А. Смирнова

НЕЙРОСЕТЕВЫЕ МОДЕЛИ В БОРЬБЕ С ФИНАНСОВЫМ МОШЕННИЧЕСТВОМ

В настоящей статье рассматривается проблема обнаружения мошеннических действий в финансовой сфере с использованием нейросетевых моделей. Проводится анализ основных схем мошенничества и их развития. Осуществляется сравнительный анализ нейросетевых архитектур с позиций их возможностей и несовершенств. Значительное внимание уделяется также этическим аспектам, связанным с данными технологиями, включая проблему ложных срабатываний. На основе проделанной работы сделаны выводы о необходимости совершенствования систем обнаружения мошенничества и перспективах дальнейших исследований.

Ключевые слова: нейросетевые модели, нейросети, мошенничество, схемы мошенничества, финансовые операции, обнаружение мошеннических операций.

УДК: 004.032.26

EDN: NDRJZS

DOI: 10.51905/2073–038_2025_2S_130

Введение

В последние десятилетия активно развивается финансово-банковская сфера: многие операции теперь совершаются через смартфоны, минуя банки и даже карты. Это значительно повышает удоб-

Анна Олеговна Смирнова – *студентка 2-го курса факультета информационных технологий ФГАОУ ВО «Московский политехнический университет» (г. Москва).*

Гульшат Батыровна Худайбердиева – *научный руководитель: ассистент кафедры «Информатика и информационные технологии» ФГАОУ ВО «Московский политехнический университет» (г. Москва).*

ство использования и снижает затраты. Одновременно с этим растет и угроза мошенничества, принимающего все более сложные и изощренные формы. Так, по данным Центробанка, только в третьем квартале 2024 г. в России было зафиксировано 348,6 тыс. мошеннических операций на 9,3 млрд руб., причем 98,6% суммы составили хищения у физических лиц. В сравнении с тем же периодом 2023 г. объем подобных операций увеличился в 2,6 раза. [4]

Существующие системы борьбы с мошенничеством часто оказываются неэффективными, поскольку излишне строгие и недостаточно гибкие, чтобы успевать за новыми схемами обмана. Одним из перспективных решений являются нейросетевые модели, способные за короткий срок обрабатывать большое количество информации, выявлять сложные закономерности и быстро адаптироваться к новым условиям.

Цель представленной работы – проанализировать возможности и ограничения нейросетевых моделей в выявлении мошеннических операций в банковской и финансовой сферах, а также рассмотреть этические аспекты и риски, связанные с их внедрением.

Распространенные схемы мошенничества

Рассмотрим ключевые виды мошеннических схем, чтобы лучше определить требования к нейросетевым моделям. Современное мошенничество направлено на захват персональных данных и конфиденциальной информации с целью наживы. Такие схемы быстро адаптируются к новым технологиям и изменениям в финансово-банковской сфере и становятся все более изощренными.

Один из старейших, но до сих пор актуальных методов – фишинг – интернет-мошенничество, когда под видом официальных источников рассылаются ссылки с целью получения паролей, данных банковских карт и прочей конфиденциальной информации. Зачастую в письме также содержатся угрозы или предостережения. Перейдя по вредоносной ссылке, пользователь может получить программу-шпиона или вирус. Существуют и более изворотливые виды фишинга: направленный фишинг, уэйлинг (от англ. *whaling*, «китобойный промысел»), смишинг и многие другие. Так, еще в 2006 г. в США средний ущерб от одной фишинговой атаки составил 1244 долл. А в 2024-м, по данным ТАСС, количество фишинговых атак в России выросло на 425%, было заблокировано в общей сложности более 22 тыс. фишинговых сайтов [5].

Другой опасный вид мошенничества – социальная инженерия, когда воздействие направлено на людей. С помощью последовательных манипуляций преступники убеждают человека добровольно раскрыть пароли или перевести средства на определенный счет. Преступники играют на эмоциях – страхе, доверии, срочности. Принципы соци-

альной инженерии строятся на понимании человеческой психологии и поведения. Основная цель – нарушить психологическое равновесие и побудить к совершению определенных действий.

Отдельно стоит упомянуть отмывание денег – процесс легализации преступных доходов. Классическая схема включает три этапа: размещение, наслоение, интеграция. Сначала деньги вводятся в оборот через поддельный бизнес или ставки, затем усложняются множеством транзакций, часто с трансграничными переводами, и, наконец, возвращаются в легальный оборот через инвестиции или фиктивные компании. Отмывание преступных денег наносит значительный удар по мировой экономике, укореняя теневые схемы и безнаказанность коррупционных структур.

Мошенники, как и технологии, не стоят на месте. Так, относительно недавно появилась технология *Deepfake* (дипфейк) – метод, позволяющий с помощью искусственного интеллекта синтезировать аудио- или видеоконтент. Алгоритмы анализируют сотни часов материала, в результате получается реалистичное сообщение, например от близкого человека или начальника. Отличить подделку сложно, особенно в стрессовой ситуации, что делает критическое мышление важнейшим инструментом защиты от современных мошеннических схем.

Финансовые потери от мошенничества исчисляются миллиардами долларов в год. Больше всего страдают частные лица, но и банки несут значительные убытки, компенсируя клиентам потери и теряя доверие. Противодействие требует вложений в системы защиты, что также увеличивает расходы.

Среди самых популярных методов защиты – многофакторная аутентификация, анализ поведенческих паттернов пользователей или ведение баз данных подозрительных операций. Однако количество мошеннических операций не сокращается. Традиционные алгоритмы, основанные на фиксированных правилах и уже известных сценариях, оказываются неэффективными в рамках постоянно развивающихся преступных схем.

Как показывает практика, подобная борьба с мошенниками превращается в вечную гонку. В такой ситуации вектор решения перемещается на использование нейросетевых моделей. В отличие от классических методов, нейросети, постоянно обрабатывая большие объемы данных, способны быстрее реагировать на изменяющуюся обстановку, а также распознавать скрытые закономерности в мошеннических действиях.

Возможности нейросетей в выявлении мошеннических операций

Сегодня стремительное развитие технологий машинного обучения и нейросетей приводит к их активному использованию в различ-

ных сферах жизни общества. Так, в России в настоящее время лидером по внедрению технологий искусственного интеллекта является именно финансовый сектор [1].

В классической антифрод-системе (от англ. *anti-fraud* – защита от мошенничества) предусмотрен фиксированный набор критериев, при отклонении от которых операция отправляется на дополнительную проверку, иногда с участием фрод-аналитика. В последние годы различные финансовые организации все активнее совершенствуют антифрод-системы: расширяется обмен данными, внедряется машинное обучение и анализ больших данных. Так, уже в 2017 г., вскоре после массового внедрения антифрод-систем в банках, на 15% снизилось количество кредитов с подозрительными признаками [2].

Проверки такого рода становятся эффективнее с использованием нейросетей. Подобные системы способны анализировать огромные объемы данных и выявлять сложные закономерности, демонстрируя превосходство перед неавтоматизированными проверками. Рассмотрим несколько основных преимуществ. Первое – гибкость и возможность ускоренной адаптации к новым схемам мошенничества. Нейросети обучаются на свежих данных и подстраиваются под новые схемы. Второе – минимизация ложных срабатываний. Стандартные алгоритмы часто блокируют легитимные операции, вызывая неудобства у клиентов, тогда как нейросети могут более точно и субъективно оценивать риски. И третье – автоматическое самообучение. По мере появления новых данных нейросетевые модели становятся все более эффективными, а случаи их ошибок – минимальными.

Особенно эффективны рекуррентные нейросети (*RNN*), способные анализировать не только основные параметры транзакций (сумму, частоту и т. д.), но и поведенческие шаблоны, геолокацию и другие данные. Так, если в аккаунт зашли из другой страны и сразу попытались перевести крупную сумму, система может пометить операцию как подозрительную. Как следствие, использование нейросетей позволяет автоматизировать и ускорить антифрод-проверки, в том числе снижая нагрузку на сотрудников. Это особенно важно в условиях роста количества транзакций и увеличения сложности мошеннических схем.

Основная задача нейросетевых моделей в выявлении мошеннических операций – классификация транзакций и обнаружение аномалий. Нейросети способны выявлять патологии в данных и указывающих на мошенничество действиях пользователей. Это особо полезно для пресечения и установления новых преступных схем. Затем ИИ относит транзакцию к легитимным или неправомерным. Дополнительно нейросети эффективно применяются в системах анализа поведения пользователей (*User Behavior Analysis*), что значительно усиливает антифрод-защиту. Например, генеративный искусственный

интеллект может автоматически создавать текстовые или аудиосообщения при подозрительных действиях, предупреждая пользователя о рисках или поясняя причины отказа в проведении операции.

Однако, несмотря на все преимущества, использование нейросетей имеет и ряд ограничений. И прежде всего – необходимость в большом объеме данных для обучения и эффективной работы механизма. Это требует регулярного пополнения и обновления баз данных с аномалиями и мошенническими операциями. Следующее ограничение – сложность интерпретации результатов: не все нейросети способны объяснить ход своих «мыслей» и работают по принципу «черного ящика», что приводит к сложности аудита и отсутствию прозрачности решений. Такая проблема требует постоянного анализа результатов, применения дополнительных проверок или использования нескольких алгоритмов отбора одновременно. Кроме того, нейросети чувствительны к качеству исходных данных – ошибки или неполные сведения могут значительно снижать их эффективность. Ну и конечно высокие вычислительные и финансовые затраты: анализ больших данных требует ресурсов, дорогостоящего оборудования, инфраструктуры. Таким образом, внедрение нейросетей связано с рисками, однако их грамотное применение способно значительно повысить безопасность и оптимизировать систему.

Хочется отметить, что использование нейросетевых моделей для автоматического обнаружения мошеннических операций в финансово-банковской сфере может стать большим шагом в совершенствовании антифрод-систем. Благодаря их возможностям могут возрасти точность и скорость обнаружения мошенничества, что в свою очередь сократит финансовые потери организаций и повысит доверие пользователей к финансовым сервисам.

Этический аспект использования нейросетевых моделей

Говоря об этической стороне внедрения такой технологии, стоит затронуть тему ложных срабатываний – ошибочного определения легальных транзакций мошенническими. Хотя использование ИИ сокращает их количество, полное искоренение практически невозможно. Это создает неудобства клиентам, подрывает доверие к банкам и может привести к опустошению клиентской базы.

В истоках возникновения ложных срабатываний лежат различные факторы. Часто это может быть связано с качеством и полнотой исходных данных: недостаток актуальных примеров или наличие в них ошибок может негативно влиять на результаты работы системы. Важную роль играет и человеческий фактор – ошибки в настройке модели или выборе архитектуры способны многократно увеличить количество сбоев. Кроме того, нейросетевая модель не всегда способна

правильно интерпретировать поведение человека. Например, клиент, накопивший на отпуск, может внезапно перевести крупную сумму из-за границы. С точки зрения алгоритма это выглядит подозрительно, но на деле – абсолютно легально. Такие ситуации трудно учесть в логике машинной обработки.

Ложные срабатывания отражаются не только на клиентах, но и на организациях: неожиданные блокировки счетов и потеря доступа к средствам в критический момент вызывает раздражение и снижает доверие. В долгосрочной перспективе это может привести к оттоку клиентов, ухудшению репутации и росту мошенничества. Кроме того, при больших количествах ложных срабатываний организации вынуждены тратить дополнительные ресурсы на разбирательства, перенастройку или полную замену системы.

Минимизировать ложные срабатывания можно через улучшение качества исходных данных и их обновление, с учетом новых мошеннических схем, а также расширяя набор критериев проверки. Эффективно и использование гибридных систем, сочетающих машинное обучение и экспертное мнение.

Помимо ложных срабатываний, использование нейросетевых моделей порождает и другие этические вопросы. Например, на основе статистки модель может дискредитировать группы людей на основании их дохода или возраста. Так, по данным Банка России, наиболее уязвимыми считаются проживающие в городе мужчины 25–44 лет, со средним образованием и уровнем дохода [6]. Проблемной остается также сложность интерпретации решений нейросети и неясность, кто несет за них ответственность. Это особенно актуально в рамках растущего интереса к регулированию искусственного интеллекта и его роли в принятии критически важных решений.

Таким образом, внедрение нейросетевых моделей требует не только технологического совершенствования алгоритмов, но и этико-правовой проработки, обеспечивающей как защиту интересов клиентов, так и устойчивость самой банковской системы.

Реальные примеры использования нейросетевых моделей

Нейросетевые модели уже активно внедряются в банковскую сферу, в частности в антифрод-системы. Преимущества таких систем подтверждаются реальными примерами, однако на практике выявляются определенные ограничения и неудачи. В этом разделе рассмотрим несколько примеров уже совершенного внедрения этой технологии в деятельность финансовых организаций.

Так, одним из успешных примеров стала компания *PayPal*, которая смогла снизить уровень мошенничества до рекордных 0,32% при среднем показателе в отрасли 1,32% с помощью использования ма-

шинного обучения [3]. В 2018 г. *HSBC* (от англ. *The Hongkong and Shanghai Banking Corporation*), один из крупнейших финансовых конгломератов в мире, также успешно внедрил нейросети для множественной защиты от мошенничества, что существенно повысило эффективность мониторинга транзакций. Ну и яркий пример использования нейросетевых моделей для борьбы с мошенничеством – отечественный финансовый сектор. Так, Сбер совместно со Сколтехом разработали новый метод обучения нейросетей, повысивший точность их работы на 20% [7].

Таким образом, современные нейросетевые модели уже доказали свою эффективность в обнаружении мошеннических операций на реальных примерах. Однако любая новая технология может столкнуться с рядом трудностей при внедрении. Например, *Deutsche Bank* не смог предотвратить незаконные операции Дж. Эпштейна, за что был оштрафован на 150 млн долл. [8]. Аналогичная ситуация произошла с австралийским банком *Westpac*: система не выявила связи транзакций с преступной деятельностью, что привело к рекордному штрафу в размере 1,3 млрд долл. и отставке руководства [9].

Эти примеры демонстрируют, что нейросетевые модели в банковской сфере и, в частности, в антифрод-системах остаются развивающейся технологией, что требует постоянного мониторинга и корректировки. Однако тренд на внедрение ИИ продолжает набирать обороты, и дальнейшие исследования в этой области позволят минимизировать риски, обеспечивая более высокий уровень безопасности финансовых операций.

* * *

Внедрение нейросетевых моделей в сферу борьбы с финансовым мошенничеством представляет огромный потенциал. Подобные технологии позволяют не только оперативно выявлять аномалии и подозрительные транзакции, но и адаптироваться к новым схемам мошенничества, тем самым снижая финансовые потери как банка, так и его клиентов, а также повышая уровень безопасности операций. Тем не менее внедрение нейросетей связано с рядом ограничений и рисков – от зависимости от качества данных до разнообразных этических вопросов.

На сегодняшний день применение нейросетевых моделей уже показывает хорошие результаты, однако не стоит забывать, что это все еще вспомогательный инструмент, требующий постоянного контроля и совершенствования.

В качестве перспектив развития этой технологии хочется выделить разработку более прозрачных (объяснимых) алгоритмов искусственного интеллекта, развитие и совершенствование механизмов

адаптации и выявления новых мошеннических схем. Актуальным направлением остается развитие гибридных нейросетевых моделей, сочетающих в себе машинное обучение и экспертное человеческое мнение. Кроме того, важной задачей является формирование правовой базы, регулирующей применение нейросетей в банковской сфере, с целью минимизации рисков как для клиентов, так и для самих организаций.

Таким образом, в долгосрочной перспективе нейросетевые модели для автоматического обнаружения мошеннических операций способны не только повысить устойчивость банковских систем к преступным действиям, но и изменить сам подход к обеспечению финансовой безопасности, сделав его более гибким, точным и адаптивным к постоянно развивающимся угрозам.

Список литературы / References

1. Искусственный интеллект в банках // TAdviser. *https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_в_банках* (дата обращения 01.03.2025).

2. Что такое антифрод: задачи и методы // FIS Group. 07.10.2020. https://fisgroup.ru/blog/antifraud-zadachy-i-metody/ (дата обращения 03.03.2025).

3. Нейросети: как искусственный интеллект помогает в бизнесе и жизни // Habr. 13.09.2017. https://habr.com/ru/amp/publications/337870/ (дата обращения 04.03.2025).

4. Смена методики увеличила мошенничество вдвое // РБК. 10.12.2024. https://www.rbc.ru/newspaper/2024/12/10/6756dfb09a79477dd39360b6 (дата обращения 01.02.2025).

5. Количество фишинговых атак в РФ выросло на 425% в 2024 г. // ТАСС. 23.10.2024. https://tass.ru/obschestvo/22215161 (дата обращения 01.03.2025).

6. Кибер мошенничество: портрет пострадавшего // Банк России. https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения 03.03.2025).

7. Учёные из Сколтеха и Сбера на 20% повысили точность нейросетей для банковской сферы // Сколтех. 27.02.2025. https://www.skoltech.ru/news/researchers-skoltech-and-sber-increased-accuracy-neural-networks-banking-20 (дата обращения 04.03.2025).

8. Superintendent Lacewell Announces DFS Imposes $150 Million Penalty on Deutsche Bank AG in Connection with Its Relationship with Jeffrey Epstein and Correspondent Banking Relationships with Danske Bank Estonia and FBME Bank // New York State Department of Financial Services. 06.07.2020. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202007071 (дата обращения 06.03.2025).

9. Westpac ordered to pay $1.3 billion penalty // AUSTRAC. 20.10.2020. https://www.austrac.gov.au/news-and-media/our-recent-work/westpac-penalty-ordered(дата обращения 04.03.2025).

10. *Антонов А. Ю*. Риски мошенничества в банковской сфере и пути их минимизации // Экономика и социум. 2023. №1–1 (104). https://cyberleninka.ru/article/n/riski-moshennichestva-v-bankovskoy-sfere-i-puti-ih-minimizatsii (дата обращения 04.03.2025).

11. *Гарифуллин И. М*. Использование нейросетей для выявления мошеннических транзакций // Инновационная наука. 2021. №3. https://cyberleninka.ru/article/n/ispolzovanie-neyrosetey-dlya-vyyavleniya-moshennecheskih-tranzaktsiy (дата обращения 03.03.2025).

12. Искусственный интеллект в банковской сфере: как AI поднимает финансовый сектор // *AllSee Team*. https://allsee.team/ai_in_banking_rising_finance (дата обращения 02.03.2025).

13. Искусственный интеллект в финансах // *Sber Developers*. 10.01.2025. https://developers.sber.ru/help/gigachat-api/ai-in-finance (дата обращения 06.03.2025).

14. *К. И. Лихоузов* Применение алгоритмов машинного обучения на платформе *Hadoop* для эффективного анализа и классификации мошеннических операций в банковской сфере // Вестник РосНОУ. 2024. №3. https://vestnik-rosnou.ru/сложные-системы-модели-анализ-и-управление-complex-systems-models-analysis-management/2024/3/45 (дата обращения 05.03.2025).

15. *Каблучко Юлия Владимировна*. Применение искусственного интеллекта в банковской сфере // Вопросы науки и образования. 2018. №16 (28). https://cyberleninka.ru/article/n/primenenie-iskusstvennogo-intellekta-v-bankovskoy-sfere (дата обращения: 04.03.2025).

16. *Мацкевич Наталия Викторовна, Костевич Елизавета Игоревна.* Противодействие мошенничеству в банковской сфере Республики Беларусь с использованием технологии *ML* и анализа *BIG DATA* // Nazariy va amaliy tadqiqotlar xalqaro jurnali. 2023. №9. https://cyberleninka.ru/article/n/protivodeystvie-moshennichestvu-v-bankovskoy-sfere-respubliki-belarus-s-ispolzovaniem-tehnologii-ml-i-analiza-big-data (дата обращения 05.03.2025).

17. *Очилов Акрам Одилович, Коновалова Ольга Александровна, Аборкина Екатерина Оскаровна, Кадиров Лутфулла Халимович, Акимов Степан Андреевич и Тураева Мехринисо Рустамовна*. 2024. Об использовании генеративного искусственного интеллекта в банковской сфере // Economics and Innovative Technologies. 12, 4 (Aug. 2024), 97–108. https://iqtisodiyot.tsue.uz/journal/index.php/iit/article/view/577 (дата обращения 07.03.2025).

18. *Римайте Кристина Кистуто.* Роль и место искусственного интеллекта в обнаружении и предотвращении информационных угроз,

направленных на финансовые организации // Хроноэкономика. 2023. №4 (42). https://cyberleninka.ru/article/n/rol-i-mesto-iskusstvennogo-intellekta-v-obnaruzhenii-i-predotvraschenii-informatsionnyh-ugroz-napravlennyh-na-finansovye (дата обращения 02.03.2025).

19. Система анализа фотоизображений (САФИ) // Global CIO. 15.12.2014 https://globalcio.ru/discussion/1780/ (дата обращения 04.03.2025).

20. *Скребцова Тамара Васильевна, Гришанова Светлана Валерьевна.* Финансовые мошенничества в банковской сфере // Экономический журнал. 2020. №3 (59). https://cyberleninka.ru/article/n/finansovye-moshennichestva-v-bankovskoy-sfere (дата обращения 05.03.2025).

21. *Черемисин Д. Г., Мкртчян В. Р.* Нейросети: применение и развитие в различных отраслях // Символ науки. 2023. №6–2. https://cyberleninka.ru/article/n/neyroseti-primenenie-i-razvitie-v-razlichnyh-otraslyah (дата обращения 04.03.2025).

Дата предоставления рукописи: 26 июня 2025 г.

About the Author

Anna O. Smirnova – *a Second Year Student of the Faculty of Information Technology at the Moscow Polytechnic University (Moscow).*
smirnova2005.05@mail.ru

Gulshat B. Khudaiberdieva – *a Scientific Supervisor: an Assistant Professor of the Department «Informatics and Information Technology» at the Moscow Polytechnic University (Moscow).*
lesolurner@gmail.com

Neural Network Models in Combating Against Financial Fraud

Annotation. This article examines the problem of detecting fraudulent activities in the financial sector using neural network models. It analyzes the main fraudulent schemes and their evolution. A comparative analysis of neural network architectures is provided, taking into account their capabilities and imperfections. Considerable attention is also s given to the ethical aspects, associated with these technologies, including the problem of false positives. Based on the completed work, conclusions were drawn about the need to improve fraud detection systems and the prospects for further research.

Keywords: neural network models, neural networks, fraud, fraud schemes, financial transactions, detection of fraudulent transactions.

08.00.13 Математические и инструментальные методы в экономике