ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

DOI: 10.18137/RNU.V9187.25.01.P.70 УДК 004.89

Абдурахман Джамал Джама
аспирант, Финансовый университет при Правительстве Российской Федерации, Москва.
Электронный адрес: jamaljolevas14psg@gmail.com
Djamal Djama Abdourahman
Postgraduate, Financial University under the Government of the Russian Federation, Moscow.
E-mail address: jamaljolevas14psg@gmail.com

УЛУЧШЕНИЕ ОБНАРУЖЕНИЯ МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ С ПОМОЩЬЮ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

Аннотация. Мошенничество с банковскими картами является распространенной и усугубляющейся проблемой в финансовом секторе, требующей инновационных решений для точного и эффективного обнаружения. Традиционные методы обнаружения мошенничества, во многих случаях эффективны, но сегодня они сталкиваются с масштабируемостью и сложностью современных схем мошенничества. Недавние достижения в области квантовых вычислений открыли новые пути для решения этих проблем. В статье представлен квантовый анализ потоков транзакций (QTFA) – инновационная квантовая методология для улучшения обнаружения мошенничества с банковскими картами. QTFA использует принципы квантовой механики, такие как суперпозиция, запутанность и квантовая оптимизация, для моделирования и анализа потоков транзакций в квантовой сети. Представляя транзакции как квантовые состояния, а их отношения как запутанности, QTFA обеспечивает точное обнаружение аномалий с помощью квантовых измерений. Экспериментальные результаты показывают, что QTFA превосходит классические методы машинного обучения, такие как случайные леса и опорные векторные машины (SVM), достигая 98-процентной точности (accuracy), 10-процентного снижения ложных срабатываний и улучшенной полноты (recall). В статье также рассматривается интеграция QTFA в реальные системы, подчеркивается ее потенциал для революционных изменений в обнаружении мошенничества, а также определяются текущие ограничения и направления будущих исследований.

Ключевые слова: мошенничество с банковскими картами, квантовые вычисления, квантовая суперпозиция, квантовая запутанность, квантовый анализ потока транзакций, машинное обучение.

Для цитирования: *Абдурахман Д.Д.* Улучшение обнаружения мошенничества с банковскими картами с помощью квантовых вычислений // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ, управление. 2025. № 1. С. 70 – 80. DOI: 10.18137/RNU.V9187.25.01.P.70

IMPROVING CREDIT CARD FRAUD DETECTION THROUGH QUANTUM COMPUTING

Abstract. Credit card fraud is a pervasive and evolving challenge in the financial sector, necessitating innovative solutions for accurate and efficient detection. Traditional fraud detection methods, while effective in many cases, often struggle with scalability and the complexity of modern fraud patterns. Recent advancements in quantum computing have opened new avenues for tackling these problems. This paper introduces *Quantum Transaction Flow Analysis (QTFA)*, a novel and innovative quantum-based methodology for enhancing credit card fraud detection. QTFA leverages the principles of quantum mechanics, such as superposition, entanglement, and quantum optimization, to model and analyze transaction flows within

a quantum network. By representing transactions as quantum states and their relationships as entanglements, QTFA enables precise anomaly detection through quantum measurement. Experimental results demonstrate that QTFA outperforms classical machine learning methods, such as Random Forests and Support Vector Machines (SVMs), achieving a 98 % accuracy rate, a 10 % reduction in false positive rates, and improved recall. This paper also explores the integration of QTFA into real-world systems, highlighting its potential to revolutionize fraud detection while identifying current limitations and directions for future research.

Keywords: bank card fraud, quantum computing, quantum superposition, quantum entanglement, quantum transaction flow analysis, machine learning.

For citation: Abdourahman D.D. (2025) Improving Credit Card Fraud Detection Through Quantum Computing. *Vestnik of Russian New University. Series: Complex Systems: Models, analysis, management*. No. 1. Pp. 70 – 80. DOI: 10.18137/RNU.V9187.25.01.P.70 (In Russian).

Введение

Обнаружение мошенничества с банковскими картами является важнейшей задачей в современной финансовой экосистеме. Традиционные системы обнаружения мошенничества, которые обычно полагаются на алгоритмы машинного обучения, статистическое обнаружение аномалий или подходы на основе правил, сталкиваются со значительными ограничениями при работе с большими объемами данных транзакций, нелинейными отношениями между различными характеристиками транзакций и всё более сложными методами мошенничества [1]. Традиционным системам всё труднее обнаружить сложные закономерности мошеннического поведения в режиме реального времени, что приводит к ложным срабатываниям (необоснованное оповещение о мошенничестве) либо необнаружению мошенничества.

Квантовые вычисления (*Quantum computing*) с их способностью обрабатывать информацию способами, принципиально отличными от классических систем, предлагают многообещающий путь для решения этих проблем [2]. Квантовая механика делает возможными такие явления, как суперпозиция (superposition) и запутанность (entanglement), которые позволяют квантовым системам исследовать несколько возможностей одновременно и моделировать сложные взаимодействия более эффективно. Используя эти возможности, квантовые вычисления могут обеспечить преобразующий подход к обнаружению мошенничества с банковскими картами.

В статье представлена новая квантовая методология обнаружения мошенничества в транзакциях по банковским картам – *Quantum Transaction Flow Analysis (QTFA)*. QTFA использует квантовые сети для моделирования потока транзакций и выявления аномалий, которые могут указывать на мошенническую деятельность. Используя квантовую механику для представления сложных взаимосвязей между транзакциями, QTFA предлагает более точную, масштабируемую и работающую в режиме реального времени альтернативу традиционным системам обнаружения мошенничества.

В статье дается всестороннее описание QTFA, ее теоретической основы, математической формулировки. Кроме того, показано, как QTFA можно применять для обнаружения мошенничества в реальном мире, иллюстрируя ее потенциал для повышения эффективности и результативности систем обнаружения мошенничества в финансовом секторе.

Связанные исследования

Обнаружение мошенничества с банковскими картами было тщательно изучено, что привело к разработке многочисленных методов, призванных бороться с меняющейся

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление», выпуск 1 за 2025 год

природой мошеннической деятельности. Классические подходы на основе правил и статистических методов легли в основу механизмов раннего обнаружения. Эти системы полагались на фиксированные пороговые значения и предопределенные правила для выявления аномалий в шаблонах транзакций. Однако они с трудом приспосабливались к динамическим стратегиям, используемым мошенниками, что часто приводило к высоким показателям ложных срабатываний и ограничению масштабируемости. Позднее применение методов машинного обучения стало более распространенным при обнаружении мошенничества; использовались такие алгоритмы, как деревья решений, случайные леса и машины опорных векторов. Эти методы анализируют большие объемы исторических данных транзакций для изучения шаблонов, указывающих на мошенническую деятельность. Кроме того, модели глубокого обучения, включая рекуррентные нейронные сети (RNN) и сверточные нейронные сети (CNN), продемонстрировали особый успех в выявлении временных и пространственных связей в данных транзакций [3]. Несмотря на эти достижения, эти методы сталкиваются с проблемами интерпретируемости и вычислительной эффективности, особенно при применении к несбалансированным наборам данных или крупномасштабным сетям транзакций [4].

Квантовые вычисления стали многообещающей альтернативой для преодоления ограничений классических методов [5]. Недавние исследования посвящены использованию алгоритмов квантового машинного обучения, таких как квантовые машины опорных векторов (QSVM) и квантовые нейронные сети (QNN), для решения проблем масштабируемости и повышения скорости вычислений [6].

В статье предложен инновационный метод *Quantum Transaction Flow Analysis (QTFA)* в качестве нового решения для обнаружения мошенничества с банковскими картами.

Методология

Методология квантового анализа потока транзакций (Quantum Transaction Flow Analysis – QTFA) предоставляет инновационную структуру для решения растущей проблемы обнаружения мошенничества с банковскими картами путем интеграции принципов квантовых вычислений. QTFA моделирует транзакции как квантовые состояния, позволяя им существовать в суперпозиции законного и мошеннического поведения. Такое представление обеспечивает многомерный анализ, который недостижим с помощью классических систем. Кодируя отдельные транзакции как квантовые состояния и связные транзакции посредством квантовой запутанности, QTFA раскрывает скрытые связи и закономерности, указывающие на мошенническую деятельность. Этот подход динамического моделирования обеспечивает адаптивность к меняющимся тенденциям мошенничества в реальном времени.

Структура использует сеть квантового потока для захвата и анализа взаимозависимостей между транзакциями. Узлы в сети представляют отдельные транзакции, в то время как взвешенные ребра (weighted edges) обозначают такие связи, как общие идентификаторы или временная близость. Эти веса помогают расставить приоритеты связей для более глубокого анализа. Вся сеть развивается с течением времени, управляемая унитарными операторами, которые включают ожидаемое поведение, полученное из исторических данных. Эта временная эволюция является ключом к обнаружению сложных схем мошенничества, которые используют уязвимости сети.

Оптимизация играет решающую роль в уточнении структуры сети, где используется алгоритм квантовой аппроксимации оптимизации (Quantum Approximate Optimization

Algorithm – QAOA) [7]. Этот гибридный алгоритм итеративно оптимизирует сеть, настраивая параметры, которые минимизируют расхождения между наблюдаемыми и ожидаемыми потоками транзакций. Чередуя квантовые и классические вычислительные слои, QAOA обеспечивает эффективное и точное представление нормального поведения транзакций, позволяя эффективно отмечать отклонения. Наконец, QTFA обнаруживает аномалии с помощью квантовых измерений, сворачивая состояния транзакций в окончательные классификации законных или мошеннических. Этот процесс также учитывает контекстную динамику транзакций, такую как географическое положение или время возникновения, с помощью адаптивных механизмов пороговой обработки. Кроме того, квантовая запутанность еще больше усиливает обнаружение, анализируя корреляции между отмеченными транзакциями, позволяя идентифицировать скоординированные мошеннические схемы. Вместе эти компоненты позиционируют QTFA как преобразующее решение для борьбы с финансовым мошенничеством с беспрецедентной точностью и масштабируемостью.

Имплементация QTFA

Имплементация квантового анализа потока транзакций (QTFA) включает несколько взаимосвязанных этапов, начиная с предварительной обработки данных транзакций, за которыми следует построение квантовой схемы (Quantum circuit) для представления сети потока транзакций. Процесс продолжается применением QAOA (Quantum Approximate Optimization Algorithm) для оптимизации сети и завершается обнаружением аномалий с помощью квантовых измерений.

Предварительная обработка данных

Предварительная обработка данных (Data Preprocessing) транзакций имеет решающее значение для подготовки данных к кодированию в квантовые состояния. Во-первых, необработанные данные проходят тщательную очистку для устранения потенциальных несоответствий, пропущенных значений и шума. Учитывая неоднородную природу наборов данных для обнаружения мошенничества, поступающих из разных источников, таких как платежные системы и платформы электронной коммерции, гармонизация данных имеет решающее значение. Это включает стандартизацию форматов атрибутов с учетом различных масштабов и типов встречающихся данных.

Второй шаг включает нормализацию. Нормализация имеет первостепенное значение для обеспечения того, чтобы каждый атрибут вносил пропорциональный вклад в последующий процесс кодирования квантового состояния. Без нормализации атрибуты с большими масштабами могут непропорционально влиять на квантовое представление, потенциально искажая результаты. Масштабирование всех атрибутов до общего диапазона (например, [0, 1]) позволяет сохранить их относительную важность, совместимость со схемами квантового кодирования. Кроме того, для повышения эффективности применяются методы отбора признаков и снижения размерности, такие как анализ главных компонент (PCA) [8]. Вычислительная сложность снижается за счет выявления и сохранения только наиболее релевантных и информативных атрибутов, что является критическим фактором, учитывая ограничения ресурсов текущего квантового оборудования.

Наконец, предварительно обработанные данные кодируются в квантовое состояние. Амплитудное кодирование отображает атрибуты каждой транзакции на амплиту-

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление», выпуск 1 за 2025 год

ды вектора квантового состояния. Этот подход предлагает компактное и эффективное представление многомерных данных, минимизируя требования к памяти по сравнению с классическими представлениями. Для этой работы используются фреймворки квантового программного обеспечения (Qiskit) для построения этих квантовых состояний на квантовых симуляторах, а затем на реальном квантовом оборудовании.

Построение Quantum Circuit

Quantum circuit (Квантовая схема) образует основу QTFA, представляя сеть потока транзакций в квантовом состоянии. Каждая транзакция отображается на кубит, а отношения между транзакциями, такие как временная близость или сходство в моделях расходов, кодируются с помощью запутывания (entanglement). Первоначально все кубиты помещаются в состояние суперпозиции с использованием Hadamard gates, представленных математически как $|\psi_0\rangle = \boldsymbol{H}^{\otimes n} |\,\mathbf{0}\rangle^{\otimes n}$, где n – количество транзакций, а H обозначает Hadamard gate.

Атрибуты транзакций кодируются в амплитуды квантового состояния с использованием параметризованных вентилей вращения (parameterized rotation gates). Например, вентиль $\boldsymbol{R}_y(\theta)$, который вращает состояние кубита на угол θ, определяется как

$$R_y(\theta) = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix}.$$

Угол θ̂ вычисляется на основе нормализованных атрибутов каждой транзакции. Для моделирования отношений между транзакциями вводится запутанность с использованием *controlled-NOT gates*. Для транзакций с сильными корреляциями создается запутанное состояние $|\psi_{entangled}\rangle = \mathbf{1}/\sqrt{\mathbf{2}}\,(|\mathbf{00}\rangle + |\mathbf{11}\rangle)$, гарантируя, что состояние одного кубита влияет на другой.

Оптимизация квантового потока с помощью QAOA

Для оптимизации сети потока транзакций и выявления аномалий QTFA использует алгоритм приближенной квантовой оптимизации (QAOA). Этот подход попеременно применяет *Cost Hamiltonian* ($\boldsymbol{H}_C$) и *Mixing Hamiltonian* ($\boldsymbol{H}_M$) для итеративного уточнения квантового состояния. *Cost Hamiltonian* (стоимостной гамильтониан) кодирует *цель* минимизации отклонений между наблюдаемыми и ожидаемыми потоками транзакций:

$$H_C = \sum_{e \in E} \left(f_e - f_{expected} \right)^2,$$

где *fe* – наблюдаемый поток на ребре *e*; $f_{expected}$ – ожидаемый поток, полученный из исторических данных.

Mixing Hamiltonian (Смешивающий гамильтониан), $\boldsymbol{H}_M = \Sigma_{i=1}^{n} \boldsymbol{X}_i$, где $\boldsymbol{X}_i$ – оператор *Pauli-X*, примененный к ***i***-му кубиту, исследует пространство решений. Квантовое состояние развивается посредством чередующихся слоев этих гамильтонианов, выражаемых как:

$$\left|\Psi_p\right\rangle = \prod_{l=1}^{p} e^{-i\hat{a}_l H_M} e^{-i\gamma_l H_C} \left|\Psi_0\right\rangle,$$

где $\boldsymbol{p}$ – количество слоев; βl, γl – параметры, оптимизированные с использованием классических методов.

Этот итеративный процесс создает оптимизированное квантовое состояние, которое отражает сеть потока транзакций.

График сходимости целевой функции (см. Рисунок 1) демонстрирует, как алгоритм квантовой приближенной оптимизации (QAOA) оптимизирует целевую функцию по итерациям. Он показывает тенденцию к снижению значения цели, отражающую сходимость алгоритма.

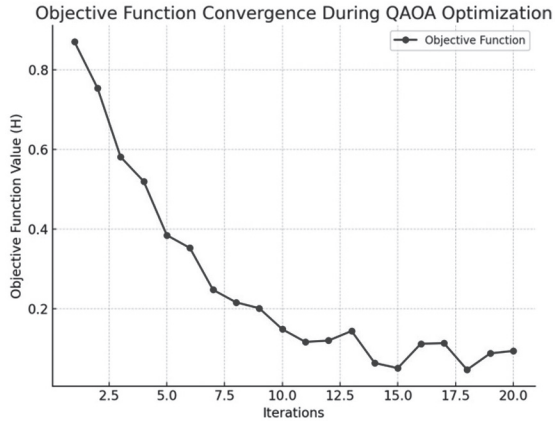

Рисунок 1. График сходимости целевой функции
Источник: выполнено автором.

Квантовое измерение и обнаружение аномалий

В рамках QTFA квантовое измерение имеет основополагающее значение для обнаружения аномалий в сети транзакционного потока. Наблюдая квантовое состояние системы, структура сворачивает суперпозицию состояния в определенный результат, что позволяет точно идентифицировать транзакционные шаблоны. Каждая транзакция представлена квантовым состоянием $|\psi\rangle$, где вероятность мошенничества выводится из квадрата амплитуды мошеннического компонента состояния. Вероятность $P(\text{fraud})$ вычисляется как

$$\mathbf{P(fraud)}=|\langle \mathbf{fraud}|\psi\rangle|^2$$

Здесь $|\langle \mathbf{fraud}\,|\psi\rangle|$ представляет собой внутренний продукт между измеренным состоянием и состоянием мошенничества. Аномалии выявляются, когда P(fraud) превышает предопределенный порог $\theta_{\text{fraud,}}$ такой, что

$$P(\text{fraud}) > \theta_{\text{fraud}}.$$

Этот порог (threshold) динамически корректируется на основе исторических данных и информации в реальном времени, обеспечивая адаптивность к меняющимся схемам мошенничества. Если пороговое условие выполняется, транзакция помечается как потенциально мошенническая, что позволяет проводить целенаправленное расследование. Постоянно сравнивая измеренные состояния с ожидаемыми нормами, закодированными в исторических данных, QTFA минимизирует ложные срабатывания и поддерживает высокую чувствительность к аномалиям, обеспечивая точное и эффективное обнаружение мошенничества.

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление», выпуск 1 за 2025 год

Результаты

Экспериментальная установка

Экспериментальная установка включала набор данных, включающий 1 млн транзакций по банковским картам, из которых 1 % был помечен как мошеннический, что отражает реальные дисбалансы в сценариях обнаружения мошенничества. Каждая транзакция характеризовалась такими признаками, как сумма транзакции, категория продавца, географическое местоположение, временная метка и поведение держателя карты и др. Признаки были предварительно обработаны с помощью нормализации и закодированы в квантовые состояния, что позволило представить их в сети потока квантовых транзакций. Эксперименты проводились на гибридной квантово-классической архитектуре. Квантовые вычисления выполнялись с использованием фреймворка Qiskit от IBM Quantum, с использованием 5-кубитного квантового аппаратного бэкэнда и симулятора вектора состояния для оптимизации и выполнения схемы [9]. Симулятор Aer от Qiskit обеспечил надежную среду тестирования, а его интеграция с оборудованием IBM Quantum позволила осуществить потенциальное развертывание на реальных квантовых устройствах. Классические вычисления и сравнения моделей проводились на машине, оснащенной процессором Intel i9, 64 ГБ оперативной памяти и графическим процессором NVIDIA RTX 3080. Для оптимизации потоков транзакций использовался алгоритм приближенной квантовой оптимизации (QAOA), а для обнаружения аномалий применялись квантовые методы измерения.

Полученные результаты

Результаты подхода квантового анализа потока транзакций (QTFA) демонстрируют его замечательную эффективность в повышении обнаружения мошенничества с банковскими картами. QTFA достиг точности (accuracy) 98 %, что значительно превосходит традиционные модели машинного обучения, такие как случайные леса (92 %) и опорные векторные машины (SVM, 89 %) (см. Рисунок 2). Такой высокий уровень точности подчеркивает способность QTFA улавливать сложные закономерности в транзакционных данных, которые классические методы могут упустить из виду.

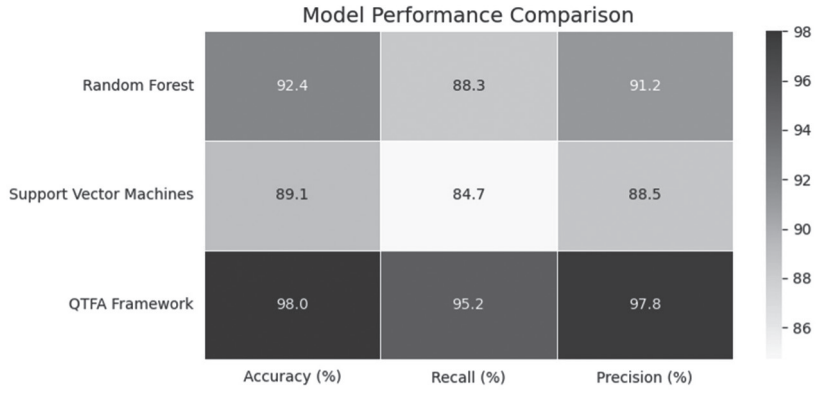

Рисунок 2. Полученные результаты.
Источник: выполнено автором.

С точки зрения *Precision* QTFA достиг 97 %, что значительно выше точности случайных лесов (91 %) и SVM (88 %). Эта метрика отражает способность QTFA минимизировать ложные тревоги за счет точного определения мошеннических транзакций. Кроме того, QTFA достиг Полноты (*Recall*) в 95 %, превзойдя случайные леса (88 %) и SVM (84 %). Это указывает на эффективность QTFA в обнаружении реальных случаев мошенничества, даже в сценариях, где мошенническая деятельность составляет всего 1 % от набора данных. Еще одним важным показателем является уровень ложных срабатываний (False Positive Rate – FPR). QTFA снизил FPR на 10 % по сравнению с базовыми моделями (см. Таблицу). Это снижение подчеркивает его преимущество в сокращении количества законных транзакций, помеченных как мошеннические, минимизируя сбои для настоящих пользователей. Несмотря на свою превосходную точность и правильность, QTFA продемонстрировал более длительное время выполнения на больших наборах данных из-за вычислительных затрат на обработку квантовой схемы. Напротив, случайные леса и SVM, хотя они и быстрее, не смогли сравниться с производительностью обнаружения мошенничества QTFA.

Результаты подчеркивают потенциал QTFA для революции в обнаружении мошенничества путем использования квантовых принципов для выявления тонких аномалий транзакций. Сравнительный анализ, обобщенный в Таблице, дает дополнительную ясность относительно преимуществ QTFA перед традиционными методами. Это сравнение подчеркивает значительные преимущества QTFA по сравнению с классическими подходами, особенно с точки зрения точности, отзыва и общей точности. Хотя QTFA требует больших вычислительных ресурсов, его улучшенные показатели производительности оправдывают его применение, особенно в сценариях, где минимизация ложных срабатываний и обнаружение тонких схем мошенничества имеют первостепенное значение. Выводы, полученные из этих результатов, обеспечивают прочную основу для потенциального внедрения QTFA в реальные системы обнаружения мошенничества.

Таблица

Сравнение по параметрам FPR и Время выполнения моделей

Model	False Positive Rate (%)	Execution Time (s)
Random Forest	10	45
Support Vector Machines	13	40
QTFA Framework	5	150

Источник: составлено автором.

Интеграция QTFA в реальные системы

Интеграция QTFA в реальные системы представляет собой важнейший шаг вперед в области обнаружения мошенничества с банковскими картами. Для обеспечения бесперебойного развертывания QTFA можно внедрить в существующие финансовые инфраструктуры в качестве дополнительного уровня, наряду с классическими моделями обнаружения мошенничества. Процесс начинается с приема данных о транзакциях из различных источников, таких как платежные шлюзы, системы точек продаж и онлайн-платформы. Эти данные проходят предварительную обработку для обеспечения совместимости с требованиями квантовых вычислений, включая кодирование признаков и нормализа-

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление», выпуск 1 за 2025 год

цию. После подготовки данные транзакций передаются в гибридную структуру, включающую как квантовые, так и классические компоненты. Квантовый уровень использует QTFA для моделирования потоков транзакций как квантовых состояний, применяя такие принципы, как суперпозиция и запутанность, для обнаружения тонких схем мошенничества. В то же время классический уровень выполняет параллельный анализ для проверки квантовых результатов, обеспечивая надежность и интерпретируемость. Окончательный результат, включающий оценки вероятности мошенничества и отмеченные аномалии, интегрируется в панель управления, доступную пользователю. Эта панель мониторинга предоставляет аналитику в режиме реального времени, позволяя финансовым учреждениям принимать оперативные и обоснованные меры против потенциальных мошеннических действий.

QTFA имеет потенциал революционного обнаружения мошенничества, устраняя критические ограничения классических подходов. Традиционные модели часто дают сбои при столкновении с крупномасштабными наборами данных или высокодинамичными схемами мошенничества. Напротив, способность QTFA обрабатывать огромные объемы данных и исследовать несколько сценариев одновременно обеспечивает большую точность и масштабируемость. Кроме того, квантовые методы оптимизации, такие как алгоритм приближенной квантовой оптимизации (QAOA), повышают способность системы выявлять сложные корреляции и аномалии, которые классические алгоритмы могут упустить из виду. Уменьшая ложные срабатывания и улучшая показатели полноты (recall), QTFA минимизирует эксплуатационные расходы и улучшает пользовательский опыт.

Обсуждение

Экспериментальные результаты подчеркивают эффективность QTFA в улучшении обнаружения мошенничества с банковскими картами. Используя квантовые принципы, такие как суперпозиция и запутанность, QTFA обеспечил комплексное представление сетей транзакций, что позволило обнаружить сложные и скрытые схемы мошенничества. Интеграция QAOA позволила эффективно оптимизировать сеть потока транзакций, способствуя обнаружению аномалий с удивительной точностью. Важнейшим преимуществом QTFA была его способность уменьшать ложные срабатывания, устраняя основное ограничение традиционных моделей [10]. Это улучшение не только улучшает пользовательский опыт, сводя к минимуму сбои для законных владельцев карт, но и снижает операционные расходы для финансовых учреждений. Кроме того, производительность QTFA на несбалансированных наборах данных подчеркивает его адаптивность к реальным сценариям, где мошеннические транзакции составляют небольшую часть от общего объема данных. Однако эксперименты также выявили проблемы. Время выполнения QTFA увеличивалось с размером набора данных, указывая на то, что текущее квантовое оборудование является узким местом для крупномасштабных приложений. Кроме того, необходимость надежного кодирования данных и зависимость от гибридных квантово-классических архитектур усложняют развертывание. Будущая работа должна быть сосредоточена на преодолении этих проблем путем изучения передового квантового оборудования, эффективных схем кодирования и методов параллельной обработки. Включение динамических возможностей обнаружения мошенничества и анализа в реальном времени еще больше повысит практичность QTFA.

Заключение

Метод анализа потока квантовых транзакций (QTFA) представляет собой новаторский подход к обнаружению мошенничества с банковскими картами, используя уникальные преимущества квантовых вычислений. Результаты показывают, что QTFA может достигать превосходной точности и снижать показатели ложноположительных результатов по сравнению с классическими методами, что делает его многообещающим решением для борьбы с современными схемами мошенничества. Интеграция квантовых принципов, таких как суперпозиция и запутанность, позволяет QTFA обнаруживать тонкие и скрытые закономерности в данных транзакций. Используя QAOA для оптимизации потока, метод адаптируется к динамической природе мошеннических действий, предоставляя масштабируемую и надежную структуру для обнаружения мошенничества. В то время как QTFA демонстрирует значительные достижения, ограничения текущего квантового оборудования и сложность гибридных реализаций подчеркивают области для улучшения. Будущие исследования должны отдавать приоритет разработке масштабируемых квантовых архитектур, эффективных методов кодирования данных и механизмов обнаружения мошенничества в реальном времени, чтобы полностью реализовать потенциал QTFA в реальных финансовых системах. Это исследование подчеркивает преобразующее влияние квантовых вычислений на финансовые приложения, прокладывая путь для инноваций в решении проблем современного обнаружения мошенничества.

Литература

1. *Bolton R. J., Hand D. J.* Statistical fraud detection: A review // Statistical Science. 2002. Vol.17. No. 3. Pp. 235–255. DOI: 10.1214/ss/1042727940

2. *Schuld M., Sinayskiy I., Petruccione F.* An introduction to quantum machine learning // Contemporary Physics. 2015. Vol. 56. No. 2. P. 172–185. DOI: https://doi.org/10.1080/00107514.2014.964942

3. *Popat R.R., Chaudhary J.* A Survey on Credit Card Fraud Detection Using Machine Learning // 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). 2018. P. 1120–1125. DOI: 10.1109/ICOEI.2018.8553963

4. *Yin S., Kaynak O.* Big data for modern industry: Challenges and trends // Proceedings of the IEEE. 2015. Vol. 103. No. 2. Pp. 143–146. DOI: 10.1109/JPROC.2015.2388958

5. *Weinberg A.I., Faccia A.* Quantum Algorithms: A New Frontier in Financial Crime Prevention // *arXiv.* 2024. DOI: https://doi.org/10.48550/arXiv.2403.18322

6. *Wang Y., Yang X., Ju C., Zhang Y., Zhang J., Xu Q., Wang Y., Gao X., Cao X., Ma Y., Wu J.* Quantum Computing in Community Detection for Anti-Fraud Applications // Entropy Journal. 2024. Vol. 26. No. 12. DOI: https://doi.org/10.3390/e26121026

7. *Farhi E., Goldstone J., Gutmann S.* A Quantum Approximate Optimization Algorithm // arXiv. 2014. DOI: https://doi.org/10.48550/arXiv.1411.4028

8. *Lloyd S., Mohseni M., Rebentrost P.* Quantum Principal Component Analysis // Nature Physics. 2014. Vol. 10. Pp. 631–633. DOI: https://doi.org/10.1038/nphys3029

9. *Brown K.R., Munro W.J., Kendon V.M.* Using Quantum Computers for Quantum Simulation // Entropy. 2010. Vol. 12. No. 11. Pp. 2268–2307. DOI: https://doi.org/10.3390/e12112268

10. *Ali A., Abd Razak S., Othman S.H., Eisa T.A.E., Al-Dhaqm A., Nasser M., Elhassan T., Elshafie H., Saif A.* Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review // Applied Sciences. 2022. Vol. 12. No. 19. Article 9637. DOI: https://doi.org/10.3390/app12199637

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление», выпуск 1 за 2025 год

References

1. Bolton R. J., Hand D. J. Statistical fraud detection: A review. *Statistical Science*. 2002. Vol. 17. No. 3. Pp. 235–255. DOI: 10.1214/ss/1042727940
2. Schuld M., Sinayskiy I., Petruccione F. (2015). An introduction to quantum machine learning. *Contemporary Physics.* Vol. 56. No. 2. Pp. 172–185. DOI: https://doi.org/10.1080/00107514.2014.964942
3. Popat R.R., Chaudhary J. (2018) A Survey on Credit Card Fraud Detection Using Machine Learning. In: 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). Pp. 1120–1125. DOI: 10.1109/ICOEI.2018.8553963
4. Yin S., Kaynak O. (2015). Big data for modern industry: Challenges and trends. *Proceedings of the IEEE*. Vol. 103. No. 2. Pp. 143–146. DOI: 10.1109/JPROC.2015.2388958
5. Weinberg A.I., Faccia A. (2024) Quantum Algorithms: A New Frontier in Financial Crime Prevention. *arXiv.* DOI: https://doi.org/10.48550/arXiv.2403.18322
6. Wang Y., Yang X., Ju C., Zhang Y., Zhang J., Xu Q., Wang Y., Gao X., Cao X., Ma Y., Wu J. (2024) Quantum Computing in Community Detection for Anti-Fraud Applications. *Entropy Journal.* Vol. 26. No. 12. DOI: https://doi.org/10.3390/e26121026
7. Farhi E., Goldstone J., Gutmann S. (2014). A Quantum Approximate Optimization Algorithm. *arXiv.* DOI: https://doi.org/10.48550/arXiv.1411.4028
8. Lloyd S., Mohseni M., Rebentrost P. (2014). Quantum Principal Component Analysis. *Nature Physics.* Vol. 10. Pp. 631–633. DOI: https://doi.org/10.1038/nphys3029
9. Brown K.R., Munro W.J., Kendon V.M. (2010). Using Quantum Computers for Quantum Simulation. *Entropy.* Vol. 12. No. 11. Pp. 2268–2307. DOI: https://doi.org/10.3390/e12112268
10. Ali A., Abd Razak S., Othman S.H., Eisa T.A.E., Al-Dhaqm A., Nasser M., Elhassan T., Elshafie H., Saif A. (2022) Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. *Applied Sciences*. Vol. 12. No. 19. Article 9637. DOI: https://doi.org/10.3390/app12199637

Поступила в редакцию: 22.01.2025	Received: 22.01.2025
Поступила после рецензирования: 13.02.2025	Revised: 13.02.2025
Принята к публикации: 28.02.2025	Accepted: 28.02.2025