Использование нейронных сетей в задаче классификации аномального поведения в финансовых транзакциях с использованием Python и Keras

А. А. Кочнев

***Аннотация*. Целью данной работы является исследование и разработка нейронных сетей для задач классификации аномального поведения в финансовых транзакциях с использованием Python и Keras. Для достижения поставленной цели был выбран датасет, состоящий из 100000 финансовых транзакций, произведен препроцессинг данных, спроектирована архитектура нейронной сети и раскрыт процесс её обучения. Основой разработанной архитектуры является входной слой, которой состоит из 30 нейронов, соответствующих 30 признакам в наших данных. Выходным слоем архитектуры выступают два слоя, подтверждающие или опровергающие мошеннические транзакции. Основой выходного слоя является функция активации softmax, которая генерирует вероятности для каждого класса. Одним из важнейших преимуществ разработанной нейронной сети является эффективность функций активации, что основано на применении ReLU (Rectified Linear Unit) для входного и скрытых слоев. Обучение модели осуществлялось на протяжении 50 эпох с использованием алгоритма оптимизации Adam и батчем размером 32. Adam был выбран в качестве оптимизатора, который обеспечивает более быструю и стабильную сходимость. По итогам тренировки в 50 эпох была достигнута точность в 88%. Важно подчеркнуть, что, несмотря на значительный дисбаланс классов в датасете, модель показала способность точно определять аномалии. Это открывает большие возможности для применения данного подхода в реальной среде, где мошеннические транзакции также обычно составляют небольшую долю от общего числа транзакций.**

Ключевые слова — аномальное поведение, нейронные сети, финансовые транзакции, Python и Keras, Rectified Linear Unit, классификация аномального поведения.

I. Введение

Динамизм современного общества и значительный рост объемов совершаемых финансовых операций являются следствием активного течения процессов цифровизации, как отражение повышения эффективности реализуемых процедур. Важно понимать, что с ростом числа онлайн-транзакций возрастает и потребность в совершенствовании систем обнаружения мошенничества. Несмотря на предоставляемые технологиями возможности, человек все чаще сталкивается со всевозможными проявлениями мошеннических операций, что, несомненно, сказывается на уровне доверия и благосостоянии. В условиях взрывного роста данных о транзакциях, традиционные подходы к обнаружению аномалий часто оказываются недостаточно эффективными. Поэтому все больший интерес вызывают методы, использующие нейронные сети. Применение нейронных сетей имеет весомое прикладное значение, а в перспективе опыт выработки решений может быть интерпретирован в других сферах. Долгосрочный характер развития подобных технологий можно рассматривать в идеализированном представлении – как итог, формируются все условия для искоренения мошенничества с транзакциями.

С использованием библиотек Python и Keras мы провели исследование, целью которого было обучение нейронной сети для классификации аномального поведения в финансовых транзакциях.

II. Методология

Для нашего исследования мы использовали датасет [1], состоящий из 100000 финансовых транзакций. Эти данные были собраны с помощью системы обработки платежей с многих онлайн-платформ, что обеспечивает широкий спектр различных типов транзакций.

Каждая транзакция в датасете была представлена набором из 30 числовых признаков. Эти признаки включали в себя различные аспекты транзакций, такие как сумма транзакции, время совершения, местоположение, а также различные статистические данные, которые могут быть связаны с мошенничеством. Например, средняя сумма транзакций для данного пользователя, количество транзакций за определенный период времени и так далее.

Отметим, что 0.5% из этих транзакций были помечены как мошеннические. Это очень низкий процент, что говорит о существенном дисбалансе классов. Дисбаланс классов — это частая проблема при работе с данными о мошенничестве, поскольку мошеннические транзакции, как правило, составляют лишь малую часть от общего числа транзакций.

Этот набор данных был разделен на обучающую и тестовую выборки в соотношении 80% к 20%. Такое

Статья получена 2 августа 2023.
Кочнев Александр Александрович, Your Next Agency, San Diego, USA
e-mail: drdispool@gmail.com.

разделение обеспечивает достаточное количество данных для обучения модели, а также оставляет независимый набор данных для тестирования эффективности обученной модели. Тестовый набор не был использован в процессе обучения и использовался только для оценки производительности модели после завершения обучения.

Важно отметить, что при разделении данных мы удостоверились, что распределение мошеннических транзакций было схожим в обучающей и тестовой выборке, чтобы обеспечить репрезентативность обеих выборок.

III. Препроцессинг данных

Препроцессинг данных является важным этапом в процессе обучения нейронных сетей. Правильная подготовка данных может значительно улучшить качество обучения и финальную производительность модели.

Выделим некоторые особенности препроцессинга данных:

1. Нормализация данных: Наши данные состояли из 30 различных признаков, каждый из которых имел разный масштаб и диапазон значений. Признаки с большими значениями могут непропорционально повлиять на обучение, поэтому мы использовали нормализацию для приведения всех признаков к одному масштабу. Каждый признак был нормализован путем вычитания среднего значения и деления на стандартное отклонение. Это обеспечивает, что все признаки имеют среднее значение 0 и стандартное отклонение 1.
2. Обработка пропущенных значений: Датасет мог содержать пропущенные значения в некоторых из признаков. В случае обнаружения пропусков, мы использовали метод заполнения пропущенных значений средним значением этого признака по всему датасету. Это простой и эффективный способ обработки пропусков, который не искажает распределение данных.
3. Удаление дубликатов: Мы также проверили наши данные на наличие дубликатов. Дубликаты могут привести к переобучению, поскольку предоставляют модели один и тот же пример несколько раз. Мы удалили все найденные дубликаты из нашего набора данных.
4. Балансировка классов: Учитывая, что в наших данных был существенный дисбаланс классов (только 0.5% данных были аномальными), мы применили технику андерсэмплинга для уравновешивания классов [2]. Это означает, что мы случайным образом удалили некоторые из обычных транзакций, чтобы их количество стало равным количеству аномальных транзакций. Это позволило избежать проблемы игнорирования меньшего класса при обучении модели.
5. Препроцессинг данных — это важная часть процесса обучения нейронных сетей. Правильная подготовка данных может значительно улучшить качество обучения и финальную производительность модели.

IV. Архитектура нейронной сети

В качестве основных инструментов для разработки нейронной сети был использован язык программирования Python, а также фреймворк для машинного обучения Keras.

Python является одним из наиболее популярных языков программирования для работы с данными и машинным обучением. Он обладает простым и читаемым синтаксисом, что делает его идеальным для быстрого прототипирования и исследовательской работы. Более того, Python имеет обширный набор библиотек для научных вычислений, обработки данных и машинного обучения, таких как NumPy, Pandas, Scikit-learn, TensorFlow и Keras.

Keras - это библиотека для создания нейронных сетей, которая работает поверх TensorFlow. Она предоставляет простой и удобный интерфейс для создания и обучения моделей глубокого обучения. С помощью Keras мы можем быстро и легко проектировать различные архитектуры нейронных сетей, экспериментировать с разными слоями и функциями активации, а также настраивать процесс обучения.

Мы выбрали следующую архитектуру нейронной сети (рис. 1):

Рисунок 1 – Архитектура нейронной сети в Keras.

Важно уточнить, что архитектура нейронной сети состоит из четырех слоев:

1. Входной слой состоял из 30 нейронов, соответствующих 30 признакам в наших данных.
2. Два скрытых слоя, каждый из которых имел 16 нейронов. Это количество было выбрано для снижения сложности модели и предотвращения переобучения.
3. Выходной слой состоял из двух нейронов, представляющих два класса наших данных: обычные транзакции и мошеннические.

В качестве функции активации мы использовали ReLU для входного и скрытых слоев и softmax для выходного слоя. ReLU была выбрана из-за своей эффективности и меньшей подверженности проблеме исчезающего градиента, в то время как softmax была использована для получения вероятностей принадлежности к каждому из двух классов.

Получившаяся архитектура нейронной сети (рис. 2),

которая была выбрана нами, имеет несколько преимуществ для задачи классификации аномального поведения в финансовых транзакциях:

1. Универсальность: Наша архитектура состоит из входного слоя с 30 нейронами, что позволяет модели учитывать все 30 признаков входных данных. Это позволяет обнаруживать различные аспекты и паттерны, которые могут быть связаны с мошенничеством. Входной слой обеспечивает модели достаточную гибкость для анализа разнообразной информации о транзакциях.
2. Снижение сложности и предотвращение переобучения: Два скрытых слоя с 16 нейронами каждый были выбраны для снижения сложности модели и предотвращения переобучения. Использование меньшего количества нейронов помогает избежать излишней сложности, что может привести к переобучению модели на обучающих данных. Более простая модель может лучше обобщать и предсказывать на новых данных.
3. Эффективность функций активации: Мы использовали ReLU (Rectified Linear Unit) в качестве функции активации для входного и скрытых слоев. ReLU является широко используемой функцией активации, которая обладает простотой вычислений и способностью поддерживать высокую эффективность градиентного спуска. Она помогает усилить активацию положительных значений и сдвинуть данные в направлении нелинейности.
4. Вероятностная интерпретация: Выходной слой с двумя нейронами использует функцию активации softmax, которая генерирует вероятности для каждого класса - обычные транзакции и мошеннические транзакции. Это позволяет получать интерпретируемые результаты и определять, с какой вероятностью каждая транзакция относится к определенному классу.

В целом, выбранная архитектура нейронной сети обеспечивает достаточную гибкость, эффективность и интерпретируемость для задачи классификации аномального поведения в финансовых транзакциях. Однако важно помнить, что эффективность модели также зависит от качества и разнообразия доступных данных для обучения.

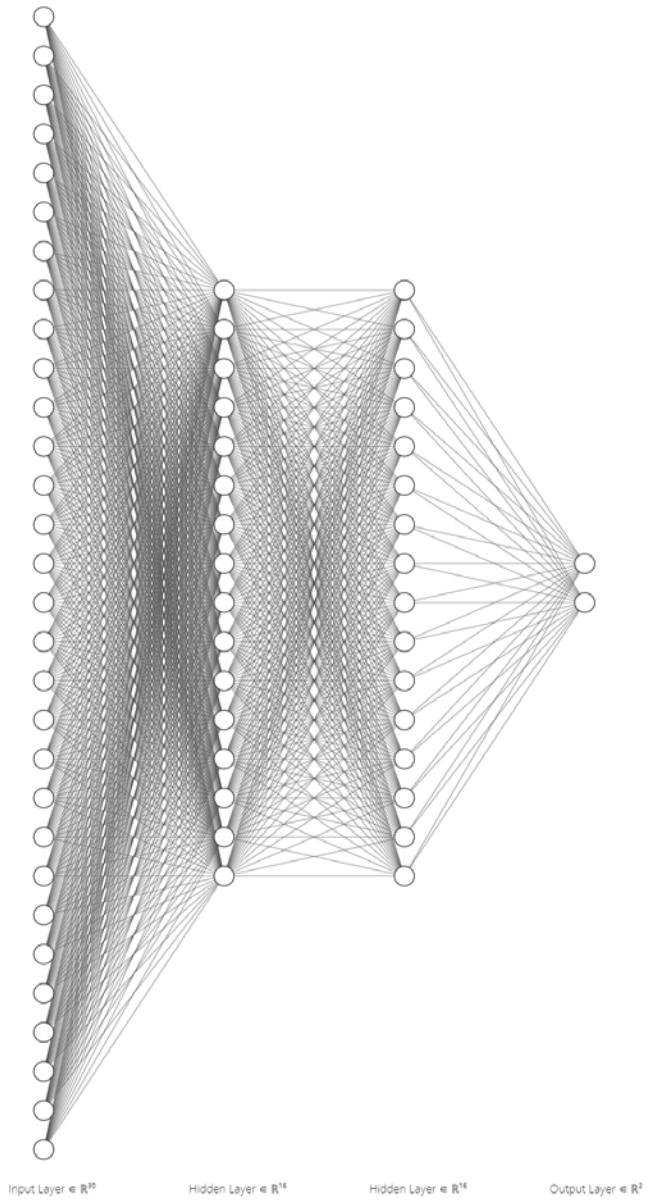

Рисунок 2 – Архитектура нейронной сети.

V. Процесс обучения

Мы обучили нашу модель на протяжении 50 эпох с использованием алгоритма оптимизации Adam и батчем размером 32. Adam был выбран в качестве оптимизатора, так как он эффективно сочетает преимущества двух других популярных алгоритмов оптимизации: RMSProp и AdaGrad, обеспечивая более быструю и стабильную сходимость.

В ходе тренировки модели нейронной сети на протяжении 50 эпох мы достигли точности в 88 процентов на валидационной выборке (рис. 3).

Это означает, что модель правильно классифицировала 88 процентов транзакций на основе предоставленных признаков. Каждую эпоху модель обрабатывала всю обучающую выборку, делая предсказания и обновляя веса нейронной сети с использованием градиентного спуска и обратного распространения ошибки. Мы также использовали раннюю остановку в качестве метода регуляризации, чтобы предотвратить переобучение.

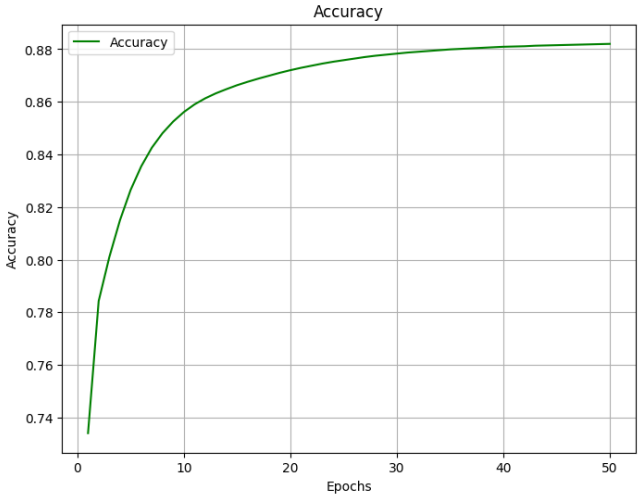

Рисунок 3 – Точность на валидационной выборке.

Модель останавливала обучение, когда ошибка на валидационной выборке начинала увеличиваться (рис. 4).

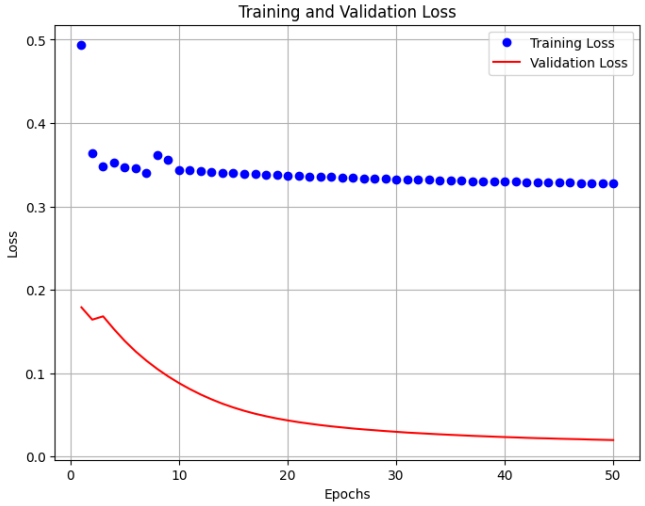

Рисунок 4 – Статистика потери.

В дальнейшем можно улучшить архитектуру нейронной сети, экспериментировать с гиперпараметрами и увеличивать объем данных для обучения, чтобы достичь еще более точной и обобщающей модели. Наша модель демонстрирует эффективность выбранной архитектуры и методов обучения в задаче классификации аномального поведения в финансовых транзакциях, что имеет важное значение для обеспечения безопасности и защиты финансовых систем от мошенничества.

VI. Обсуждение

Проблема борьбы с незаконными финансовыми операциями с применением современных технологий имеет глобальный мировой характер. Сегодня существует множество положительных примеров, связанных с эффективным и своевременным выявлением случаев коррупции, незаконных финансовых операций и прочих проявлений мошенничества, нарушения законодательства, когда современные технологии позволили раскрыть сложные схемы преступности. Искусственные нейронные сети являются одним из тех инструментов, опираясь на которые человечество получает возможность эффективно управлять данными и предостерегать от незаконных посягательств. Сфера незаконных финансовых операций настолько велика, что её исследованием занимается все мировое сообщество.

Современные научные исследования в области применения нейронных сетей и искусственного интеллекта для целей борьбы с мошенничеством и незаконными финансовыми операциями имеют достаточно разносторонний характер. В связи с этим важно обратиться к некоторым работам авторов, раскрывающим современное состояние и нерешенные проблемы в области использования нейронных сетей для борьбы с финансовыми преступлениями.

В работе К.А. Кузьмина нейронные сети рассматриваются в качестве прикладного способа предостережения пользователей кредитных карт о возможных случаях мошенничества. Автор придерживается позиции о том, что первичной задачей банка в таком случае является поиск путей дополнительной защиты конфиденциальных данных, в чем видит перспективы применения нейронных сетей. Искусственный интеллект, по мнению К.А. Кузьмина, обладает ключевым преимуществом – не несет за собой риски влияния человеческого фактора, когда в силу случайности или корыстных целей происходит утечка конфиденциальной информации [3]. На схожие условия указывают и Э.Г. Милкова [4], Н.Ш. Ватолкина, О.П. Федоткина, В.Г. Феклин [5] и многие другие авторы. В.А. Тверитинова в этом вопросе демонстрирует необходимость не столько исключения человека из процессов с повышенным уровнем угроз, сколько включения инструментов автоматизации и оптимизации его функций, в чем видит возможности использования современных технологий [6].

А.А. Сафонов видит, что искусственный интеллект может применяться в деятельности правоохранительных органов, в том числе не только для финансовых, но и других преступлений [7]. М.А. Желудков в контексте вопроса указывает на необходимость скорейшей адаптации правоохранительных органов и их цифровой трансформации. При отсутствии реагирования на становление цифровой среды, в которой формируется собственная цифровая преступность, определяются особые риски несоответствия деятельности правоохранительных органов современным требованиям [8]. Ф.В. Безгачев в этом вопросе предлагает некоторые пути реализации искусственного интеллекта в деятельности полиции, в частности, в целях распознавания материалов по делу (анализ речи, изображений, текста), а также прогнозирования (выдвижение версий). Автором названы общие проблемы реализации подобных систем: отсутствие развитого законодательства, требования к оцифровке, неэффективность затрат, сложности разработки и многие другие [9]. Тем не менее, отрицать перспективы применения искусственного интеллекта и нейронных

сетей в описанных целях не приходится. Важно не столько сфокусироваться на проблемах и перспективах, сколько определять пути воспроизводства алгоритмов и осуществлять их тестовый ввод в деятельность соответствующих структур.

Применение искусственного интеллекта и нейронных сетей в целях борьбы с финансовыми преступлениями может происходить как в системе автоматизации уже существующих механизмов, так и создания новых, дополнительных или заменяющих мер защиты. С.Л. Ларионова придерживается позиции о том, что необходимо в большей степени работать с автоматизацией современных задач, переводить их в автономный и закрытый характер, обеспечивая тем самым защиту от незаконных операций. Исследование автора имеет прикладное значение, поскольку в нем раскрываются дополнительные инструменты, предназначенные для извлечения данных с последующим применением в антифорд-системах [10]. Е.Г. Багреева и соавторы видят необходимость частного развития искусственного интеллекта со стороны банковских организаций [11]. Сегодня эти процессы активно запущены в ведущих мировых и отечественных банках, однако все еще сохраняются угрозы методов социальной инженерии и другие. В целом, полностью устранить влияние проблемы мошенничества в финансовой среде, как и в любой другой, невозможно. Тем не менее, имеются все ресурсы для создания максимально отзывчивой и защищенной среды, как минимум с точки зрения аппаратных решений и алгоритмического обеспечения. Защита информации в этой структуре, по мнению Д.В. Резника, становится ключевым инструментом на пути к обеспечению безопасности государства, его населения и процессов внутри частных компаний [12].

Несмотря на большое число исследований, посвященных проблемам борьбы с незаконными финансовыми операциями посредством методов искусственного интеллекта и применения искусственных нейронных сетей, сегодня данная проблема остается малоизученной с точки зрения практики. Литературный обзор позволяет установить недостаточную степень развития прикладных решений и скрытия их механизмов работы, что особенно характерно для частных коммерческих компаний. Тем не менее, мы можем выделить некоторые исследования, которые посвящены отдельным аспектам работы с незаконными финансовыми транзакциями.

Примечательной является работа Ю.М. Бекетной, которая проводит сравнение методов машинного обучения для выявления сомнительных операций клиентов. Автор раскрывает структуру алгоритмов финансового мониторинга, и, опираясь на открытые данные финансовой отчетности банковских организаций, проводит корреляцию между результатами работы алгоритмов и лицензированием банков (отзыв лицензий). По итогам исследования автор показывает, какие проблемы позволяет решить использование алгоритмов обнаружения аномалий и их классификации. Ключевой эффект от использования нейронных сетей – оптимизация работы специалистов ввиду автоматической обработки больших объемов информации, что несет за собой коммерческую выгоду для банков, и, следовательно, на перспективу может рассматриваться в качестве прикладного способа решения проблем [13].

А.А. Меньщиков и М.Ю. Федосенко фокусируются на более малой проблеме – поиск оптимальных методов предварительной обработки данных платежей для целей преодоления влияния ограничений несбалансированности классов. В качестве первоосновы раскрываются гибридные методы использования алгоритмов искусственного интеллекта, что позволяет создать более верные условия для принятия решений и реализации поставленных алгоритмических задач [14]. С.П. Корнюхина и О.Р. Лапонина в этом вопросе следуют позиции применения алгоритмов машинного обучения, что позволяет выявлять угрозы и проявления нестабильности системы [15].

Аномальное финансовое поведение, несмотря на его некоторые специфические черты, может выявляться в системах за счет широкого числа решений. Ярким примером эффективного использования искусственного интеллекта для целей выявления аномального поведения является анализ работы с файлами на устройстве, что представлено в работе И.В. Машечкина, М.И. Петровского и Д.В. Царева. Авторы выделяют следующие возможности подобных систем:

- выявление авторизации пользователя в системе, идентификация конкретного лица, осуществляющего действия в системе;
- выявление нецелевого использования устройств, материалов и корпоративных ресурсов;
- выявление доступа и обращения к общим корпоративным документам, которые не предназначены для данного пользователя, что создает потенциал для предостережения утечки данных [16].

Описанные операции в очередной раз указывают на необходимость работы с теми аспектами, в которых задействуется человек и его ресурсы. Аналогичные условия и проблемы выделены в работе И.Б. Саенко, И.В. Котенко и М.Х. Аль-Бари. Авторы считают, что главным местом риска работы являются хранилища данных, в которых необходимо работать с аномалиями пользователей и предостерегать кибератаки на систему. Решение данной задачи раскрывается в структуре построения искусственных нейронных сетей, нацеленных на выявление аномального поведения [17].

Таким образом, проведенный обзор подтверждает прикладное значение и возможности масштабирования систем идентификации аномального поведения пользователей, отдельных процессов или компонентов при работе с данными на основе искусственного интеллекта. Прикладное значение раскрывается в структуре реального использования систем обнаружения для выработки мер и системных мероприятий,

основанных на нейросетевом подходе [18]. Все это свидетельствует о реальных перспективах использования нейронных сетей в задаче классификации аномального поведения в финансовых транзакциях с использованием Python и Keras.

VII. Заключение

В ходе нашего исследования, мы успешно разработали и протестировали модель нейронной сети для классификации аномального поведения в финансовых транзакциях. Модель, основанная на четырехслойной архитектуре и обученная с использованием оптимизатора Adam, показала обещающие результаты. Используя обширный датасет из 100 000 финансовых транзакций, мы обучили модель, которая достигла точности 88% в идентификации аномальных транзакций. Важно подчеркнуть, что, несмотря на значительный дисбаланс классов в нашем датасете (где только 0.5% транзакций были мошенническими), модель показала способность довольно точно определять аномалии. Это открывает большие возможности для применения данного подхода в реальной среде, где мошеннические транзакции также обычно составляют небольшую долю от общего числа транзакций.

Пример использования в реальной жизни мог бы быть таким: предположим, у нас есть крупный банк, который проводит миллионы транзакций каждый день. Внедрение такой модели в инфраструктуру банка позволило бы автоматически сканировать каждую транзакцию на предмет подозрительной активности, значительно уменьшая вероятность успешного мошенничества и улучшая общую безопасность клиентов.

Например, если система определяет транзакцию как потенциально мошенническую, она может автоматически блокировать эту транзакцию и отправлять уведомление соответствующему отделу безопасности для дальнейшего рассмотрения. Такой подход значительно облегчает работу специалистов по безопасности, так как они могут сосредоточиться на конкретных случаях, отмеченных системой, вместо того чтобы проходить через миллионы транзакций вручную.

В дальнейшем, мы планируем исследовать более сложные модели и методы для улучшения производительности. Существуют перспективы внедрения нашей модели в реальную среду и наблюдения за ее производительностью в долгосрочной перспективе. В целом, данное исследование представляет собой важный шаг вперед в области идентификации мошеннических действий в финансовой сфере. Используя современные технологии машинного обучения, можно значительно улучшить безопасность финансовых операций и защитить клиентов от потенциального мошенничества.

Библиография

[1] A. Mauboussin "Dataset of Financial Transactions, Labeled with Intent and Expense Category," Timescale, 02 07 2022. [Online]. Available: https://www.surgehq.ai/blog/financial-transactions-dataset-annotated-with-intent-and-expense-category. [Accessed 02 07 2023].

[2] A.G. Marakhtanov, E.O. Parenchenkov, N.V. Smirnov, "Determination of electronic fraud by machine learning methods in the case of an unbalanced dataset," *Bulletin of the Perm National Research Polytechnic University. Electrical engineering, information technology, control systems*, no. 36, pp. 80-95, 2020.

[3] K.A. Kuzmin, “Neural networks as a tool for detecting credit card fraud,” *URAO Bulletin*, no. 5, pp. 136-140, 2014.

[4] E.G. Milkova, "The use of digital transformation and artificial intelligence in the fight against corruption," *International Journal of Applied Sciences and Technologies "Integral"*, no. 2, pp. 247-252, 2021.

[5] N.Sh. Vatolkina, O.P. Fedotkina, V.G. Feklin, “Digital Financial Assets: Technological Possibilities for Regulation and Control,” *Vestnik TSEU*, no. 3(103), pp. 96-110, 2022.

[6] V.A. Tveritinova, "Automation as a Means of Improving the Efficiency of Specialized Depository Employees," *E-Scio*, no. 4, pp. 1-7, 2023.

[7] A.A. Safonov, "On the use of artificial intelligence by law enforcement officers in order to detect and investigate crimes," *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, no. 3, pp. 173-175, 2023.

[8] M.A. Zheludkov, “Justification of the need to adapt the activities of law enforcement agencies to the conditions of the digital transformation of the criminal environment,” *Lex Russica*, no. 4(173), pp. 63-70, 2021.

[9] F.V. Bezgachev, "The use of artificial intelligence (neural networks) in police activities," *Law and Power*, no. 3, pp. 78-82, 2023.

[10] S.L. Larionova, “Mechanisms to combat fraud in online financial services systems,” *Financial Markets and Banks*, no. 3, pp. 47-52, 2023.

[11] E.G. Bagreeva, N.E. Ismailov, L.M. Bobyleva, "Artificial intelligence as a counteraction to fraud in the banking sector," *Eurasian Advocacy*, no. 2(57), pp. 90-95, 2022.

[12] D.V. Reznik, “Artificial neural networks. security use case analysis,” *The Scientific Heritage*, no. 67, pp. 50-53, 2021.

[13] Yu.M. Beketnova, “Comparative Analysis of Machine Learning Methods for Identifying Signs of Involvement of Credit Institutions and Their Clients in Dubious Transactions,” *Finance: Theory and Practice*, Vol. 25, no. 5, pp. 186-199, 2021.

[14] A.A. Menshchikov, M.Yu. Fedosenko, “Methods and approaches to payment data preprocessing under the condition of strong class imbalance,” *StudNet*, no. 9, pp. 1-16, 2021.

[15] S.P. Kornyukhina, O.R. Laponina, “Investigation of the possibilities of deep learning algorithms for protection against phishing attacks,” *International Journal of Open Information Technologies*, Vol. 11, no. 6, 2023.

[16] I.V. Mashechkin, M.I. Petrovsky, D.V. Tsarev, "Methods of machine learning for analyzing user behavior when working with text data in information security problems," *Bulletin of the Moscow University. Series 15. Computational Mathematics and Cybernetics*, no. 4, pp. 33-48, 2016.

[17] I.B. Saenko, I.V. Kotenko, M.Kh. Al-Bari, “Using Artificial Neural Networks to Detect Anomalous Behavior of Data Center Users,” *Cybersecurity Issues*, no. 2(48), pp. 87-97, 2022.

[18] K.N. Kolyutsky, "Neural network approach to detecting anomalies in the information system," *Bulletin of the Moscow University of Finance and Law*, no. 1, pp. 49-52, 2012.

Using neural networks in the problem of classifying anomalous behavior in financial transactions using Python and Keras

A. A. Kochnev

***Abstract*. The purpose of this work is to study and develop neural networks for the problems of classifying anomalous behavior in financial transactions using Python and Keras. To achieve this goal, a dataset was chosen, consisting of 100,000 financial transactions, data was preprocessed, the architecture of the neural network was designed, and the process of its training was disclosed. The basis of the developed architecture is the input layer, which consists of 30 neurons corresponding to 30 features in our data. The output layer of the architecture is two layers that confirm or deny fraudulent transactions. The basis of the output layer is the softmax activation function, which generates probabilities for each class. One of the most important advantages of the developed neural network is the efficiency of activation functions, which is based on the use of ReLU (Rectified Linear Unit) for the input and hidden layers. The model was trained for 50 epochs using the Adam optimization algorithm and a batch size of 32. Adam was chosen as the optimizer, which provides faster and more stable convergence. Based on the results of training in 50 epochs, an accuracy of 88% was achieved. It is important to emphasize that, despite the significant imbalance of classes in the dataset, the model showed the ability to accurately detect anomalies. This opens up great opportunities for applying this approach in a real environment, where fraudulent transactions also usually make up a small proportion of the total number of transactions.**

Keywords — abnormal behavior, neural networks, financial transactions, Python and Keras, Rectified Linear Unit, classification of anomalous behavior.

REFERENCES

[1] A. Mauboussin "Dataset of Financial Transactions, Labeled with Intent and Expense Category," Timescale, 02 07 2022. [Online]. Available: https://www.surgehq.ai/blog/financial-transactions-dataset-annotated-with-intent-and-expense-category. [Accessed 02 07 2023].

[2] A.G. Marakhtanov, E.O. Parenchenkov, N.V. Smirnov, "Determination of electronic fraud by machine learning methods in the case of an unbalanced dataset," *Bulletin of the Perm National Research Polytechnic University. Electrical engineering, information technology, control systems*, no. 36, pp. 80-95, 2020.

[3] K.A. Kuzmin, "Neural networks as a tool for detecting credit card fraud," *URAO Bulletin*, no. 5, pp. 136-140, 2014.

[4] E.G. Milkova, "The use of digital transformation and artificial intelligence in the fight against corruption," *International Journal of Applied Sciences and Technologies "Integral"*, no. 2, pp. 247-252, 2021.

[5] N.Sh. Vatolkina, O.P. Fedotkina, V.G. Feklin, "Digital Financial Assets: Technological Possibilities for Regulation and Control," *Vestnik TSEU*, no. 3(103), pp. 96-110, 2022.

[6] V.A. Tveritinova, "Automation as a Means of Improving the Efficiency of Specialized Depository Employees," *E-Scio*, no. 4, pp. 1-7, 2023.

[7] A.A. Safonov, "On the use of artificial intelligence by law enforcement officers in order to detect and investigate crimes," *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, no. 3, pp. 173-175, 2023.

[8] M.A. Zheludkov, "Justification of the need to adapt the activities of law enforcement agencies to the conditions of the digital transformation of the criminal environment," *Lex Russica*, no. 4(173), pp. 63-70, 2021.

[9] F.V. Bezgachev, "The use of artificial intelligence (neural networks) in police activities," *Law and Power*, no. 3, pp. 78-82, 2023.

[10] S.L. Larionova, "Mechanisms to combat fraud in online financial services systems," *Financial Markets and Banks*, no. 3, pp. 47-52, 2023.

[11] E.G. Bagreeva, N.E. Ismailov, L.M. Bobyleva, "Artificial intelligence as a counteraction to fraud in the banking sector," *Eurasian Advocacy*, no. 2(57), pp. 90-95, 2022.

[12] D.V. Reznik, "Artificial neural networks. security use case analysis," *The Scientific Heritage*, no. 67, pp. 50-53, 2021.

[13] Yu.M. Beketnova, "Comparative Analysis of Machine Learning Methods for Identifying Signs of Involvement of Credit Institutions and Their Clients in Dubious Transactions," *Finance: Theory and Practice*, Vol. 25, no. 5, pp. 186-199, 2021.

[14] A.A. Menshchikov, M.Yu. Fedosenko, "Methods and approaches to payment data preprocessing under the condition of strong class imbalance," *StudNet*, no. 9, pp. 1-16, 2021.

[15] S.P. Kornyukhina, O.R. Laponina, "Investigation of the possibilities of deep learning algorithms for protection against phishing attacks," *International Journal of Open Information Technologies*, Vol. 11, no. 6, 2023.

[16] I.V. Mashechkin, M.I. Petrovsky, D.V. Tsarev, "Methods of machine learning for analyzing user behavior when working with text data in information security problems," *Bulletin of the Moscow University. Series 15. Computational Mathematics and Cybernetics*, no. 4, pp. 33-48, 2016.

[17] I.B. Saenko, I.V. Kotenko, M.Kh. Al-Bari, "Using Artificial Neural Networks to Detect Anomalous Behavior of Data Center Users," *Cybersecurity Issues*, no. 2(48), pp. 87-97, 2022.

[18] K.N. Kolyutsky, "Neural network approach to detecting anomalies in the information system," *Bulletin of the Moscow University of Finance and Law*, no. 1, pp. 49-52, 2012.