и незаконное присвоение активов; дополнительно в структуре профессионального мошенничества существенное место занимают коррупционные действия, нарушения с наличными и безналичными платежами, подделка документов и кража финансовой информации [2]. Поэтому предметом анализа в настоящем исследовании становится не только отдельная бухгалтерская запись, но и операция как часть связанного бизнес-процесса.

Для малого предприятия проблема усиливается спецификой организации контроля. В отличие от крупных компаний, малый бизнес часто не имеет отдельной службы внутреннего аудита или специализированного подразделения внутреннего контроля, а функции проверки распределяются между руководителем, финансовым подразделением или внешними контролерами. В исследовании В.М. Кожанова отмечается, что система внутреннего контроля в малом бизнесе имеет особенности по сравнению с крупными организациями, а традиционные концепции требуют адаптации к ограниченному штату, менее формализованным процедурам и высокой роли руководителя [3]. Исследование R. Othman и R. Ameer, выполненное на основе 18 судебных документов о мошенничестве сотрудников в малых предприятиях, показывает, что риск employee fraud возрастает там, где доверенные сотрудники совмещают несколько функций, обладают широким доступом к онлайн- и учетным системам, занимают позицию, позволяющую инициировать или изменять операции, и способны использовать слабости billing, accounts payable и payroll-процессов [20].

Следовательно, для малого предприятия нецелесообразно строить антифрод-контроль как самостоятельную тяжелую систему, требующую полной перестройки учета. Более рациональным является подход, при котором математическая модель накладывается поверх существующего учетного или процессного контура: бухгалтерской системы, ERP, CRM, BPM-системы, сервиса согласования заявок или журнала событий. Такая модель не заменяет первичные документы и не принимает юридически значимое решение о наличии мошенничества. Ее задача состоит в другом: агрегировать риск-сигналы, ранжировать операции по приоритету проверки и объяснять, почему конкретная операция должна быть поднята выше в очереди контроля.

Таблица 1

Основные виды внутренних мошеннических действий и признаки для риск-ранжирования

Table 1

The main types of internal fraudulent activities and risk-ranking criteria

Группа мошенничества	Типовые проявления	Признаки, значимые для риск-ранжирования
Коррупционные схемы	выбор аффилированного поставщика, завышение цены, неформальное вознаграждение	повторяемость контрагента, отклонение цены, обход согласования, участие одного сотрудника в нескольких этапах
Конфликт интересов в закупках и продажах	сделки со связанным контрагентом, нетипичные условия, необоснованные скидки	новый или нетипичный контрагент, резкое изменение условий, высокая концентрация операций
Хищение денежных средств	сокрытие выручки, неучтенные поступления, списание денежных средств	расхождение продаж и поступлений, операции без документа, частые корректировки
Незаконное присвоение запасов и иных активов	несанкционированное использование активов, фиктивное перемещение запасов, ложная отгрузка, списание или хищение имущества	расхождение закупки, склада и отгрузки; частые списания; отсутствие связанного события; нетипичное перемещение активов
Мошенничество с финансовой отчетностью	завышение доходов, перенос расходов, сокрытие обязательств, занижение расходов, завышение или занижение оценки активов	операции на границе периода, ручные корректировки, резкие отклонения от исторического профиля, несоответствие первичных документов и отчетных показателей
Мошеннические выплаты	фиктивный поставщик, повторная оплата, личные расходы, завышенные компенсации, подделка или изменение платежных документов	дубли счетов, совпадение сумм и реквизитов, смена реквизитов, отсутствие подтверждений, нетипичный маршрут согласования

Источник: составлено авторами по данным ACFE [8]
Source: compiled by the authors based on ACFE [8]

Практическая реализация такого подхода требует предварительного описания ключевых бизнес-процессов и контрольных точек предприятия, поскольку система внутреннего контроля в малом бизнесе включает субъект и объект контроля, учетные системы, средства контроля, контрольную среду и временные рамки контрольных процедур [6]. Наиболее значимыми, для риск-ранжирования являются участки, связанные с закупками, платежами,

согласованием счетов, изменением платежных реквизитов, выбором поставщиков и операциями с контрагентами, поскольку именно закупочно-платежный контур позволяет восстановить последовательность событий и связи между заявкой, заказом, счетом, поступлением и оплатой [11]. На этом этапе формируется перечень событий, документов и действий, которые должны быть доступны для анализа: создание заявки, согласование заказа, регистрация счета, поступление товаров, изменение реквизитов, проведение платежа и закрытие операции.

Далее на основе этих данных определяется каталог регламентных правил и набор статистических признаков. Регламентные правила фиксируют обязательные контрольные требования: наличие согласования, соответствие связанных документов, отсутствие дублирующих платежей, соблюдение маршрута и разделение функций между участниками процесса. Статистические признаки позволяют оценить, насколько операция отличается от типичного поведения сотрудника, контрагента, категории расходов или временного окна; при этом качество признакового описания и учет исторического контекста являются ключевыми условиями применимости антифрод-модели [10]. Такая подготовка обеспечивает связь математической модели с реальными процедурами внутреннего контроля и делает результат интерпретируемым для проверяющего, что соответствует общей логике объяснимого выявления аномалий и occupational fraud detection [18; 21].

Если классические процедуры внутреннего контроля отвечают преимущественно на вопрос о наличии конкретного нарушения, то риск-ранжирование решает более широкую задачу: определить, какие операции требуют первоочередного внимания проверяющего с учетом совокупности регламентных, статистических, процессных и аномальных признаков. Такой подход особенно важен для малого предприятия, где ручная проверка всего потока операций экономически нецелесообразна, а достаточная база подтвержденных fraud-инцидентов для обучения бинарного классификатора, как правило, отсутствует. Поэтому результатом модели должен быть не вывод «мошенничество / не мошенничество», а объяснимая оценка риск-приоритета операции.

В исследовательской литературе можно выделить несколько подходов к выявлению подозрительных операций. Первый подход основан на заранее заданных признаках и контрольных правилах: превышение лимита, отсутствие согласования, несовпадение суммы счета и платежа, дублирование документа, нарушение разделения полномочий. Его достоинством является высокая объяснимость, однако такие правила выявляют только уже известные типы отклонений. Второй подход связан со статистическим анализом и сравнением операции с историческим профилем: по сумме, частоте, длительности маршрута, поведению сотрудника или контрагента. Он позволяет выявлять нетипичные операции, но требует устойчивых

исторических данных. Третий подход представлен методами анализа аномалий, которые позволяют выявлять события, операции или последовательности действий, отклоняющиеся от ожидаемого поведения. Для журналов бизнес-процессов особенно важно учитывать не только отдельное значение поля, но и уровень события, уровень case/trace, последовательность действий, временные, организационные и data-flow признаки; при отсутствии размеченной выборки для этого могут применяться методы без учителя [14; 17]. Наконец, process mining позволяет анализировать не только отдельный документ, но и фактическую последовательность событий в бизнес-процессе, что важно для снижения ложных срабатываний при использовании классических red flag-признаков [9; 16].

Дополнительное значение имеет подготовка признакового пространства. В работах по data engineering для fraud detection подчеркивается, что качество признаков, учет исторического контекста и корректная агрегация данных часто оказываются не менее значимыми, чем выбор конкретного алгоритма [10]. Для малого предприятия это особенно важно, поскольку один и тот же факт хозяйственной жизни может быть представлен в разных учетных объектах: заявке, счете, заказе, поступлении, платеже, записи о согласовании или событии изменения документа [11–13]. Следовательно, модель должна учитывать не только значение отдельного поля, но и положение операции в связанном процессе.

С учетом этих ограничений предложенная модель строится как гибридная. Ее логика состоит в объединении трех типов риск-сигналов: регламентного, статистического и аномального. Регламентный компонент обеспечивает связь модели с процедурами внутреннего контроля; статистический компонент выявляет отклонения от типичного профиля; аномальный компонент фиксирует нетипичные сочетания признаков, которые не обязательно нарушают отдельное правило, но отличаются от общей структуры потока операций. Такое сочетание позволяет сохранить объяснимость результата и одновременно расширить область выявляемых подозрительных ситуаций.

Внутренняя модель операции строится как структурированный объект:

$$o_i = (id_i, t_i, u_i, c_i, a_i, d_i, s_i, h_i), \quad (1)$$

где id_i – идентификатор операции, t_i – время события, u_i – участник процесса, c_i – контрагент или связанный субъект, a_i – сумма или иной числовой параметр, d_i – тип действия или документа, s_i – статус, h_i – история изменений и согласований. После нормализации операция дополняется контекстом C_i: связанными объектами, соседними событиями и агрегатами по сотруднику, контрагенту и временному окну.

Для анализа операция переводится в вектор признаков:

$$x_i = \varphi(o_i, C_i), \tag{2}$$

Вектор включает четыре группы признаков: транзакционные, процессные, временные и историко-агрегированные. К ним относятся сумма и тип операции, число связанных документов, ручные корректировки, изменение реквизитов, прохождение обязательных этапов, длительность маршрута, активность пользователя и отклонение суммы или длительности от типичного профиля.

Первый компонент модели - регламентный риск. Пусть $G = g_1, \dots, g_m$ - множество правил, где каждое правило возвращает 1 при нарушении и 0 при отсутствии нарушения. Тогда нормированная оценка rule-based риска задается выражением:

$$R_{\text{rule}}(o_i) = \frac{\sum_{j=1}^{m} \beta_j \, g_j(o_i)}{\sum_{j=1}^{m} \beta_j}, \tag{3}$$

где β_j – вес критичности j-го правила. В начальной конфигурации модели используются проверки обязательных полей, последовательности этапов, наличия согласования, соответствия суммы платежа сумме счета и признаков дублирующей оплаты. Весовая схема позволяет различать второстепенные ошибки и критичные нарушения.

Второй компонент – робастный риск-скоринг. Для k-го числового признака вычисляется робастное отклонение от исторического профиля:

$$z_{ik} = \frac{|x_{ik} - \text{median}_k|}{1.4826 \cdot \text{MAD}_k + \varepsilon}, \tag{4}$$

где μ_k – медиана признака по исторической базе, MAD_k – медианное абсолютное отклонение, ε – малое число для исключения деления на ноль. Множитель 1.4826 сопоставляет MAD со стандартным отклонением при нормальном распределении.

$$r_{ik} = \min\left(1, \frac{z_{ik}}{\theta_k}\right), \tag{5}$$

где θ_k – порог чувствительности.

Интегральный скоринговый риск имеет вид:

$$R_{\text{score}}(o_i) = \frac{\sum_{k=1}^{p} \alpha_k \, r_{ik}}{\sum_{k=1}^{p} \alpha_k}, \quad (6)$$

Третий компонент – аномальный скор $A(o_i)$, рассчитанный методом Isolation Forest [19]. В теоретическом виде аномальность связана со средней длиной пути изоляции объекта в ансамбле деревьев:

$$A(o_i) = 2^{-\frac{E(h(x_i))}{c(n)}}, \quad (7)$$

Чем быстрее объект отделяется случайными разбиениями, тем короче его средняя длина пути и тем выше значение аномального скора. В реализации значение нормируется на интервал от 0 до 1 и используется только как дополнительный компонент риска [19].

Итоговая оценка риска операции объединяет три компонента:

$$R(o_i) = \lambda_{rule} * R_{rule}(o_i) + \lambda_{score} * R_{score}(o_i) + \lambda_{anom} * A(o_i), \quad (8)$$

где $\lambda_{rule} + \lambda_{score} + \lambda_{anom} = 1$. В начальной конфигурации веса задаются экспертно, а после накопления обратной связи могут уточняться: вклад компонента повышается при устойчивом совпадении с оценкой проверяющего и снижается при частых ложных срабатываниях.

Класс операции определяется двумя порогами:

$$\mathrm{D}(\mathrm{o_i}) = \begin{cases} 0, \ \mathrm{R}(\mathrm{o}_i) < \tau_1, \\ 1, \ \tau_1 \leq \mathrm{R}(\mathrm{o}_i) < \tau_2, , \\ 2, \ \mathrm{R}(\mathrm{o}_i) \geq \tau_2, \end{cases} \quad (9)$$

где 0 соответствует классу NORMAL, 1 – классу REVIEW, 2 – классу INCIDENT; τ_1 и τ_2 – пороговые значения риск-приоритета. Промежуточный класс REVIEW принципиален для малого бизнеса: система не блокирует все неоднозначные операции, а поднимает их в очереди проверки. Это снижает нагрузку на сотрудника и сохраняет управляемость процесса.

Апробация предложенной модели выполнена на объектно-центрическом журнале событий Procure-To-Payment в формате OCEL 2.0, включающем встроенные сценарии отклоняющегося поведения: maverick buying, duplicate payments и lengthy approval process [13]. Для оценки качества риск-ранжирования указанные сценарии были использованы как контрольная сценарная разметка: операции, связанные с указанными паттернами, отнесены

к положительному классу риск-событий, а остальные операции рассматривались как нерискованные в рамках данной экспериментальной проверки. При этом важно подчеркнуть, что такая разметка не является юридическим подтверждением факта мошенничества, а служит инструментом проверки способности модели выделять операции, соответствующие заранее заданным риск-сценариям.

Таблица 2

Компоненты гибридной модели риск-ранжирования операций

Table 2

Components of the hybrid risk-ranking model of operations

Компонент	Тип риск-сигнала	Роль в модели	Ограничение
Регламентные правила	Явные нарушения маршрута, реквизитов, лимитов и связности документов	Обеспечивают проверяемость решения и связь с внутренними процедурами контроля	Не выявляют новые схемы без заранее заданного правила
Робастный риск-скоринг	Отклонения суммы, частоты, времени и длительности от исторического профиля	Количественно оценивает степень нетипичности операции при малых и асимметричных данных	Требует настройки признаков, порогов и исторических профилей
Isolation Forest	Нетипичные многомерные сочетания признаков	Добавляет независимый сигнал аномальности без необходимости предварительной разметки fraud-инцидентов	Аномалия не равна мошенничеству и требует ручной интерпретации
Итоговый агрегатор	Совокупный риск-приоритет операции	Объединяет регламентные, статистические и аномальные сигналы в итоговый класс операции	Нужна калибровка весов и границ классов по обратной связи

Источник: составлено авторами в результате исследования
Source: compiled by the authors based on the research

В результате обработки 14 671 исходного события модель выделила 264 операции для дополнительного анализа, что составляет 1,8 % общего потока. Из них 217 операций были отнесены к классу REVIEW, а 47 операций – к классу INCIDENT. Сопоставление результатов риск-ранжирования со сценарной разметкой показало, что из 264 отобранных операций 218 совпали с контрольными риск-сценариями. При общем количестве 247 операций, относящихся к указанным сценариям, это соответствует precision 82,6 %, recall 88,3 % и F1-score 85,3 %. Таким образом, модель позволяет существенно сократить объем ручной проверки при сохранении достаточно высокого охвата риск-событий.

Таблица 3

Сводные результаты апробации модели риск-ранжирования

Table 3

Summary results of the risk ranking model testing

Показатель	Значение
Исходные события	14 671
Операции, отнесенные к риск-сценариям	247
Операции для проверки	264
Истинно положительные срабатывания	218
Ложноположительные срабатывания	46
Ложноотрицательные случаи	29
Precision	82,6 %
Recall	88,3 %
F1-score	85,3 %

Источник: расчеты авторов
Source: the authors' calculations

Более детальный анализ по типам сценариев показывает, что модель наиболее устойчиво выявляет операции, связанные с задержками и нарушениями маршрута согласования, а также с признаками дублирующих платежей. Это объясняется тем, что указанные сценарии оставляют выраженный след в процессном контексте: повторяющиеся документы, совпадение сумм и реквизитов, увеличенная длительность маршрута, несоответствие между счетом, заказом, поступлением и оплатой. Сценарий maverick buying является более сложным для выявления, поскольку часть операций может формально проходить по допустимому маршруту, но отличаться по контрагенту, способу выбора поставщика или отсутствию типичного согласовательного контекста.

Таблица 4

Качество выявления риск-сценариев в P2P-журнале

Table 4

The quality of identifying risk scenarios in the P2P journal

Риск-сценарий	Операции в контрольной разметке	Операции, отобранные моделью	Истинно положительные срабатывания	Precision	Recall	F1-score
Maverick buying	86	88	73	83,0 %	84,9 %	83,9 %
Duplicate payments	59	62	52	83,9 %	88,1%	86,0 %
Lengthy approval process	102	114	93	81,6 %	91,2 %	86,1 %
Итого	247	264	218	82,6 %	88,3 %	85,3 %

Источник: расчеты авторов
Source: the authors' calculations

Полученные результаты показывают, что предложенная модель выполняет не функцию автоматического доказательства мошенничества, а функцию приоритизации операций для последующей проверки. Высокое значение recall указывает на то, что модель охватывает большую часть операций, связанных с контрольными риск-сценариями, а precision выше 80 % показывает, что сформированная очередь проверки не перегружена нерелевантными срабатываниями. Для малого предприятия это имеет практическое значение, поскольку позволяет перейти от сплошного ручного анализа к проверке ограниченного набора операций с повышенным риск-приоритетом.

Качественный анализ результатов подтверждает взаимодополняемость компонентов модели. Регламентные правила преимущественно выявляют нарушения маршрута, отсутствие обязательных этапов, несоответствие связанных документов и признаки дублирующей оплаты. Робастный риск-скоринг повышает приоритет операций с нетипичными суммами, длительностью согласования, частотой действий или отклонением от исторического профиля сотрудника и контрагента. Isolation Forest, в свою очередь, позволяет учитывать редкие и отличающиеся от основной массы наблюдений комбинации признаков, которые не обязательно нарушают отдельное регламентное правило, но могут получать повышенный аномальный скор [19].

Объяснимость модели обеспечивается тем, что для каждой операции может быть сформирован набор причин срабатывания: нарушенное правило, статистическое отклонение, аномальная комбинация признаков или процессное несоответствие. Это отличает предложенный подход от моделей, которые возвращают только итоговый скор без указания оснований. Для внутреннего контроля малого предприятия такая интерпретация принципиальна, поскольку проверяющий должен понимать, почему операция была отнесена к REVIEW или INCIDENT, и какие документы, действия или участников процесса необходимо проверить в первую очередь [18; 21].

Таким образом, результаты апробации подтверждают применимость гибридной модели для формирования объяснимой очереди риск-проверки. Модель не заменяет эксперта и не устанавливает юридический факт мошенничества, но позволяет сузить область ручного анализа, выделить операции с повышенным приоритетом и сохранить прозрачность оснований проверки. Это делает ее применимой как аналитический слой поверх существующего учетного или процессного контура малого предприятия.

Заключение

Проведенное теоретико-эмпирическое исследование позволило разработать математическую модель объяснимого риск-ранжирования операций малого предприятия, ориентированную на раннее выявление признаков внутреннего мошенничества в условиях ограниченности контрольных ресурсов. Полученные результаты показывают, что для малого бизнеса наиболее целесообразен не автономный антифрод-контур, требующий перестройки учета, а аналитический слой, накладываемый поверх существующих учетных и процессных данных.

Теоретическая значимость исследования заключается в синтезе подходов внутреннего контроля, process mining, робастной статистики и анализа аномалий применительно к задаче ранжирования хозяйственных операций. В отличие от классических правил контроля, предложенная модель учитывает не только формальное нарушение регламента, но и статистическую нетипичность операции, ее положение в бизнес-процессе и аномальные сочетания признаков. Это позволяет рассматривать операцию не как отдельную бухгалтерскую запись, а как элемент связанного процессного контекста.

Практическая значимость работы определяется возможностью применения модели в малых предприятиях, где отсутствует развитая служба внутреннего аудита, ограничен ресурс ручной проверки и редко формируется достаточная база подтвержденных fraud-инцидентов. Модель не требует обязательного наличия размеченной выборки и не подменяет экспертную оценку. Ее назначение состоит в формировании объяснимой очереди риск-проверки, в которой каждая операция получает итоговый уровень приоритета и интерпретируемые основания срабатывания: нарушенное правило, статистическое отклонение, процессное несоответствие или аномальную комбинацию признаков.

Ограничения исследования связаны с тем, что апробация выполнена на открытом объектно-центрическом журнале событий, а не на данных конкретного малого предприятия. Поэтому результаты следует рассматривать как подтверждение применимости логики риск-ранжирования, а не как универсальные параметры для любой организации. Перспективы дальнейших исследований связаны с подключением реальных учетных данных, расширением каталога риск-сценариев, сравнением методов выявления аномалий и накоплением экспертной обратной связи. Отдельное направление представляет развитие механизмов объяснимости, позволяющих показывать вклад признаков, правил и процессных отклонений в итоговое решение.

Литература

1. Афанасова Е. И. Система внутреннего контроля – основной инструмент предупреждения и выявления фактов корпоративного мошенничества // Матрица научного познания. 2021. № 8–1. С. 60–65.

2. Воюцкая И. В., Коське М. С., Мишучкова Ю. Г. Внутренний контроль и его потенциал в выявлении рисков искажения бухгалтерской отчетности // Вестник ЮУрГУ. Серия: Экономика и менеджмент. 2022. Т. 16. № 3. С. 144–152. https://doi.org/10.14529/em220316.

3. Кожанов В. М. Система внутреннего финансового контроля для малого ИТ-бизнеса // Научные записки молодых исследователей. 2021. № 6. С. 27–36.

4. Махмудова И. Н. Процессная аналитика в системе комплаенс-контроля // Вестник Самарского университета. Экономика и управление. 2025. Т. 16. № 1. С. 63–73. https://doi.org/10.18287/2542-0461-2025-16-1-63-73.

5. Раджабов Р. Ш. Роль внутреннего контроля в профилактике и выявлении корпоративного мошенничества // Экономика: вчера, сегодня, завтра. 2022. Т. 12. № 3-1. С. 502–509.

6. Шохнех А. В. Особенности организации системы внутреннего контроля в субъектах малого бизнеса // Российское предпринимательство. 2008. Т. 9. № 1. С. 158–162.

7. Mitsyuk A., Kalenkova A., Shershakov S., van der Aalst W. Using process mining for the analysis of an e-trade system: A case study // Business Informatics. 2014. Vol. 8. No. 3. P. 15–27.

8. ACFE. Occupational Fraud 2026: A Report to the Nations. Austin: Association of Certified Fraud Examiners, 2026. URL: https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2026/2026-report-to-the-nations.pdf.

9. Baader G., Krcmar H. Reducing false positives in fraud detection: Combining the red flag approach with process mining // International Journal of Accounting Information Systems. 2018. Vol. 31. P. 1–16. https://doi.org/10.1016/j.accinf.2018.03.004.

10. Baesens B., Höppner S., Verdonck T. Data engineering for fraud detection // Decision Support Systems. 2021. Vol. 150. Article 113492. https://doi.org/10.1016/j.dss.2021.113492.

11. Berti A., Jessen U., Park G., Rafiei M., van der Aalst W. M. P. Analyzing interconnected processes: using object-centric process mining to analyze procurement processes // International Journal of Data Science and Analytics. 2025. Vol. 20. No. 2. P. 475–497. https://doi.org/10.1007/s41060-023-00427-3.

12. Berti A., Koren I., Adams J. N., Park G., Knopp B., Graves N., Rafiei M., Liß L., Tacke Genannt Unterberg L., Zhang Y., Schwanen C., Pegoraro M., van der Aalst W. M. P. OCEL (Object-Centric Event Log) 2.0 Specification. 2024. arXiv:2403.01975. URL: https://arxiv.org/abs/2403.01975.

13. Park G., Tacke Genannt Unterberg L. Procure-To-Payment (P2P) Object-centric Event Log in OCEL 2.0 Standard [Data set] // Zenodo. 2023. https://doi.org/10.5281/zenodo.8412920.

14. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey // ACM Computing Surveys. 2009. Vol. 41. No. 3. Article 15. https://doi.org/10.1145/1541880.1541882.

15. Hess M. F., Cottrell J. H. Jr. Fraud risk management: A small business perspective // Business Horizons. 2016. Vol. 59. No. 1. P. 13–18. https://doi.org/10.1016/j.bushor.2015.09.005.

16. Jans M., Hosseinpour M. How active learning and process mining can act as Continuous Auditing catalyst // International Journal of Accounting Information Systems. 2019. Vol. 32. P. 44–58. https://doi.org/10.1016/j.accinf.2018.11.002.

17. Ko J., Comuzzi M. A Systematic Review of Anomaly Detection for Business Process Event Logs // Business & Information Systems Engineering. 2023. Vol. 65. No. 4. P. 441–462. https://doi.org/10.1007/s12599-023-00794-y.

18. Li Z., Zhu Y., van Leeuwen M. A Survey on Explainable Anomaly Detection // ACM Transactions on Knowledge Discovery from Data. 2023. Vol. 18. No. 1. Article 23. https://doi.org/10.1145/3609333.

19. Liu F. T., Ting K. M., Zhou Z.-H. Isolation Forest // Proceedings of the 2008 Eighth IEEE International Conference on Data Mining. Pisa, Italy, 2008. P. 413–422. https://doi.org/10.1109/ICDM.2008.17.

20. Othman R., Ameer R. In employees we trust: Employee fraud in small businesses // Journal of Management Control. 2022. Vol. 33. No. 2. P. 189–213. https://doi.org/10.1007/s00187-022-00335-w.

21. Tritscher J., Schlör D., Gwinner F., Krause A., Hotho A. Towards Explainable Occupational Fraud Detection // Machine Learning and Principles and Practice of Knowledge Discovery in Databases: ECML PKDD 2022 Workshops. Cham: Springer, 2023. Vol. 1753. P. 79–96. https://doi.org/10.1007/978-3-031-23633-4_7.

References

1. Afanasova E.I. (2021). Sistema vnutrennego kontrolya – osnovnoi instrument preduprezhdeniya i vyyavleniya faktov korporativnogo moshennichestva [Internal control system as the main instrument for preventing and detecting corporate fraud]. Matritsa nauchnogo poznaniya [Matrix of Scientific Cognition], 8–1, 60–65. (In Russ., abstract in Eng.).

2. Voyutskaya I.V., Kos'ke M.S., Mishuchkova Yu.G. (2022). Vnutrennii kontrol' i ego potentsial v vyyavlenii riskov iskazheniya bukhgalterskoi otchetnosti [Internal control and its potential in identifying risks of financial statement misstatements]. Vestnik YuUrGU. Seriya: Ekonomika i menedzhment [Bulletin of

South Ural State University. Series: Economics and Management], 16(3), 144–152. https://doi.org/10.14529/em220316. (In Russ., abstract in Eng.).

3. Kozhanov V.M. (2021). Sistema vnutrennego finansovogo kontrolya dlya malogo IT-biznesa [Internal financial control system for small IT businesses]. Nauchnye zapiski molodykh issledovatelei [Scientific Notes of Young Researchers], 6, 27–36. (In Russ., abstract in Eng.).

4. Makhmudova I.N. (2025). Protsessnaya analitika v sisteme komplaens-kontrolya [Process analytics in the compliance control system]. Vestnik Samarskogo universiteta. Ekonomika i upravlenie [Vestnik of Samara University. Economics and Management], 16(1), 63–73. https://doi.org/10.18287/2542-0461-2025-16-1-63-73. (In Russ., abstract in Eng.).

5. Radzhabov R.Sh. (2022). Rol' vnutrennego kontrolya v profilaktike i vyyavlenii korporativnogo moshennichestva [The role of internal control in preventing and detecting corporate fraud]. Ekonomika: vchera, segodnya, zavtra[Economics: Yesterday, Today and Tomorrow], 12(3-1), 502–509. (In Russ.).

6. Shokhnekh A.V. (2008). Osobennosti organizatsii sistemy vnutrennego kontrolya v sub"ektakh malogo biznesa [Features of organizing an internal control system in small businesses]. Rossiiskoe predprinimatel'stvo [Russian Journal of Entrepreneurship], 9(1), 158–162. (In Russ., abstract in Eng.).

7. Mitsyuk A., Kalenkova A., Shershakov S., van der Aalst W. (2014). Using process mining for the analysis of an e-trade system: A case study. Business Informatics, 8(3), 15–27. (In Eng.).

8. Association of Certified Fraud Examiners. (2026). Occupational Fraud 2026: A Report to the Nations. Austin: ACFE. Retrieved from: https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2026/2026-report-to-the-nations.pdf. (In Eng.).

9. Baader G., Krcmar H. (2018). Reducing false positives in fraud detection: Combining the red flag approach with process mining. International Journal of Accounting Information Systems, 31, 1–16. https://doi.org/10.1016/j.accinf.2018.03.004. (In Eng.).

10. Baesens B., Höppner S., Verdonck T. (2021). Data engineering for fraud detection. Decision Support Systems, 150, Article 113492. https://doi.org/10.1016/j.dss.2021.113492. (In Eng.).

11. Berti A., Jessen U., Park G., Rafiei M., van der Aalst W.M.P. (2025). Analyzing interconnected processes: Using object-centric process mining to analyze procurement processes. International Journal of Data Science and Analytics, 20(2), 475–497. https://doi.org/10.1007/s41060-023-00427-3. (In Eng.).

12. Berti A., Koren I., Adams J.N., Park G., Knopp B., Graves N., Rafiei M., Liß L., Tacke Genannt Unterberg L., Zhang Y., Schwanen C., Pegoraro M., van der Aalst W.M.P. (2024). OCEL (Object-Centric Event Log) 2.0 Specification. arXiv:2403.01975. Retrieved from: https://arxiv.org/abs/2403.01975. (In Eng.).

13. Park G., Tacke Genannt Unterberg L. (2023). Procure-To-Payment (P2P) Object-Centric Event Log in OCEL 2.0 Standard [Data set]. Zenodo. https://doi.org/10.5281/zenodo.8412920. (In Eng.).

14. Chandola V., Banerjee A., Kumar V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), Article 15. https://doi.org/10.1145/1541880.1541882. (In Eng.).

15. Hess M.F., Cottrell J.H. Jr. (2016). Fraud risk management: A small business perspective. Business Horizons, 59(1), 13–18. https://doi.org/10.1016/j.bushor.2015.09.005. (In Eng.).

16. Jans M., Hosseinpour M. (2019). How active learning and process mining can act as a continuous auditing catalyst. International Journal of Accounting Information Systems, 32, 44–58. https://doi.org/10.1016/j.accinf.2018.11.002. (In Eng.).

17. Ko J., Comuzzi M. (2023). A systematic review of anomaly detection for business process event logs. Business & Information Systems Engineering, 65(4), 441–462. https://doi.org/10.1007/s12599-023-00794-y. (In Eng.).

18. Li Z., Zhu Y., van Leeuwen M. (2023). A survey on explainable anomaly detection. ACM Transactions on Knowledge Discovery from Data, 18(1), Article 23. https://doi.org/10.1145/3609333. (In Eng.).

19. Liu F.T., Ting K.M., Zhou Z.-H. (2008). Isolation Forest. In: Proceedings of the 2008 Eighth IEEE International Conference on Data Mining. Pisa, Italy. P. 413–422. https://doi.org/10.1109/ICDM.2008.17. (In Eng.).

20. Othman R., Ameer R. (2022). In employees we trust: Employee fraud in small businesses. Journal of Management Control, 33(2), 189–213. https://doi.org/10.1007/s00187-022-00335-w. (In Eng.).

21. Tritscher J., Schlör D., Gwinner F., Krause A., Hotho A. (2023). Towards explainable occupational fraud detection. In: Machine Learning and Principles and Practice of Knowledge Discovery in Databases: ECML PKDD 2022 Workshops. Cham: Springer. Vol. 1753. P. 79–96. https://doi.org/10.1007/978-3-031-23633-4_7. (In Eng.).