УДК 004.891.2 Вестник УрФО № 3(57) / 2025, с. 17–23

Кушнир Н. В., Власенко А. В., Колесников Д. С., Яцкевич Е. С.

10.14529/secur250302

ОБНАРУЖЕНИЕ АНОМАЛИЙ В ФИНАНСОВЫХ ТРАНЗАКЦИЯХ С ПОМОЩЬЮ АВТОЭНКОДЕРОВ

В данной работе рассматривается задача выявления подозрительных финансовых транзакций с использованием нейросетевых автоэнкодеров. Подобные транзакции зачастую могут быть индикатором мошеннической активности, что делает проблему их своевременного обнаружения критически важной для систем финансовой безопасности.

Вначале проведён обзор существующих подходов к детектированию аномалий, включая классические статистические методы и современные алгоритмы машинного обучения. Отмечается, что большинство традиционных моделей сталкиваются с трудностями при работе с данными, в которых наблюдается существенный дисбаланс классов, характерный для финансовых операций (мошеннические транзакции составляют крайне малую долю от общего объёма).

На этом фоне использование автоэнкодеров представляется целесообразным решением. Данный тип нейронных сетей позволяет строить компактное внутреннее представление нормальных данных, а затем выявлять аномалии на основе величины ошибки восстановления. В исследовании применён полносвязный симметричный автоэнкодер, обученный на открытом наборе данных транзакций.

Результаты экспериментов показывают, что предложенная модель способна эффективно выделять отклонения от типичного поведения. Чтобы подтвердить качество разработанного метода, был проведён сравнительный анализ с признанными подходами, такими как метод изолирующего леса и логистической регрессии. Анализ показал, что использование нейронных сетей позволяет значительно повысить точность выявления подозрительных транзакций, что свидетельствует о перспективности внедрения такого подхода на практике. Исследование подчёркивает важность интеграции моделей автоэнкодинга и глубокого обучения для эффективного решения проблем финансового мониторинга. Практическое применение полученных результатов открывает возможности для совершенствования существующих механизмов предотвращения мошенничества, наделяя их способностью оперативно реагировать на появление новых форм противоправных действий.

Ключевые слова: *обнаружение аномалий, автоэнкодер, нейросети, финансовые транзакции, выявление мошенничества, ошибка восстановления, несбалансированные данные, глубокое обучение.*

DETECTING ANOMALIES IN FINANCIAL TRANSACTIONS USING AUTOENCODERS

This paper considers the problem of detecting suspicious financial transactions using neural network autoencoders. Such transactions can often be an indicator of fraudulent activity, which makes the problem of their timely detection critically important for financial security systems.

First, an overview of existing approaches to anomaly detection is provided, including classical statistical methods and modern machine learning algorithms. It is noted that most traditional models face difficulties when working with data in which there is a significant class imbalance characteristic of financial transactions (fraudulent transactions account for an extremely small proportion of the total volume).

Against this background, the use of autoencoders seems to be an appropriate solution. This type of neural network allows you to build a compact internal representation of normal data, and then identify anomalies based on the magnitude of the recovery error. The study uses a fully connected symmetric autoencoder trained on an open set of transaction data.

The experimental results show that the proposed model is able to effectively identify deviations from typical behavior. To assess its quality, a comparison was made with alternative methods, including Isolation Forest and logistic regression. The analysis showed that the neural network architecture demonstrates a higher sensitivity in detecting fraudulent transactions, which confirms its prospects for practical application.

Thus, the conducted research highlights the importance of using autoencoders and neural network technologies in general when solving financial analytics problems. The results obtained can serve as a basis for the development of more reliable protection systems capable of adapting to new types of fraudulent schemes.

Keywords: *anomaly detection, autoencoder, neural networks, financial transactions, fraud detection, reconstruction error, imbalanced data, deep learning.*

Введение

Современная финансовая индустрия находится в условиях интенсивной цифровизации. Это явление значительно упрощает проведение транзакций и расширяет возможности пользователей, однако одновременно повышает уязвимость системы перед различными угрозами безопасности. Одной из наиболее острых проблем является рост числа мошеннических операций, связанных с использованием украденных персональных данных и созданием поддельных аккаунтов. Несмотря на то что подавляющее большинство транзакций является легитимным, даже относительно небольшая доля мошеннических действий способна привести к серьёзным финансовым потерям и подорвать доверие клиентов к системе.

В этой связи задача своевременного и надёжного обнаружения аномальных транзакций приобретает особую значимость. Традиционные методы, основанные на фиксированных правилах или простых статистических моделях, показывают ограниченную эффективность в условиях постоянно меняющихся мошеннических схем. Злоумышленники непрерывно адаптируют свои стратегии, что снижает результативность жёстко детерминированных алгоритмов и требует внедрения более гибких и интеллектуальных подходов [1].

Одним из перспективных направлений в этой области является использование методов машинного обучения, а именно нейросетевых архитектур, способных выявлять скры-

тые зависимости и обучаться на больших массивах данных. Среди таких моделей особое внимание привлекают автоэнкодеры. Их ключевая особенность заключается в способности восстанавливать входные данные после их сжатия, формируя компактное внутреннее представление. Аномальные транзакции, как правило, плохо соответствуют выученным закономерностям и, следовательно, воспроизводятся сетью с высокой ошибкой. Этот эффект позволяет использовать автоэнкодеры в качестве эффективного инструмента для обнаружения отклонений.

Применение автоэнкодеров имеет ряд преимуществ перед традиционными методами. Во-первых, их работа не требует большого количества размеченных данных, что особенно важно при выраженном дисбалансе классов: количество мошеннических операций значительно уступает числу нормальных транзакций. Во-вторых, архитектура модели позволяет классифицировать операции на нормальные и подозрительные, опираясь исключительно на величину ошибки реконструкции. Таким образом, подход не только обеспечивает адаптивность к новым угрозам, но и повышает надёжность функционирования финансовых систем.

Целью данной работы является исследование эффективности применения автоэнкодеров в задаче выявления аномальных транзакций, а также анализ направлений возможного совершенствования данной модели.

Автоэнкодер представляет собой разновидность искусственной нейронной сети, предназначенную для построения сжатого представления исходных данных при сохранении ключевых признаков и их последующего восстановления. Обучение, как правило, проводится в безучительном режиме, когда целевая переменная совпадает со входным вектором. Архитектура автоэнкодера включает три основных блока: энкодер, выполняющий преобразование входных данных в скрытое представление; бутылочное горлышко (или латентное пространство), содержащее упрощённое описание исходных данных; и декодер, восстанавливающий входную информацию на основе скрытого представления. Архитектура автоэнкодера приведена на рисунке 1. Такая структура обеспечивает возможность выявления несоответствий и делает автоэнкодеры ценным инструментом анализа данных в условиях высокой изменчивости угроз.

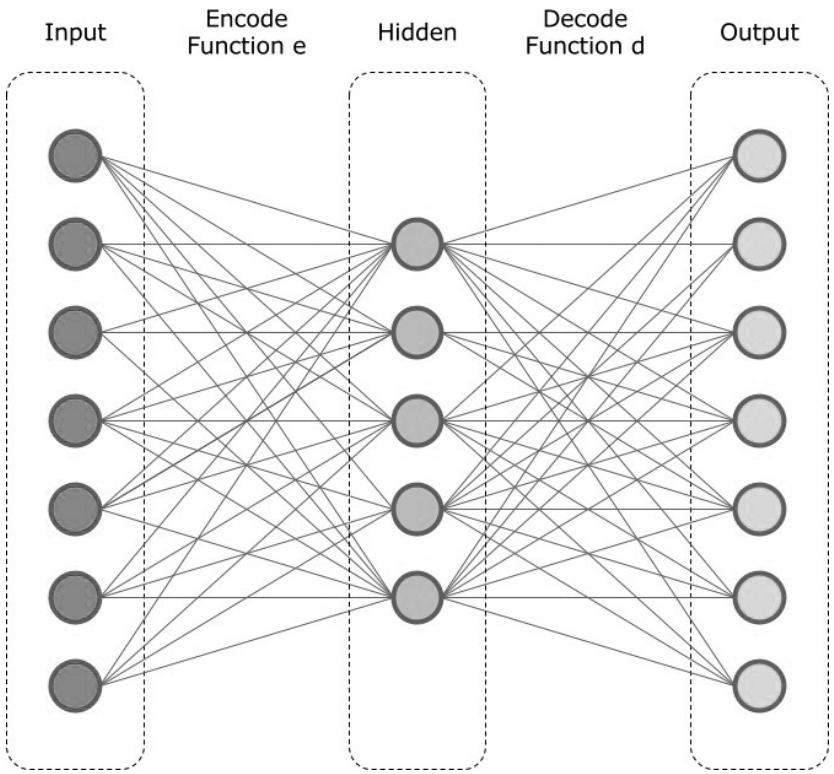

Рис.1. Схема архитектуры энкодера

Обнаружение аномалий в финансовых транзакциях с помощью автоэнкодеров

В задачах обнаружения аномалий автоэнкодеры обучаются преимущественно на примерах, относящихся к «нормальному» поведению системы. При этом транзакции, не соответствующие общей закономерности, воспроизводятся сетью с заметными искажениями. Это приводит к увеличению ошибки восстановления, которая и используется как основной критерий для классификации операции как аномальной. Таким образом, величина ошибки играет ключевую роль: при превышении заранее установленного порогового значения транзакция рассматривается как подозрительная. Следует отметить, что подбор оптимального порога является эмпирическим процессом и во многом определяет баланс между чувствительностью модели и её специфичностью.

Автоэнкодеры могут иметь различную архитектуру и уровень сложности: от простейших полносвязных структур до более продвинутых модификаций на основе сверточных и рекуррентных слоёв. Для анализа финансовых транзакций чаще всего применяются полносвязные автоэнкодеры, так как данные в подобных задачах представлены числовыми векторами признаков. Эффективность такой модели напрямую зависит как от качества исходных данных, так и от объема обучающей выборки. В этом контексте автоэнкодеры выступают как мощный инструмент безнадзорного выявления аномалий, особенно в ситуациях, когда число реальных примеров мошенничества крайне ограничено. Подобный подход находит применение не только в финансовой сфере, но и в более широком контексте кибербезопасности.

Для проведения эксперимента в настоящем исследовании был выбран открытый датасет **Credit Card Fraud Detection**, характеризующийся ярко выраженным дисбалансом классов: доля мошеннических транзакций составляет менее 1% от общего числа записей. Предобработка данных включала нормализацию числовых признаков, а также разделение выборки на тренировочную, тестовую и валидационную части.

Для задачи обнаружения аномалий использовалась архитектура автоэнкодера, включающая энкодер и декодер. Энкодер сжимал входные данные в латентное представление размерности 10, после чего декодер выполнял реконструкцию исходного вектора признаков. Обучение модели проводилось с использованием оптимизатора **Adam**, при этом применялась стратегия ранней остановки, позволяющая предотвратить переобучение и повысить обобщающую способность сети [3].

Оценка качества модели осуществлялась с применением таких метрик, как **MSE (среднеквадратичная ошибка), Precision, Recall, F1-score и AUC.** Результаты тестирования приведены на рисунке 2. Исследование продемонстрировало высокую эффективность разработанной модели: автоэнкодер продемонстрировал более высокие показатели по сравнению с такими традиционными методами, как логистическая регрессия и Isolation Forest.

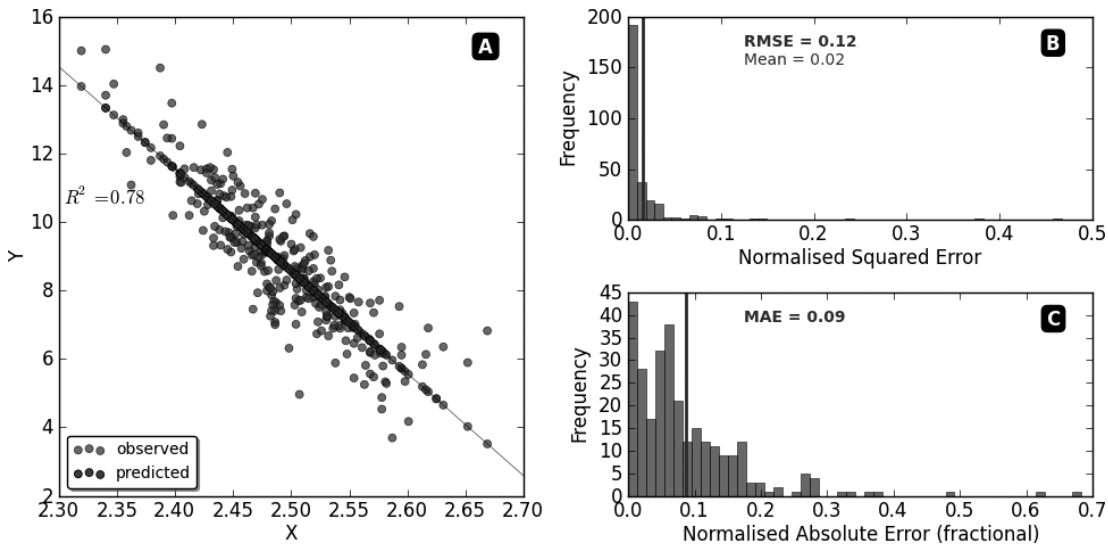

Рис. 2. График ошибок восстановления (MSE) для нормальных и аномальных транзакций

Проведенный анализ показал, что предложенная модель автоэнкодера работает лучше, чем традиционные методы (логистическая регрессия, алгоритм изоляции леса). Автоэнкодер точнее определяет необычные финансовые операции. Это говорит о том, что нейросети-автоэнкодеры очень хорошо выявляют подозрительные транзакции и могут быть полезны в финансах.

Главным критерием проверки качества стало среднее квадратичное отклонение (MSE), которое чётко отображало разницу между исходными и реконструированными финансовыми записями. Малое значение ошибки означало отсутствие подозрений относительно конкретной транзакции, а высокий показатель ошибки мог указывать на возможное нарушение нормального режима поведения. Экспериментально доказано, что автоэнкодер эффективно восстанавливает обычные финансовые события, чему соответствует минимальное значение среднего квадрата ошибок. Оценка успешности распознавания злоумышленников проводилась с использованием таких показателей, как точность (Precision), полнота (Recall) и коэффициент сбалансированности (F1-score), критически важных в ситуации существенного перекоса распределения типов событий. Предложенная модель показала отличные способности по обнаружению редких нарушений. Показатель F1-score обеспечил оптимальное соотношение между уровнем чувствительности и специфичности, сведя количество ошибочных сигналов к минимуму. Ещё одним убедительным аргументом стало изучение кривых ROC и вычисленной площади под ними (AUC). Методы дали стабильное разделение обычных и нестандартных записей. Обзор методов также зафиксировал превосходство предлагаемого подхода перед классическими моделями, включая логистическую регрессию и Isolation Forest, практически по всем важным критериям оценки, таким как точность, полнота и площадь под ROC-кривой. Немаловажным аспектом оказалось определение порога принятия решений, основанного на величине ошибки реконструкции. Точная настройка этого показателя оказала решающее влияние на равновесие между количеством найденных преступных операций и числом случайных предупреждений. Следует подчеркнуть важное свойство автоэнкодеров — независимость от заранее помеченных примеров отклонений и способность самостоятельно раскрывать скрытую структуру сложных многомерных данных.

Итоги эксперимента, которые приведены на рисунке 3, ещё раз подтверждают значимость в задаче нахождения сомнительных финансовых манипуляций. В перспективе качество выявления мошенничества может быть улучшено за счёт применения более сложных модификаций, таких как вариационные автоэнкодеры (VAE), которые учитывают вероятностную природу данных и способны обеспечить более точное разделение транзакций [5].

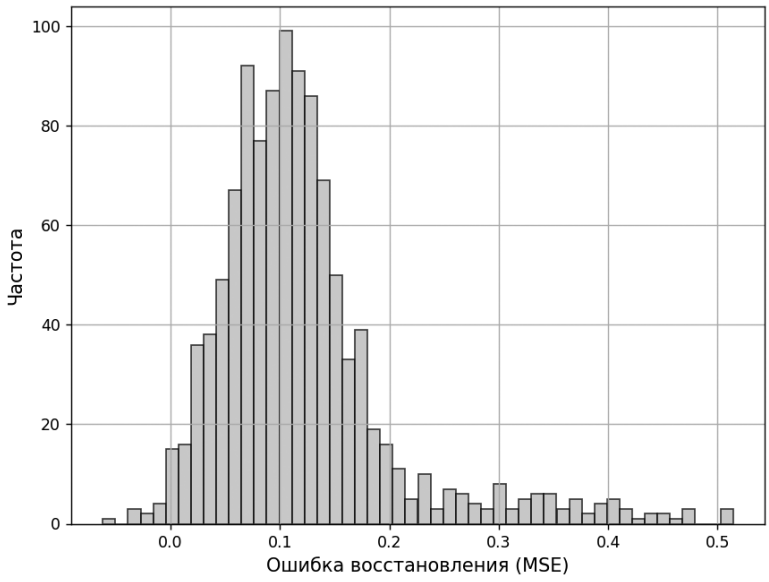

Рис. 3. Гистограмма распределения транзакций по ошибке восстановления (MSE)

Проведённое исследование наглядно подтвердило, что автоэнкодеры являются крайне действенным инструментом для выявления аномалий в финансовых транзакциях. Модель не только успешно воссоздаёт нормальные операции, глубже понимая их типичные черты, но и уверенно обнаруживает редкие, подозрительные отклонения, к которым относятся и мошеннические действия.

Как показало сравнение с другими методами, автоэнкодеры работают результативнее классических подходов — логистической регрессии и Isolation Forest — особенно когда данные сильно несбалансированны. Эти выводы свидетельствуют о том, что такие технологии легко адаптируются к реальным условиям эксплуатации, где выявление отдельных эпизодов злоупотреблений имеет ключевое значение для обеспечения защищённости и поддержания уверенности пользователей. Применение автоэнкодеров способствует созданию инновационных подходов к контролю финансовых потоков. Благодаря снижению числа неверных сигналов тревоги и улучшению выявления рисков, повышается устойчивость всей банковской инфраструктуры. Поскольку каждая допущенная погрешность способна привести к серьёзным финансовым потерям и удару по имиджу организации, подобные инструменты приобретают особую важность. Однако возможности дальнейшего роста сохраняются. Перспективным подходом является создание сложных моделей, например, вариационных автоэнкодеров. Эти модели умеют учитывать случайные факторы, что делает их более гибкими и эффективными. Такое сочетание технологий может значительно повысить точность обнаружения мошенничества и устойчивость к новым, более сложным схемам обмана.

В целом, автоэнкодеры показали свою эффективность в выявлении подозрительных операций в финансовой сфере. Их применение в системах безопасности помогает существенно уменьшить риски, связанные с мошенничеством. Дальнейшее исследование и улучшение этих методов является важной задачей, как для научных исследований, так и для практического применения.

Литература

1. Развитие алгоритмов и программ для защиты информации в сфере финансовых технологий. URL: https://www.elibrary.ru/item.asp?id=58908413 (дата обращения: 07.04.2025).

2. Финансовое мошенничество в современном мире. URL: https://www.elibrary.ru/item.asp?id=54279278 (дата обращения: 07.04.2025).

3. Повышение точности кластеризации QRS-комплексов с помощью вариационного автоэнкодера. URL: https://www.elibrary.ru/item.asp?id=68018062 (дата обращения: 07.04.2025).

4. Исследование влияния batch-size на качество обучения нейронных сетей. URL: https://elibrary.ru/item.asp?id=65663440 (дата обращения: 07.04.2025).

5. Анализ эффективности алгоритмов обучения на основе градиентного спуска в задаче дообучения предварительно обученной нейросети. URL: https://elibrary.ru/item.asp?id=48115024 (дата обращения: 07.04.2025).

References

1. Razvitiye algoritmov i programm dlya zashchity informatsii v sfere finansovykh tekhnologiy. URL: https://www.elibrary.ru/item.asp?id=58908413 (data obrashcheniya: 07.04.2025).

2. Finansovoye moshennichestvo v sovremennom mire. URL: https://www.elibrary.ru/item.asp?id=54279278 (data obrashcheniya: 07.04.2025).

3. Povysheniye tochnosti klasterizatsii QRS-kompleksov s pomoshch'yu variatsionnogo avtoenkodera. URL: https://www.elibrary.ru/item.asp?id=68018062 (data obrashcheniya: 07.04.2025).

4. Issledovaniye vliyaniya batch-size na kachestvo obucheniya neyronnykh setey. URL: https://elibrary.ru/item.asp?id=65663440 (data obrashcheniya: 07.04.2025).

5. Analiz effektivnosti algoritmov obucheniya na osnove gradiyentnogo spuska v zadache doobucheniya predvaritel'no obuchennoy neyroseti. URL: https://elibrary.ru/item.asp?id=48115024 (data obrashcheniya: 07.04.2025).

КУШНИР Надежда Владимировна, старший преподаватель кафедры информационных систем и программирования ФГБОУ ВО «Кубанский государственный технологический университет». 350072, г. Краснодар, ул. Московская, д. 2. E-mail: kushnir.06@mail.ru

ВЛАСЕНКО Александра Владимировна, кандидат технических наук, доцент, Врио заведующего кафедрой информационной безопасности, профессор кафедры ФГКОУ ВО «Краснодарский университет МВД России». 350005, г. Краснодар, ул. Ярославская 128. E- mail: alex_vlasenko@list.ru

КОЛЕСНИКОВ Даниил Сергеевич, студент 4 ФГБОУ ВО «Кубанский государственный технологический университет». 350072, г. Краснодар, ул. Московская, д. 2. E-mail: dan-kol@bk.ru

ЯЦКЕВИЧ Евгений Сергеевич, магистрант 2 курса ФГБОУ ВО «Кубанский государственный технологический университет». 350072, г. Краснодар, ул. Московская, д. 2. E-mail: es_yatskevich@internet.ru

KUSHNIR Nadezhda Vladimirovna, Senior Lecturer at the Department of Information Systems and Programming of the Federal State Budgetary Educational Institution of Higher Education «Kuban State Technological University». 2 Moskovskaya St., Krasnodar, 350072. E-mail: kushnir.06@mail.ru

VLASENKO Alexandra Vladimirovna, Candidate of Technical Sciences, Associate Professor, Acting Head of the Department of Information Security Professor of the Department, of the Krasnodar University of the Ministry of Internal Affairs of Russia, 128 Yaroslavskaya str., Krasnodar, 350005. E-mail: alex_vlasenko@list.ru

KOLESNIKOV Daniil Sergeevich, 4th year student of the Federal State Budgetary Educational institution of Higher Education "Kuban State Technological University". 2 Moskovskaya St., Krasnodar, 350072. E-mail: dan-kol@bk.ru

YATSKEVICH Evgeny Sergeevich, 2nd year Master's student at the Federal State Budgetary Educational Institution of Higher Education «Kuban State Technological University». 2 Moskovskaya St., Krasnodar, 350072. E-mail: es_yatskevich@internet.ru