

Шуляк Полина Викторовна

студентка

ФГБОУ ВО «Санкт-Петербургский государственный
архитектурно-строительный университет»

г. Санкт-Петербург

ФИНАНСОВЫЕ МАХИНАЦИИ: КАК ИХ РАСПОЗНАТЬ

Аннотация: статья посвящена систематизации признаков финансовых махинаций и методов их распознавания в системе экономической безопасности. Раскрываются сущность и виды махинаций: фальсификация отчётности, фиктивные операции, мошенничество в платёжной сфере, легализация доходов. Выделяются «красные флаги» и «треугольник мошенничества». Рассматриваются три группы методов: аналитические (коэффициентный анализ, оценка банкротства), цифровые (Big Data, ИИ, нейросети с точностью 95–98% в реальном времени) и организационно-правовые (финансовый мониторинг, государственный и внутренний контроль). Вывод: эффективное распознавание возможно лишь при комплексном применении всех трёх групп и постоянном обновлении инструментов детекции.

Ключевые слова: финансовые махинации, мошенничество, экономическая безопасность, фальсификация отчётности, красные флаги, финансовый мониторинг, машинное обучение, искусственный интеллект.

Введение.

Стремительная цифровизация экономики ведёт к росту электронных платежей и безналичных расчётов, одновременно расширяя возможности злоупотреблений. Финансовые махинации становятся системной угрозой экономической безопасности хозяйствующих субъектов и государства. Поэтому своевременное распознавание мошеннических схем – базовое требование к системе управления рисками, а не только задача служб безопасности. Актуальность темы обусловлена противоречием: методы выявления мошенничества совершенствуются, но зло-

умышленники быстро адаптируются, и традиционные способы защиты уже недостаточно надёжны. Нужен комплексный подход, объединяющий аналитические, цифровые и организационно-правовые инструменты.

Объект исследования – финансовые махинации как угроза экономической безопасности; предмет – методы и индикаторы их распознавания. Цель – систематизировать признаки финансовых махинаций и методы их выявления для построения эффективной системы противодействия. Задачи: раскрыть сущность и виды махинаций; выделить ключевые индикаторы («красные флаги»); охарактеризовать аналитические, цифровые и организационно-правовые методы; сформулировать рекомендации по системе раннего выявления. Методологическая основа – анализ и обобщение публикаций по экономической безопасности, финансовому мониторингу и противодействию мошенничеству.

Сущность и признаки финансовых махинаций.

Финансовые махинации – умышленные действия для неправомерной выгоды через искажение финансовой информации, обман контрагентов или манипулирование потоками. В системе экономической безопасности это внутренняя угроза: подрывает достоверность учёта и дестабилизирует управленческие решения. Учётная система должна отсеивать опасные операции и предотвращать мошенничество.

Основные виды: фальсификация отчётности («креативный учёт») ради привлекательного образа компании; фиктивные операции, включая фиктивные сделки, обналичивание и транзит средств; мошенничество в платёжной сфере – несанкционированные транзакции, подставные лица, смена поведенческих паттернов клиента; легализация (отмывание) доходов, выявляемая финансовым мониторингом.

Распознавание опирается на мотивацию нарушителя. Концепция «треугольника мошенничества» предполагает одновременное наличие давления, возможности и самооправдания: чем больше этих элементов, тем выше вероятность махинаций.

Практическая диагностика строится на «красных флагах»: расхождения между отчётными и фактическими данными, резкие колебания выручки и дебиторской задолженности, рост доли наличных операций, нетипичные контрагенты и транзакции, аномальный рост расходов при стабильной выручке, частые изменения учётной политики. Подозрение вызывают прежде всего документы для внешних пользователей, тогда как управленческий учёт чаще отражает реальное положение дел.

Своевременность выявления особенно важна: схемы развиваются во времени, поэтому устойчивое отклонение связанных показателей надёжнее единичного факта. Основу защиты бизнеса в условиях цифровой трансформации формируют организационные, технические и кадровые меры, усиление внутреннего контроля и процедуры расследования.

Методы распознавания и противодействия.

Методы распознавания финансовых махинаций делят на аналитические, цифровые и организационно-правовые.

Аналитические методы основаны на изучении финансовой отчётности и поиске признаков искажений. Ключевой – коэффициентный метод: наиболее значимы отношение общего долга к капиталу, дебиторской задолженности к продажам и Z-балл; финансовое неблагополучие повышает вероятность мошеннической отчётности. Дополняют его статистические методы и машинное обучение, автоматизирующие выявление аномалий и адаптированные к российскому регулированию.

Цифровые методы используют Big Data и ИИ. В Росфинмониторинге это позволяет выявлять сомнительные операции и прогнозировать угрозы. Для детекции в реальном времени применяют нейросети (LSTM, GRU, Transformer, графовые сети, автоэнкодеры): точность достигает 95–98%, снижается число ложных срабатываний, хотя эффективность зависит от данных и задачи.

Организационно-правовые механизмы создают институциональную основу: финансовый мониторинг, нормативное регулирование и взаимодействие госорганов, банков и бизнеса. Предупреждение фиктивных операций эффективно при согласованном государственном и внутреннем контроле.

Рекомендации: мониторинг «красных флагов», сочетание коэффициентного и статистического анализа, цифровая детекция аномалий в реальном времени, усиление внутреннего контроля, обучение персонала и политика экономической безопасности. Ключевое условие – комплексность: отдельные методы фрагментарны, а их интеграция обеспечивает устойчивое выявление мошеннических схем.

Заключение.

Проведённое исследование позволяет сделать ряд выводов. Финансовые махинации представляют собой системную угрозу экономической безопасности и реализуются в разнообразных формах – от фальсификации отчётности и фиктивных операций до мошенничества в платёжной сфере и легализации доходов. Их своевременное распознавание требует понимания мотивации нарушителя и опирается на систему индикаторов, важнейшими из которых являются расхождения отчётных данных, аномалии в структуре задолженности и нетипичные транзакции.

Установлено, что эффективное выявление махинаций достигается только при комплексном подходе. Аналитические методы (коэффициентный анализ, оценка вероятности банкротства) позволяют обнаружить признаки искажений в отчётности; цифровые методы на основе больших данных, машинного обучения и нейросетей обеспечивают детекцию аномалий, в том числе в режиме реального времени; организационно-правовые механизмы финансового мониторинга и внутреннего контроля формируют институциональную основу противодействия. Согласованное применение всех трёх групп методов, а также постоянное обновление инструментов детекции в ответ на эволюцию мошеннических схем является необходимым условием устойчивой защиты финансовых операций и обеспечения экономической безопасности.

Список литературы

1. Детекция мошенничества в транзакциях в реальном времени: нейросети для поиска аномалий и смены поведенческих паттернов клиента / А. Ю. Аджиева, А. Д. Данилов, Д. Р. Бесшапошников, И. В. Виноградов // Инновационная экономика: информация, аналитика, прогнозы. – 2026. – № 1. – С. 81–87.
2. Архитектурные решения в задаче выявления мошенничества при анализе информационных потоков в экономике / А. А. Грушо, М. И. Забежайло, Н. А. Грушо, Е. Е. Тимонина // Информатика и её применения. – 2019. – Т. 13, № 2. – С. 22–28.
3. Методы выявления и предотвращения мошенничества в системе бухгалтерского учёта / И. А. Бабалыкова, Д. Д. Вязовкин, П. А. Емельянова, А. А. Рау // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2021. – № 169. – С. 222–234. – DOI 10.21515/1990-4665-169-019 (дата обращения: 13.10.2026). – Текст : электронный.
4. Выжитович, А. М. Методические и практические аспекты применения искусственного интеллекта в деятельности Росфинмониторинга / А. М. Выжитович, Я. О. Каменева, О. В. Панагушина // Сибирская финансовая школа. – 2025. – № 3. – С. 58–65.