УДК 336: 343

Современные и традиционные методы выявления финансового мошенничества: сравнительный анализ инноваций и проверенных практик

П.Ю. Леонов
к.э.н., доцент кафедры финансового мониторинга НИЯУ МИФИ, Москва
Email: PYLeonov@mephi.ru
Е.Р. Мысева
старший преподаватель кафедры финансового мониторинга
НИЯУ МИФИ, Москва
Email: ERMyseva@mephi.ru
В.А. Романовский
ассистент кафедры финансового мониторинга НИЯУ МИФИ, Москва
Email: VARomanovskii@mephi.ru

Аннотация: *Данная статья посвящена сравнительному анализу инновационных и традиционных подходов в выявлении мошеннических действий в финансовом секторе. Выявлены достоинства и недостатки современных и традиционных методов.*

Ключевые слова: *мошенничество, выявление мошенничества, финансовое мошенничество, анализ, машинное обучение, искусственный интеллект, блокчейн*

Modern and traditional methods of detection detection: a comparative analysis of innovations and proven practices

P.Y. Leonov
Ph.D. in Economics, Associate Professor, Financial Monitoring Department
NRNU MEPhI, Moscow
Email: PYLeonov@mephi.ru
E.R. Myseva
Senior Lecturer, Financial Monitoring Department
NRNU MEPhI, Moscow
Email: ERMyseva@mephi.ru
V.A. Romanovsky
Assistant of the Financial Monitoring Department
NRNU MEPhI, Moscow
Email: VARomanovskii@mephi.ru

Abstract: *This article is devoted to a comparative analysis of innovative and traditional approaches in detecting fraudulent activities in the financial sector. The advantages and disadvantages of modern and traditional methods are identified.*

Keywords: *fraud, fraud detection, financial fraud, analysis, machine learning, artificial intelligence, blockchain*

Современный финансовый рынок можно охарактеризовать высокой скоростью развития и большим количеством разнообразных транзакций, что создает благоприятные условия для мошеннических действий. Согласно статистике, каждый день во всём мире регистрируются около 500 тысяч различных случаев финансовых махинаций. Наиболее распространены среди них это мошенничество с банковскими картами, подделка документов, мошеннические операции в электронной коммерции и так далее. Мошенничество может проявляться во многих формах и влиять на все сферы бизнеса. Исследования, которые провели PricewaterhouseCoopers в 2024 г., показывает, что более 60% организаций понесли финансовые потери, связанные с мошенничеством, причём почти 30% сообщили об убытках более 1 000 000 $. 25% заявили, что мошенничество нарушило их работу, то есть пострадали внутренние бизнес-процессы организации. 20% отметили падение морального духа сотрудников, то есть появилось необходимость улучшения микроклимата кампании. По мере развития финансовой области и мер защиты, активно развиваются мошеннические схемы в сети, которые приходятся на хакеров (порядка 30%). В данной статье будут рассмотрены не только традиционные методы выявления финансовые мошенничества, но и современные.

Традиционные методы обнаружения мошенничества в финансовых операциях включают различные подходы и техники, которые применяются для выявления подозрительных действий. Эти методы могут быть как ручными, так и автоматизированными, и они часто основываются на правилах и алгоритмах, разработанных на основе исторических данных.

Далее рассматриваются основные традиционные методы:

1. Правила и пороговые значения

Фиксированные правила: Аудиторы и аналитики разрабатывают набор правил, которые определяют, какие транзакции считаются подозрительными. Например, если сумма транзакции превышает определенный порог, она может быть помечена для дальнейшего анализа.

Пороговые значения: Установление пороговых значений для различных параметров (например, частота транзакций, сумма, географическое местоположение) позволяет выявлять аномалии.

2. Анализ исторических данных

Сравнительный анализ: Сравнение текущих транзакций с историческими данными позволяет выявлять отклонения от нормального поведения.

Например, если клиент обычно совершает небольшие покупки, а затем делает крупную транзакцию, это может вызвать подозрения.

Тренды и паттерны: Анализ трендов в поведении клиентов может помочь выявить изменения, которые могут указывать на мошенничество.

3. Методы статистического анализа

Регрессионный анализ: используется для выявления взаимосвязей между различными переменными и определения, какие из них могут указывать на мошеннические действия.

Кластерный анализ: позволяет группировать транзакции по схожим характеристикам и выявлять аномалии в группах, которые могут указывать на мошенничество.

4. Мониторинг транзакций в реальном времени

Системы мониторинга: когда происходит транзакция, например, покупка по кредитной карте или онлайн-перевод, данные быстро фиксируются. Затем они отправляются в систему мониторинга. Затем эта система применяет ряд сложных алгоритмов для анализа данных в реальном времени. Эти алгоритмы учитывают различные факторы. Они учитывают сумму транзакции и место ее совершения. Они также изучают прошлое поведение клиента. Наконец, они проверяют наличие шаблонов или тенденций, которые могут указывать на мошенничество. Система сравнивает текущую транзакцию с обширной базой данных известных шаблонов мошенничества и использует методы машинного обучения для выявления новых и появляющихся шаблонов мошенничества. Как только система обнаруживает потенциально мошенническую транзакцию, она отправляет оповещение группе по обнаружению мошенничества организации. Затем эта группа может подробно рассмотреть транзакцию, собрать дополнительную информацию при необходимости и принять обоснованное решение о том, следует ли заблокировать транзакцию или разрешить ее продолжение. Весь этот процесс происходит в течение нескольких секунд, гарантируя, что мошеннические действия будут идентифицированы и устранены в режиме реального времени.

Сигналы тревоги: во время обнаружения подозрительных транзакций система будет автоматически отправлять уведомления соответствующим специалистам для дальнейшего расследования.

5. Проверка идентификации и аутентификации

Многофакторная аутентификация: Использование нескольких методов аутентификации (например, пароли, SMS-коды, биометрические данные) для подтверждения личности клиента может помочь предотвратить мошенничество.

Проверка личности: Регулярная проверка идентификации клиентов и их транзакционной активности помогает выявлять подозрительные действия.

6. Обучение и осведомленность сотрудников

Обучение персонала: Обучение сотрудников методам выявления мошенничества и повышению осведомленности о потенциальных рисках может помочь в раннем обнаружении подозрительных действий.

Создание культуры безопасности: Формирование культуры безопасности в организации, где сотрудники активно сообщают о подозрительных действиях, может значительно повысить эффективность обнаружения мошенничества.

В таблице 1 представлены достоинства и недостатки традиционных методов.

Таблица 1 – Достоинства и недостатки традиционных методов

Достоинства традиционных методов	Недостатки традиционных методов
Простота реализации: Традиционные методы, такие как правила и пороговые значения, легко разрабатывать и внедрять в существующие системы. Они не требуют сложных алгоритмов или значительных вычислительных ресурсов.	**Ложные срабатывания**: Установленные правила могут приводить к высокому уровню ложных срабатываний, когда законные транзакции помечаются как подозрительные. Это может вызывать неудобства для клиентов и увеличивать нагрузку на службы безопасности.
Простота реализации: Традиционные методы, такие как правила и пороговые значения, легко разрабатывать и внедрять в существующие системы. Они не требуют сложных алгоритмов или значительных вычислительных ресурсов.	**Неполнота и ограниченность**: Традиционные методы могут не охватывать все возможные схемы мошенничества, особенно если мошенники используют новые методы, которые не были учтены при разработке правил.
Быстрота обработки: Эти методы могут быстро обрабатывать транзакции в реальном времени, что позволяет оперативно выявлять подозрительные операции и минимизировать потенциальные убытки.	**Отсутствие адаптивности**: Статические правила могут не адаптироваться к изменениям в поведении клиентов или новым схемам мошенничества, что делает их менее эффективными со временем.
Прозрачность и интерпретируемость: Правила и пороговые значения легко объяснить и интерпретировать. Это позволяет аудиторам и сотрудникам службы безопасности понимать, почему транзакция была помечена как подозрительная.	**Сложность настройки**: Установление правильных пороговых значений и правил может быть сложным и требовать глубокого анализа данных и понимания поведения клиентов.
Низкие затраты на внедрение: Внедрение традиционных методов может потребовать меньше затрат на	**Ограниченная способность к выявлению сложных схем**:

технологии и обучение по сравнению с более сложными методами, такими как машинное обучение.	Традиционные методы могут не справляться с более сложными схемами мошенничества, которые требуют анализа взаимосвязей между различными транзакциями и пользователями.
Подход к известным схемам мошенничества: Традиционные методы хорошо работают для выявления известных схем мошенничества, которые можно легко закодировать в правилах.	

Современные методы

1. Искусственный интеллект и машинное обучение

Эти технологии позволяют анализировать большие объемы данных и выявлять аномалии в транзакциях. Алгоритмы машинного обучения могут обучаться на исторических данных, чтобы распознавать паттерны мошенничества и адаптироваться к новым схемам, что делает их более эффективными по сравнению с традиционными методами.

2. Мониторинг транзакций в реальном времени

Системы, которые отслеживают каждую операцию в реальном времени, могут мгновенно блокировать подозрительные транзакции. Это позволяет предотвратить финансовые потери до того, как они произойдут, и обеспечивает более высокий уровень безопасности для клиентов.

3. Анализ поведения пользователей

Этот метод включает сравнение текущих действий клиентов с их историей транзакций. Выявление необычных паттернов, таких как резкое изменение привычек покупок, может сигнализировать о мошенничестве. Такой подход помогает выявлять потенциальные угрозы на ранних стадиях.

4. Многофакторная аутентификация

Использование нескольких методов подтверждения личности (например, пароли, SMS-коды, биометрические данные) значительно усложняет доступ мошенников к счетам. Это повышает уровень безопасности и защищает клиентов от несанкционированных транзакций.

5. Технология 3D Secure

Этот протокол добавляет дополнительный уровень безопасности при онлайн-платежах, требуя подтверждения от владельца карты. Это может включать ввод одноразового кода или ответ на контрольный вопрос, что снижает риск мошенничества при интернет-покупках.

6. Системы антифрода

Специальные программы, которые анализируют транзакции и выявляют мошеннические схемы, основываясь на заранее заданных правилах и алгоритмах. Эти системы могут автоматически помечать подозрительные операции для дальнейшего анализа.

7. Блокчейн-технологии

Использование децентрализованных реестров обеспечивает прозрачность и неизменность транзакций, что затрудняет мошеннические действия. Блокчейн позволяет отслеживать каждую транзакцию и обеспечивает высокий уровень доверия к данным.

8. Анализ социальных сетей

Изучение взаимодействий и связей между пользователями может помочь выявить мошеннические схемы, основанные на коллаборации злоумышленников. Этот метод позволяет анализировать поведение групп пользователей и выявлять аномалии.

9. Системы предупреждения о мошенничестве

Эти системы автоматически уведомляют клиентов о подозрительных действиях на их счетах, что позволяет быстро реагировать на потенциальные угрозы. Уведомления могут быть отправлены через SMS, электронную почту или мобильные приложения.

10. Обучение сотрудников

Регулярные тренинги и семинары для работников финансовых учреждений помогают повысить осведомленность о новых методах мошенничества и способах их предотвращения. Обучение сотрудников позволяет создать культуру безопасности в организации.

11. Использование биометрических данных

Внедрение технологий распознавания лиц, отпечатков пальцев или радужной оболочки глаза для аутентификации пользователей значительно повышает уровень безопасности. Биометрические данные сложно подделать, что делает их надежным средством защиты.

12. Анализ больших данных

Обработка и анализ больших объемов информации из различных источников позволяет выявлять скрытые паттерны и тенденции, связанные с мошенничеством. Этот метод помогает финансовым учреждениям принимать более обоснованные решения на основе данных.

Современные методы обнаружения мошенничества в финансовых операциях предлагают множество преимуществ, но также имеют и свои недостатки. В таблице 2 представлены достоинства и недостатки перечисленных выше современных методов.

Таблица 2 – Достоинства и недостатки современных методов

Искусственный интеллект и машинное обучение	
Достоинства	**Недостатки**
Адаптивность: Алгоритмы могут обучаться на новых данных и адаптироваться к изменяющимся схемам мошенничества.	**Необходимость в больших данных**: для эффективного обучения требуется большое количество размеченных данных.

Высокая точность: Способность выявлять сложные паттерны и аномалии, которые могут быть неочевидны для традиционных методов.	**Сложность интерпретации**: Результаты могут быть трудны для понимания, что затрудняет объяснение клиентам и регуляторам.
Мониторинг транзакций в реальном времени	
Достоинства	**Недостатки**
Мгновенная реакция: позволяет быстро блокировать подозрительные транзакции, предотвращая финансовые потери. **Повышение безопасности**: обеспечивает постоянный контроль за транзакциями.	**Ложные срабатывания**: Высокий уровень ложных срабатываний может привести к неудобствам для клиентов и увеличению нагрузки на службы поддержки. **Затраты на инфраструктуру**: требует значительных инвестиций в технологии и системы мониторинга.
Анализ поведения пользователей	
Достоинства	**Недостатки**
Индивидуальный подход: позволяет выявлять аномалии на основе уникального поведения каждого клиента. **Раннее выявление**: помогает обнаруживать мошенничество на ранних стадиях, что снижает риски.	**Сложность настройки**: требует тщательной настройки и анализа, чтобы правильно определить нормальное поведение. **Чувствительность к изменениям**: Изменения в поведении клиентов (например, поездки или покупки) могут привести к ложным срабатываниям.
Многофакторная аутентификация	
Достоинства	**Недостатки**
Увеличение безопасности: Сложность доступа для мошенников значительно возрастает. **Гибкость**: можно использовать различные методы аутентификации в зависимости от ситуации.	**Неудобство для пользователей**: Дополнительные шаги аутентификации могут вызывать недовольство клиентов. **Зависимость от технологий**: Необходимость в надежных устройствах и соединениях для выполнения аутентификации.
Технология 3D Secure	
Достоинства	**Недостатки**
Дополнительный уровень безопасности: защищает онлайн-транзакции, требуя подтверждения от владельца карты. **Снижение мошенничества**: уменьшает количество мошеннических транзакций при онлайн-покупках.	**Сложность для пользователей**: может вызывать неудобства, если процесс подтверждения слишком сложен или медлителен. **Не все продавцы поддерживают**: некоторые онлайн-магазины могут не использовать 3D Secure, что снижает его эффективность.
Системы антифрода	
Достоинства	**Недостатки**

Снижение мошенничества: Эффективные антифрод-системы значительно уменьшают количество мошеннических транзакций, что защищает финансовые учреждения от убытков. **Защита данных клиентов**: Системы помогают предотвратить утечку конфиденциальной информации, что повышает уровень доверия клиентов к банкам и другим финансовым организациям. **Анализ больших данных**: Современные антифрод-системы используют технологии машинного обучения и анализа больших данных для выявления сложных схем мошенничества, что позволяет им адаптироваться к новым угрозам. **Мониторинг в реальном времени**: Возможность отслеживания транзакций в режиме реального времени позволяет быстро реагировать на подозрительные действия и предотвращать финансовые потери. **Автоматизация процессов**: Системы могут автоматизировать многие процессы, связанные с проверкой транзакций, что снижает нагрузку на сотрудников и повышает эффективность работы.	**Высокие затраты на внедрение**: Разработка и внедрение антифрод-систем требуют значительных финансовых вложений, что может быть проблемой для малых и средних предприятий. **Ложные срабатывания**: Высокий уровень ложных срабатываний может привести к неудобствам для клиентов, когда законные транзакции блокируются, что требует дополнительного времени и ресурсов для их разблокировки. **Сложность настройки**: Настройка антифрод-системы под конкретные условия и требования бизнеса может быть сложной задачей, требующей глубоких знаний и опыта. **Зависимость от технологий**: Эффективность антифрод-системы может зависеть от качества используемых технологий и алгоритмов, что может привести к уязвимостям. **Человеческий фактор**: несмотря на автоматизацию, окончательное решение о мошенничестве часто остается за сотрудниками, что может привести к ошибкам в интерпретации данных.
Блокчейн-технологии	
Достоинства	**Недостатки**
Прозрачность и неизменность: обеспечивает высокий уровень доверия к данным и защищает от подделок. **Децентрализация**: уменьшает риски, связанные с централизованными системами.	**Сложность внедрения**: Интеграция блокчейн-технологий в существующие системы может быть сложной и затратной. **Ограниченная скорость транзакций**: Некоторые блокчейн-системы могут иметь ограничения по скорости обработки транзакций.
Анализ социальных сетей	
Достоинства	**Недостатки**
Выявление скрытых паттернов: Анализ социальных сетей позволяет выявлять сложные	**Сложность интерпретации:** Результаты анализа могут быть сложными для интерпретации, особенно

взаимосвязи и паттерны, которые могут указывать на мошеннические действия, такие как коллаборация между злоумышленниками. **Обнаружение аномалий**: Метод помогает выявлять аномалии в поведении пользователей, которые могут быть связаны с мошенничеством, например, резкие изменения в активности или необычные связи между участниками. **Улучшение понимания схем мошенничества**: SNA позволяет глубже понять, как мошеннические схемы функционируют, что помогает в разработке более эффективных стратегий предотвращения и обнаружения мошенничества. **Интеграция с другими данными**: Анализ социальных сетей может быть интегрирован с другими источниками данных (например, транзакционными данными), что позволяет создать более полное представление о поведении пользователей. **Визуализация данных**: SNA предоставляет инструменты для визуализации сетевых структур, что помогает аналитикам и специалистам по безопасности лучше понимать взаимосвязи и выявлять потенциальные угрозы.	если сеть имеет сложную структуру. Это может затруднить принятие решений на основе полученных данных. **Необходимость в больших объемах данных:** Для эффективного анализа требуется значительное количество данных о взаимодействиях между пользователями, что может быть сложно собрать и обработать. **Чувствительность к шуму:** Анализ может быть подвержен влиянию шумовых данных и ложных связей, что может привести к неправильным выводам. **Зависимость от качества данных:** Эффективность анализа социальных сетей зависит от качества и полноты данных. Неполные или искаженные данные могут привести к ошибочным результатам. **Этические и правовые вопросы:** Использование данных из социальных сетей может вызывать этические и правовые вопросы, связанные с конфиденциальностью и защитой данных пользователей.
Системы предупреждения о мошенничестве	
Достоинства	**Недостатки**

Мгновенная реакция: Системы могут быстро уведомлять клиентов о подозрительных транзакциях, что позволяет им немедленно реагировать и предотвращать возможные финансовые потери. **Повышение осведомленности клиентов**: Уведомления о подозрительных действиях помогают клиентам быть более внимательными к своим счетам и транзакциям, что может снизить риск мошенничества. **Автоматизация процессов**: Системы автоматизируют процесс мониторинга и уведомления, что снижает нагрузку на сотрудников и позволяет им сосредоточиться на более сложных задачах. **Улучшение репутации**: Эффективные системы предупреждения о мошенничестве могут повысить доверие клиентов к финансовым учреждениям, так как они демонстрируют активные меры по защите их средств. **Снижение финансовых потерь**: Быстрое уведомление о подозрительных действиях может помочь предотвратить мошеннические транзакции, что снижает финансовые потери как для клиентов, так и для учреждений.	**Ложные срабатывания** Высокий уровень ложных срабатываний может привести к тому, что законные транзакции будут помечены как подозрительные, что вызывает неудобства для клиентов и увеличивает нагрузку на службы поддержки. **Зависимость от технологий**: Эффективность систем зависит от качества используемых алгоритмов и технологий. Неправильные настройки могут привести к пропуску мошеннических действий или к чрезмерному количеству ложных тревог. **Необходимость в постоянном обновлении**: Системы требуют регулярного обновления и настройки, чтобы оставаться эффективными в условиях постоянно меняющихся схем мошенничества. **Чувствительность к изменениям в поведении клиентов**: Изменения в привычках клиентов (например, поездки или крупные покупки) могут привести к ложным срабатываниям, что требует дополнительного анализа и вмешательства. **Потенциальные проблемы с конфиденциальностью**: Уведомления о подозрительных действиях могут вызывать вопросы о конфиденциальности и защите данных клиентов, особенно если информация передается через небезопасные каналы.
Обучение сотрудников	
Достоинства	**Недостатки**
Повышение осведомленности: Обучение помогает сотрудникам лучше понимать схемы мошенничества и методы, которые используют злоумышленники, что позволяет им быть более внимательными к потенциальным угрозам.	**Затраты на обучение**: Проведение тренингов и семинаров может потребовать значительных финансовых и временных ресурсов, что может быть проблемой для малых и средних предприятий. **Необходимость регулярного обновления**:

Улучшение навыков анализа: Сотрудники получают навыки анализа данных и выявления аномалий, что позволяет им более эффективно реагировать на подозрительные транзакции. **Создание культуры безопасности**: Регулярное обучение способствует формированию культуры безопасности в организации, где сотрудники активно участвуют в предотвращении мошенничества и сообщают о подозрительных действиях. **Снижение финансовых потерь**: Обученные сотрудники могут быстрее выявлять и предотвращать мошеннические действия, что снижает финансовые потери как для клиентов, так и для учреждения. **Адаптация к новым угрозам**: Обучение позволяет сотрудникам быть в курсе новых схем мошенничества и технологий, что помогает им адаптироваться к изменяющимся условиям.	Схемы мошенничества постоянно меняются, поэтому обучение должно проводиться регулярно, что требует дополнительных затрат и усилий. **Разные уровни восприятия**: Сотрудники могут иметь разные уровни понимания и восприятия информации, что может привести к неравномерному уровню подготовки и эффективности. **Человеческий фактор**: Даже обученные сотрудники могут допускать ошибки в интерпретации данных или принятии решений, что может привести к пропуску мошеннических действий. **Сопротивление изменениям**: Некоторые сотрудники могут быть не готовы к изменениям в процессах или технологиях, что может затруднить внедрение новых методов и подходов.
Использование биометрических данных	
Достоинства	**Недостатки**
Высокий уровень безопасности: Биометрические данные уникальны для каждого человека, что делает их трудными для подделки. Это значительно повышает уровень безопасности по сравнению с традиционными методами аутентификации, такими как пароли или PIN-коды. **Удобство для пользователей**: Биометрическая аутентификация часто более удобна для пользователей, так как не требует запоминания паролей или ввода длинных кодов. Например, пользователи могут просто прикоснуться к сканеру отпечатков пальцев или взглянуть в камеру для распознавания лиц.	**Риски утечки данных**: Биометрические данные, если они будут украдены или скомпрометированы, могут быть использованы злоумышленниками для доступа к учетным записям. В отличие от паролей, биометрические данные не могут быть изменены, что делает их более уязвимыми. **Сложность защиты данных**: Хранение и обработка биометрических данных требуют высоких стандартов безопасности и защиты, что может быть сложно и дорого для организаций. **Проблемы с точностью**: Биометрические системы могут давать ложные срабатывания (ошибочно

Снижение случаев мошенничества: Использование биометрических данных может значительно снизить риск мошенничества, так как злоумышленникам будет сложнее получить доступ к учетным записям, используя поддельные или украденные данные. **Быстрая аутентификация**: Биометрические системы могут обеспечивать быструю аутентификацию, что особенно важно в условиях, когда требуется мгновенный доступ, например, при проведении финансовых транзакций. **Устойчивость к забыванию**: В отличие от паролей, биометрические данные не могут быть забыты, что снижает количество обращений в службу поддержки для восстановления доступа.	идентифицируя пользователя) или пропуски (не распознавая законного пользователя). Это может привести к неудобствам для клиентов и дополнительным затратам на поддержку. **Этические и правовые вопросы**: Использование биометрических данных может вызывать опасения по поводу конфиденциальности и защиты личной информации. Необходимость получения согласия пользователей на сбор и использование их биометрических данных также может быть проблемой. **Зависимость от технологий**: Эффективность биометрических систем зависит от качества используемых технологий и оборудования. Неправильная настройка или устаревшее оборудование могут снизить уровень безопасности.
Анализ больших данных	
Достоинства	**Недостатки**
Выявление скрытых паттернов: Анализ больших данных позволяет выявлять сложные и скрытые паттерны, которые могут указывать на мошеннические действия. Это может включать аномалии в транзакциях, которые не были бы заметны при использовании традиционных методов. **Прогнозирование мошенничества**: С помощью предиктивной аналитики можно прогнозировать потенциальные мошеннические действия на основе исторических данных. Это позволяет финансовым учреждениям заранее принимать меры для предотвращения мошенничества. **Улучшение принятия решений**: Анализ больших данных предоставляет более полное представление о поведении клиентов и транзакциях, что помогает руководству принимать более	**Сложность обработки**: Обработка и анализ больших объемов данных требуют значительных вычислительных ресурсов и сложных алгоритмов, что может быть дорого и сложно для внедрения. **Необходимость в качественных данных**: Эффективность анализа больших данных зависит от качества и полноты данных. Неполные или искаженные данные могут привести к неправильным выводам и ошибкам в интерпретации. **Проблемы с конфиденциальностью**: Сбор и анализ больших объемов данных могут вызывать опасения по поводу конфиденциальности и защиты личной информации клиентов. Необходимость соблюдения законодательства о защите данных (например, GDPR) может усложнить процесс. **Человеческий фактор**:

обоснованные решения и разрабатывать стратегии по борьбе с мошенничеством. **Автоматизация процессов**: Современные инструменты анализа больших данных могут автоматизировать процессы мониторинга и выявления мошенничества, что снижает нагрузку на сотрудников и повышает эффективность работы. **Адаптивность**: Системы, основанные на анализе больших данных, могут адаптироваться к изменениям в поведении клиентов и новым схемам мошенничества, что делает их более эффективными в долгосрочной перспективе.	Несмотря на автоматизацию, окончательное решение о мошенничестве часто остается за сотрудниками, что может привести к ошибкам в интерпретации данных и принятию неверных решений. **Зависимость от технологий**: Эффективность анализа больших данных зависит от качества используемых технологий и инструментов. Устаревшие или неправильно настроенные системы могут снизить уровень безопасности и эффективности.

Несмотря на наличие традиционных методов обнаружения мошеннических действий, таких как аудит и проверка документов, современные технологии предоставляют новые возможности для более эффективного выявления и предотвращения финансовых махинаций. Инновационные подходы, основанные на анализе больших данных, машинном обучении и искусственном интеллекте, позволяют значительно повысить скорость и точность обнаружения аномалий в финансовых операциях. Однако, несмотря на достижения в этой области, необходимо продолжать совершенствование методов борьбы с мошенничеством, учитывая постоянно меняющиеся схемы и технологии, используемые мошенниками.

Для улучшения системы обнаружения мошенничества в финансовой сфере рекомендуется внедрить комплексный подход, который объединяет как традиционные, так и современные методы. Важно развивать межведомственное сотрудничество между финансовыми учреждениями, правоохранительными органами и государственными структурами для обмена информацией и лучшими практиками. Также следует инвестировать в обучение и повышение квалификации сотрудников, чтобы они могли эффективно использовать новые технологии и инструменты для выявления мошенничества.

Список использованных источников:

1. Авагян А.А., Мирзоян М.А., Кабанова Н.А. Проблема финансовых пирамид и современных способов мошенничества на финансовых и

криптовалютных рынках // Вестник евразийской науки. 2024. Т. 16. № S4 (5). EDN: https://www.elibrary.ru/AXKCIF.

2. Басова М. Е. Финансовое мошенничество / М. Е. Басова // Право и экономика. – 2020. – № 2. – С. 72-76.

3. Белов Р.А. Использование искусственного интеллекта в бухгалтерском учете и аудите: новые возможности и вызовы // Научные высказывания. 2023. №8 (32). С. 51-55. 2.

4. Боргардт Е.А., Бобель Д.Н. Технологии искусственного интеллекта в системе управления качеством // Международный журнал гуманитарных и естественных наук. 2021. № 8.1. С. 178-180.

5. Ермолаев Е.А., Завьялов Ю.С. Манипулирование на финансовом рынке как форма инвестиционного мошенничества (признаки и определение) // Финансовый бизнес. 2019. № 6 (203). С. 16-24. EDN: https://www.elibrary.ru/KKBHGX.

6. Кибермошенничество: портрет пострадавшего/ Банк России. [Электронный ресурс] – Режим доступа: https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (Дата обращения 20.05.2025).

7. Опрос PwC: российские компании стали чаще сталкиваться с экономическими преступлениями [Электронный ресурс] – Режим доступа: https://www.banki.ru/news/lenta/?id=10464980 (Дата обращения 20.05.2025).

8. PwC [Электронный ресурс] – Режим доступа: https://www.pwc.com/gx/en.html (Дата обращения 20.05.2025).

Дополнительная информация

Исследование выполнено за счет гранта Российского научного фонда № 25-28-00901 (https://rscf.ru/project/25-28-00901/) по проекту «Повышение эффективности финансового аудита с помощью технологий больших данных».