DOI 10.46320/2077-7639-2025-2-135-181-188

Современные технологии выявления и предотвращения корпоративного мошенничества

Сафина Р.Р., Цзян Т.

Одним из наиболее распространенных явлений в современном мире является корпоративное мошенничество, которое несет особые риски и ущерб как для самой компании и собственников бизнеса, так и для общества в целом. Причинами мошеннических действий могут быть введение в заблуждение инвесторов и (или) собственников путем преднамеренного искажения данных финансовой отчетности, разногласия и конфликты между собственниками и топ-менеджментом компании, а также желание мажоритарных акционеров лишить миноритарных доли прибыли. Для выявления мошеннических схем в современных условиях возникает необходимость применения эффективных финансовых и цифровых технологий, основанных на использовании учетных и отчетных данных и направленных на выявление индикаторов наличия различных злоупотреблений и махинаций.

Объект исследования – корпоративное мошенничество. Предмет исследования – технологии выявления и предотвращения корпоративного мошенничества. Цель исследования – проанализировать и обобщить имеющийся российский и зарубежный опыт реализации современных методов и технологий противодействия корпоративному мошенничеству.

В статье рассмотрены теоретические аспекты корпоративного мошенничества, факторы риска его возникновения, а также современные методы выявления и предотвращения мошеннических действий, включая финансовые индикаторы и цифровые технологии.

ДЛЯ ЦИТИРОВАНИЯ ГОСТ 7.1–2003

Сафина Р.Р., Цзян Т. Современные технологии выявления и предотвращения корпоративного мошенничества // Дискуссия. – 2025. – Вып. 135. – С. 181–188.

КЛЮЧЕВЫЕ СЛОВА

Корпоративное мошенничество, коррупция, бухгалтерская (финансовая) отчетность, искажение, цифровые технологии.

DOI 10.46320/2077-7639-2025-2-135-181-188

Modern technologies for detecting and preventing corporate fraud

Safina R.R., Jiang T.

One of the most common phenomena in the modern world is corporate fraud, which carries special risks and damage both for the company itself and the business owners, and for society as a whole. The causes of fraudulent actions may be misleading investors and (or) owners by deliberately distorting financial reporting data, disagreements and conflicts between the owners and top management of the company, as well as the desire of majority shareholders to deprive minority shareholders of their share of the profit. To identify fraudulent schemes in modern conditions, there is a need to use effective financial and digital technologies based on the use of accounting and reporting data and aimed at identifying indicators of the presence of various abuses and machinations.

Object of the study – corporate fraud. Subject of the study – technologies for detecting and preventing corporate fraud. The purpose of the study is to analyze and summarize the existing Russian and foreign experience in implementing modern methods and technologies to combat corporate fraud.

The article examines the theoretical aspects of corporate fraud, risk factors for its occurrence, as well as modern methods for identifying and preventing fraudulent activities, including financial indicators and digital technologies.

FOR CITATION APA

Safina R.R., Jiang T. Modern technologies for detecting and preventing corporate fraud. *Diskussiya [Discussion]*, 135, 181–188.

KEYWORDS

Corporate fraud, corruption, accounting (financial) reporting, distortion, digital technologies.

ВВЕДЕНИЕ

Корпоративное мошенничество является одной из финансовых угроз для инвесторов. Современные технологии, включая искусственный интеллект, методы анализа данных, машинное обучение позволяют существенно повысить эффективность выявления признаков мошенничества и минимизировать риски мошеннических схем.

Благодаря постоянному развитию и совершенствованию финансовых и цифровых технологий открываются новые возможности и способы предупреждения, выявления и предотвращения различных видов и форм корпоративного мошенничества.

ОСНОВНАЯ ЧАСТЬ

Понятие «*мошенничество*» содержится в нормах уголовного законодательства РФ и представляет «*хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием*». Статьей 159 Уголовного кодекса Российской Федерации предусмотрены следующие виды мошенничества:

— совершенное группой лиц по предварительному сговору;

— совершенное лицом с использованием своего служебного положения;

— сопряженное с преднамеренным неисполнением договорных обязательств в сфере предпринимательской деятельности.

При этом в соответствии с п. 7 ст. 159 УК РФ ущерб может быть «значительным» – не менее двухсот пятидесяти тысяч рублей, «крупным» – превышающим четыре миллиона пятьсот тысяч рублей, «особо крупным» – превышающим восемнадцать миллионов рублей [1].

Кроме того, факты мошенничества часто находятся под прикрытием «мнимых» и «притворных» сделок, понятия которых содержатся и раскрываются в нормах Гражданского законодательства и Федерального закона РФ № 402-ФЗ «О бухгалтерском учете».

В российском законодательстве не закреплено понятие «корпоративное мошенничество». На практике под «корпоративным мошенничеством», как правило, понимаются мошеннические действия сотрудников компании и (или) ее руководителей.

На рисунке 1 представлена модель отнесения известных видов мошенничества по категориям. Данная модель, известная как «дерево мошенничества», была разработана Ассоциацией дипломированных экспертов по мошенничеству (Association of Certified Fraud Examiners, ACFE) [2].

Как видно из рисунка 1, под основными категориями корпоративного мошенничества, согласно представленной модели, следует рассматривать коррупцию, мошенничество в финансовой отчетности, а также незаконное присвоение имущества с помощью различных махинаций.

Согласно российскому законодательству «*коррупция*» означает *«злоупотребление служебным положением, дачу взятки, получение взятки, злоупотребление полномочиями, коммерческий подкуп либо иное незаконное использование физическим лицом своего должностного положения вопреки законным интересам общества и государства в целях получения выгоды в виде денег, ценностей, иного имущества или услуг имущественного характера, иных имущественных прав для себя или для третьих лиц либо незаконное предоставление такой выгоды указанному лицу другими физическими лицами»* [3].

Для более глубоко понимания и представления разновидностей мошенничества с финансовой отчетностью была рассмотрена сущность понятий «*Искажение финансовой отчетности», «Манипуляция учетными записями», «Вуалирование баланса», «Фальсификация финансовой отчетности».*

Понятие *«искажение»* раскрывается в международном стандарте аудита 450 и представляет

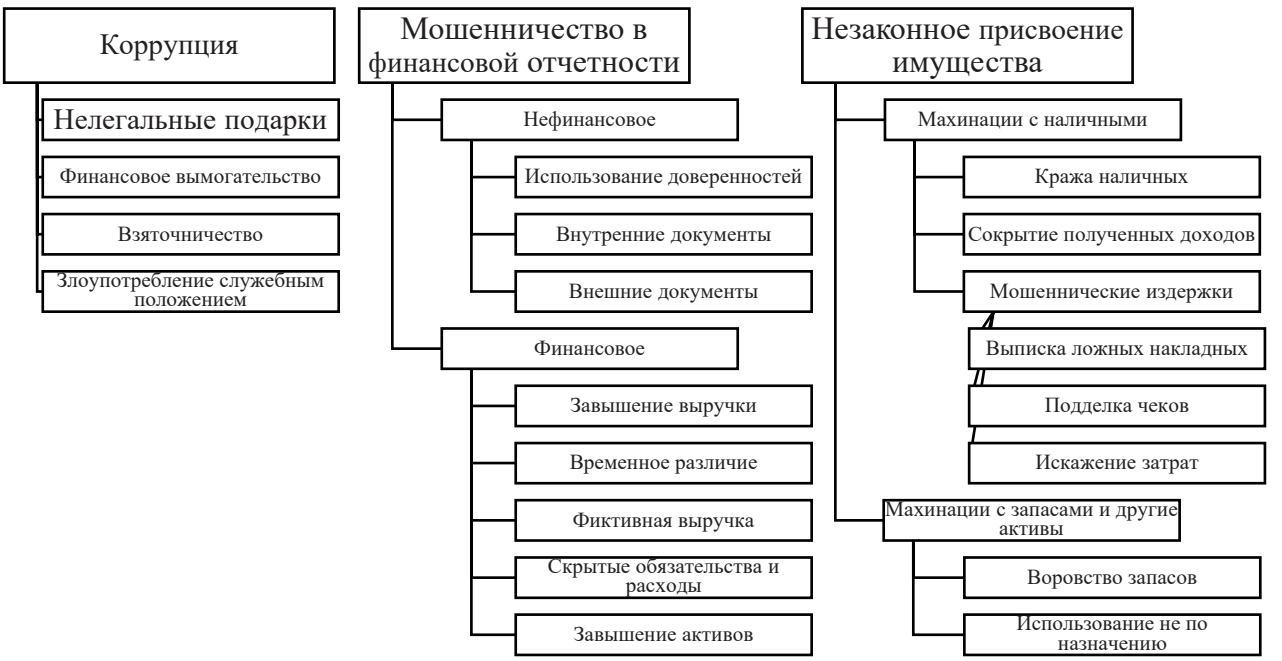

Рисунок 1. Дерево мошенничества

Источник: [2].

собой «*расхождение между включенной в отчетность суммой, классификацией, представлением или раскрытием информации в финансовой отчетности и суммой, классификацией, представлением или раскрытием информации, которые требуются в соответствии с применимой концепцией подготовки финансовой отчетности*» [4]. При этом согласно стандарту искажения могут быть как «следствие недобросовестных действий», то есть преднамеренными или совершаться в результате «ошибок», имея непреднамеренный характер.

Манипуляция с бухгалтерской (финансовой) отчетностью совершается в целях введения в заблуждение пользователей такой отчетности, а проводимое с помощью *вуалирования* и *фальсификации* отчетных данных, являются одним из способов мошенничества.

Группировка вышеприведенных терминологий позволила определить их взаимосвязь и представить, как способы «*мошенничества в финансовой отчетности*» (рисунок 2).

Таким образом, любые искажения и манипуляции с отчетностью приводят к *мошенничеству.*

На наличие искажений информации, содержащейся в финансовой отчетности, указывают основные признаки, представленные на рисунке 3.

К ним относятся:

— наличие отрицательных денежных потоков при устойчивом росте прибыли;

— значительные суммы созданных резервов;

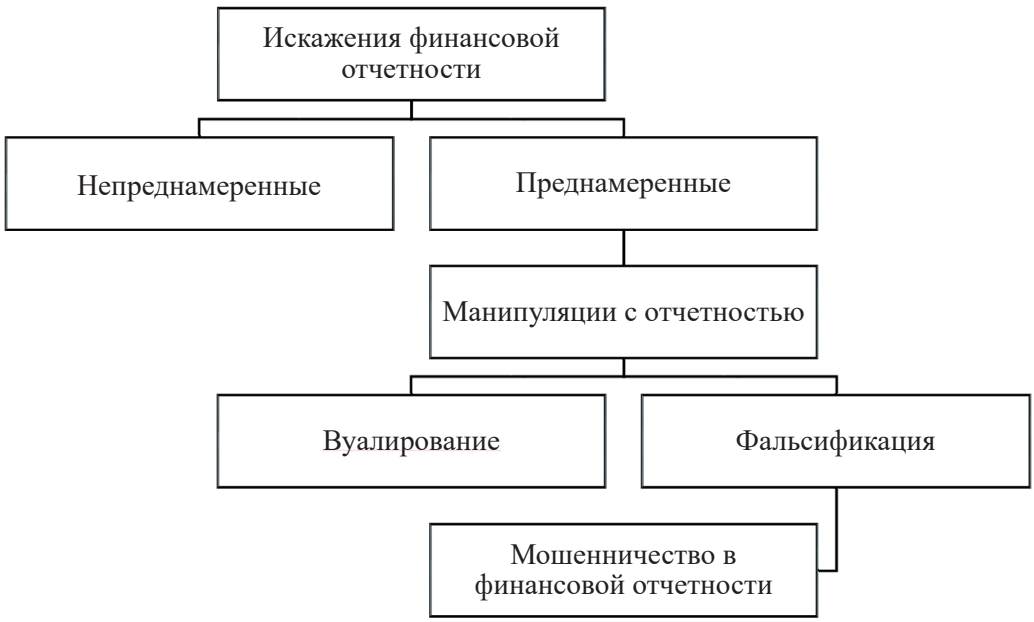

Рисунок 2. Способы мошенничества с финансовой отчетностью

Рисунок 3. Признаки искажения информации

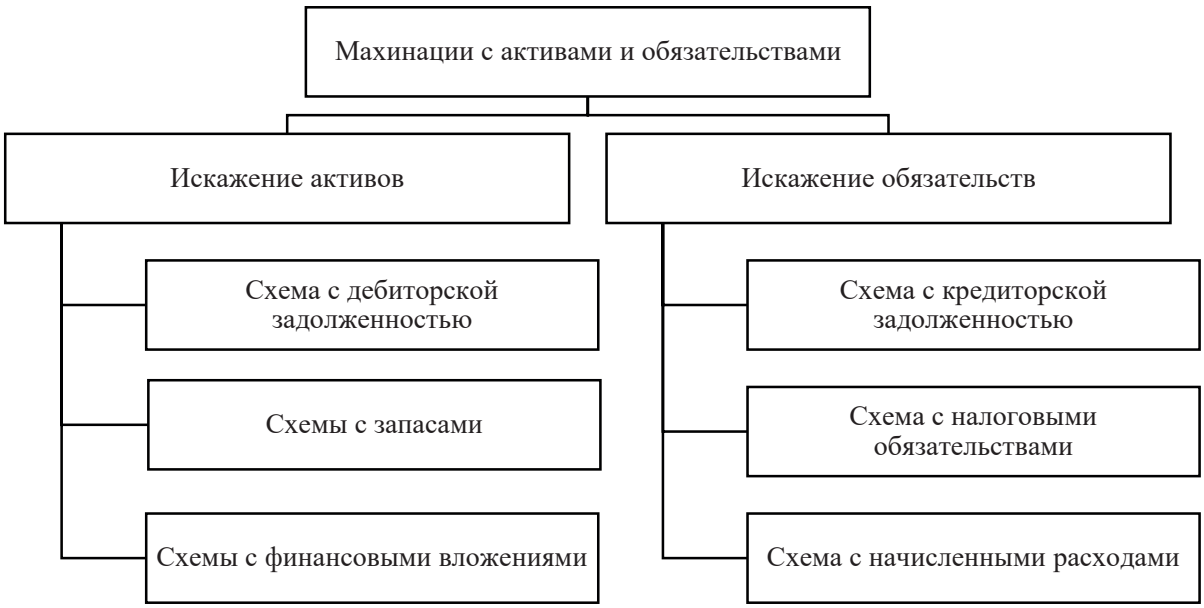

Рисунок 4. Примеры мошенничества с активами и обязательствами

— резкий рост запасов, основных средств и так далее.

Примеры махинаций с активами и обязательствами, результатом которых является мошенничество, представлены на рисунке 4.

Для эффективного недопущения мошенничества с финансовой отчетностью необходима действенная система ее предупреждения и предотвращения на законодательном уровне.

На международном уровне к документу, направленному на ужесточение требований к финансовой отчётности и процессу её подготовки, а также на обеспечение контроля за финансово-хозяйственной деятельности публичных компаний относится *Закон Сарбейнса-Оксли,* принятый в США 30 июля 2002 года. Данный закон был принят как результат многочисленных корпоративных скандалов, связанных с коррупцией, мошенничеством и фальсификацией финансовой отчетности крупными компаниями, одной из которых является американская энергетическая компания Enron, обанкротившаяся в 2001 году.

Российское законодательство предусматривает в обязательном порядке создание с 1 июля 2020 года для публичных компаний Комитетов по аудиту при Совете Директоров *«для предварительного рассмотрения вопросов, связанных с контролем за финансово-хозяйственной деятельностью публичного общества, в том числе с оценкой независимости аудиторской организации публичного общества и отсутствием у нее конфликта интересов, а также с оценкой качества проведения аудита бухгалтерской (финансовой) отчетности общества»* [5].

В ходе исследований были рассмотрены методы противодействия корпоративному мошенничеству, которые можно подразделить на следующие группы: предупреждение, выявление и расследование.

В каждой из представленных групп можно выделить организационные и технические методы. Например, к организационным можно отнести принятие соответствующей внутренней документации и ознакомление персонала с этими документами. Такими документами являются «Политика по противодействию коррупции» и «Кодекс этики» («Кодекс корпоративного поведения»), которые должны быть разработаны и утверждены при построении системы внутреннего контроля и составлять корпоративную культуру и контрольную среду, исключающую возможность совершения мошенничества.

Технические методы предусматривают использование программных продуктов для:

— защиты информации финансового характера от внесения в нее искажений;

— предотвращения утечки информации из компании;

— выявления ошибок в отчетности и базах данных, указывающих на факт совершения мошеннических действий.

В ходе исследований рассмотрен порядок обнаружения мошенничества механизмами искусственного интеллекта, которые могут широко

Таблица 1

Примеры использования искусственного интеллекта при выявлении и предупреждении мошенничества, связанного с коррупцией

Наименование продукта	Страна-разработчик	Пример использования	Цель использования
Робот ACE	Великобритания компания Ravn	Расследование дела Rolls-Royce	ускорение обработки больших объемов данных [6]
Модель на основе нейронных сетей	Испания	Использование в регионах страны	прогнозирование коррупции в зависимости от экономических условий региона, определение вероятности коррупционных нарушений и условий их совершения [7]
Платформа управления цифровыми коммуникациями Shield	Израиль, компания Shield FC	Применение для выявления преднамеренных попыток мошенничества	комплаенс-контроль в сфере коммуникаций, снижения рисков и повышения эффективности надзора, упреждающий мониторинг недобросовестного поведения для выявления рыночных манипуляций [7]

применяться для поиска и выявления существующих мошеннических схем, а также предсказания и предотвращения их появления в будущем (таблица 1).

При использовании искусственного интеллекта анализируются закономерности в финансовых операциях и выявление необычного или подозрительного поведения.

Так, например, в феврале 2017 года Бюро по расследованию случаев серьезного мошенничества Великобритании (Serious Fraud Office – SFO) использовало робот ACE в ходе коррупционного разбирательства в компании Rolls-Royce [6]. Данный робот, способный анализировать и обобщать данные из различных источников, включая текстовые файлы, таблицы и даже изображения, в том числе в формате PDF, был создан британской стартап-компанией в сфере искусственного интеллекта Ravn Systems.

Расследование по делу о коррупции и мошенничестве компании Rolls-Royce, являющейся вторым по рыночной доле производителем авиационных двигателей в мире, было начато в 2012 году. Компанию обвинили в даче взяток чиновникам в 12 странах мира. Использование робота ACE позволило семи специалистам-следователям обработать в автоматическом режиме более 30 млн. документов (по 600 тыс. документов в день), отсортировав их на «важные» и «неважные». В итоге Rolls-Royce признала вину и согласилась выплатить штраф, превышающий $800 млн.

Блокчейн, который представляет собой одну из технологий распределенных баз данных, также может быть использован в целях противодействия коррупции. Использование данной технологии позволяет отслеживать денежные потоки, затрудняет манипулирование данными, а также не позволяет изменять или удалять информацию о транзакциях.

Так, технология блокчейн использовалась Всемирной продовольственной программой в рамках пилотного проекта «Building Blocks» для изучения возможности повышения эффективности, безопасности и прозрачности прямых денежных переводов беженцам, в том числе минимизации коррупционных рисков, таких как взяточничество и вымогательство со стороны посредников [7].

Big data, представляющая анализ больших и сложных массивов данных, может использоваться для целей противодействия коррупции по следующим направлениям:

— выявление, расследование, мониторинг и аудит подозрительных операций;
— оценка коррупционных рисков;
— важные расследования.

Например, по данным *Международного консорциума журналистов-расследователей (International Consortium of Investigative Journalists – ICIJ)* анализ big data с использованием технологии Linkurious и базы данных Neo4j применялся журналистами-расследователями при работе с *«Архивом Пандоры». Данный архив «содержит рекордное количество информации – около 11,9 млн файлов, общий объем которых достигает 2,94 терабайта, принадлежащих 14 компаниям, которые предоставляли своим клиентам услуги по размещению их активов в офшорных зонах»* [8].

«В ходе анализа документов журналисты выявили множество фактов использования высокопоставленными лицами из более чем 90 стран и территорий офшорных зон для покупки собственности или сокрытия активов: в их число вошли свыше 330 политиков, включая 35 бывших и нынешних глав го-

сударств, 130 миллиардеров из списка Forbes, звезды эстрады и спорта, супермодели» [8].

Важная роль в выявлении мошенничества отводится анализу финансовых показателей. Ненормальные показатели ликвидности, чрезмерный уровень задолженности и необоснованная прибыльность могут указывать на наличие финансовых манипуляций.

Постоянный мониторинг ключевых финансовых показателей деятельности хозяйствующего субъекта и проведение сравнительного анализа с отраслевыми значениями позволяют эффективно и своевременно выявлять потенциальные риски финансового мошенничества и защищать интересы инвесторов.

К аналитическим методам выявления и предотвращения мошенничества с финансовой отчетностью, относятся: закон Бенфорда, система показателей Бениша и анализ расхождения денежного потока и операционной прибыли.

Закон Бенфорда позволяет выявить ошибки и искажения в числовом массиве данных путем сопоставления частоты появления каждой цифры в анализируемом массиве данных с вероятностью появления цифры в случайном ряду, построенном согласно закону Бенфорда.

«Закон Бенфорда или закон первой цифры гласит, что в таблицах чисел, основанных на данных источников из реальной жизни цифра 1 на первом месте встречается гораздо чаще, чем все остальные (приблизительно в 30 % случаях), а также вероятность того, что цифра будет стоять на первом месте в числе тем больше, чем меньше цифра» [9].

На основе закона Бенфорда американским математиком Марк Нигрини разработана программа «Digital Analysis», позволяющая выявлять различные мошеннические финансовые схемы ухода от налогообложения. Данная программа особенно активно используется аудиторскими компаниями большой четверки.

Модель «Бениша» (модель «M-score»), предложенная профессором Мессодом Д. Бенишем в 1999 г., используется для выявления взаимосвязей между показателями бухгалтерского баланса и отчета о финансовых результатах. Модель основана на расчете сводного индекса «M-score» путем сложения следующих показателей: *«индекс оборачиваемости дебиторской задолженности в днях; индекс валовой маржи; индекс качества активов; индекс роста выручки; индекс амортизации; индекс коммерческих и управленческих расходов; индекс суммарных начислений к суммарным активам; индекс финансового рычага»* [10]. Значение сводного индекса для организаций, манипулирующих с прибылью, должно превышать «минус 2,22». Данный метод часто используется аудиторами при выявлении рисков мошенничества с финансовой отчетностью.

Во многом модель Бениша (M-score) имеет сходство с моделью Альтмана (Z-score), однако сконцентрирована на выявлении признаков возможного мошенничества, а не банкротства.

Еще один аналитический метод выявления мошенничества с финансовой отчетностью заключается в анализе с использованием данных отчёта о движении денежных средств. Согласно данному методу, чистая прибыль (убыток), отраженная в финансовой отчетности, и сальдо денежных потоков от текущих операций должны быть тесно взаимосвязаны путем определения коэффициента денежных средств, полученных от текущей деятельности (Кдсто):

$$К_{дсто} = \frac{Сальдо\ денежных\ потоков\ от\ текущих\ операций}{Чистая\ прибыль\quad убыток}$$

Из приведенной формулы следует, что с изменением прибыли аналогично должны изменяться и сальдированные денежные потоки от текущей деятельности. Несоответствие данному правилу указывает на манипуляции с прибылью и является признаком мошенничества.

ЗАКЛЮЧЕНИЕ

Таким образом, по результатам представленной в статье информации по использованию отдельных финансовых и цифровых технологий в области выявления и предупреждения корпоративного мошенничества сделаны выводы о современных тенденциях развития данных технологий.

Список литературы

1. *Уголовный* кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 28.02.2025).
2. *Мухаметшин, Р. Т.* Мошенничество в финансовой отчетности / Р. Т. Мухаметшин // Экономический анализ: теория и практика. – 2009. – № 6(135). – С. 49-58.
3. *Федеральный* закон от 25.12.2008 № 273-ФЗ (ред. от 08.08.2024) «О противодействии коррупции».
4. *МСА 450* «Оценка искажений, выявленных в ходе аудита» (введен в действие на территории Российской Федерации Приказом Минфина России от 09.01.2019 № 2н).
5. *Федеральный* закон от 26.12.1995 № 208-ФЗ (ред. от 30.11.2024) «Об акционерных обществах».
6. *[Электронный ресурс].* – Режим доступа: https://anticor.world/main/news_page/vlasti_velikobritanii_ispolzovali_

iskusstvennyy_intellekt_v_korruptsionnom_rassledovanii.

7. *[Электронный ресурс].* – Режим доступа: https://anticor.world/main/news_page/opublikovan_doklad_ob_ispolzovanii_novyh_tehnologiy_v_borbe_s_korruptsiey.
8. *[Электронный ресурс].* – Режим доступа: https://anticor.world/main/news_page/yaschik_pandory_opublikovany_rezultaty_rassledovaniya_ob_ofshorah_soten_politikov_i_oligarhov.
9. *Кувакина, Л. В., Долгополова, А. Ф.* Современные наукоемкие технологии. – 2013. – № 6. – С. 74-76. – [Электронный ресурс]. – Режим доступа: https://top-technologies.ru/ru/article/view?id=31987.
10. *Бахтеев, А. В., Арженовский, С. В.* Аналитические процедуры как инструмент идентификации риска фальсификации финансовой отчетности: методологический и методический аспекты // Аудиторские ведомости. – 2016. – № 12. – С. 45-60.
11. *Рощектаев, С. А., Рощектаева, У. Ю.* Выявление фактов фальсификации финансовой отчетности: модель М. Бениша // Научный вестник Южного института менеджмента. – 2018. – № 2. – С. 37-43. – [Электронный ресурс]. – Режим доступа: https://doi.org/10.31775/2305-3100-2018-2-37-43.
12. *Короролева, Л. П.* Противодействие мошенничеству в сфере предпринимательской деятельности с применением информационных технологий / Л. П. Королева, А. И. Гучмазов // Вестник Академии знаний. – 2024. – № 3. – С. 245-251. – [Электронный ресурс]. – Режим доступа: http://elib.fa.ru/art2024/bv580.pdf.
13. *Полещук, А. Д.* Аналитические подходы выявления фальсификации бухгалтерской (финансовой) отчетности // Экономика и бизнес: теория и практика. – 2016. – № 5. – С. 139-141.

References

1. *The Criminal* Code of the Russian Federation" dated 13.06.1996 № 63-FZ (as amended on 28.02.2025).
2. *Mukhametshin, R. T.* Fraud in financial statements / R. T. Mukhametshin // Economic analysis: theory and practice. – 2009. – № 6(135). – Pp. 49-58.
3. *Federal* Law № 273-FZ of December 25, 2008 (as amended on 08.08.2024) "On Combating Corruption".
4. *ISA 450* "Assessment of Misstatements Identified during the Audit" (introduced in the Russian Federation by Order of the Ministry of Finance of the Russian Federation dated 09.01.2019 № 2h).
5. *Federal* Law № 208-FZ dated 26.12.1995 (as amended on 30.11.2024) "On Joint Stock Companies".
6. *[Electronic resource].* – Access mode: https://anticor.world/main/news_page/vlasti_velikobritanii_ispolzovali_iskusstvennyy_intellekt_v_korruptsionnom_rassledovanii.
7. *[Electronic resource].* – Access mode: https://anticor.world/main/news_page/opublikovan_doklad_ob_ispolzovanii_novyh_tehnologiy_v_borbe_s_korruptsiey.
8. *[Electronic resource].* – Access mode: https://anticor.world/main/news_page/yaschik_pandory_opublikovany_rezultaty_rassledovaniya_ob_ofshorah_soten_politikov_i_oligarhov.
9. *Kuvakina, L. V., Dolgopolova, A. F.* Modern high-tech technologies. - 2013. – № 6. – Pp. 74-76. – [Electronic resource]. – Access mode: https://top-technologies.ru/ru/article/view?id=31987.
10. *Bakhteev, A. V., Arzhenovsky, S. V.* Analytical procedures as a tool for identifying the risk of falsification of financial statements: methodological and methodological aspects // Audit statements. – 2016. – № 12. – Pp. 45-60.
11. *Roshchektaev, S. A., Roshchektaeva, U. Y.* Identification of facts of falsification of financial statements: the model of M. Benisha // Scientific Bulletin of the Southern Institute of Management. – 2018. – № 2. – Pp. 37-43. – [Electronic resource]. – Access mode: https://doi.org/10.31775/2305-3100-2018-2-37-43.
12. *Kororoleva, L. P.* Countering fraud in the field of entrepreneurial activity using information technology / L. P. Koroleva, A. I. Guchmazov // Bulletin of the Academy of Knowledge. – 2024. – № 3. – Pp. 245-251. – [Electronic resource]. – Access mode: http://elib.fa.ru/art2024/bv580.pdf.
13. *Poleshchuk, A. D.* Analytical approaches to detecting falsification of accounting (financial) statements // Economics and Business: theory and practice. – 2016. – № 5. – Pp. 139-141.

Информация об авторах

Сафина Р.Р., доцент кафедры корпоративных финансов и учетных технологий Уфимского государственного нефтяного технического университета, аттестованный аудитор (г. Уфа, Российская Федерация).

Цзян Т., магистрант кафедры корпоративных финансов и учетных технологий Уфимского государственного нефтяного технического университета, независимый исследователь (г. Уфа, Российская Федерация).

Information about the authors

Safina R.R., Associate Professor of corporate finance and accounting technologies Department of Ufa State Petroleum Technological University (Ufa, Russian Federation).

Jiang T., magister student at the Department of Corporate Finance and Accounting Technologies of the Ufa State Petroleum Technological University, independent researcher (Ufa, Russian Federation).