ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРИНЯТИЕ РЕШЕНИЙ
ARTIFICIAL INTELLIGENCE AND DECISION MAKING

УДК 004.056.53 **DOI: 10.18413/2518-1092-2025-10-4-0-5**

Абрамов К.В.[1]
Балабанова Т.Н.[2]
Белов А.С.[2]
Новиков А.Г.[3]

НЕЙРОННЫЕ СЕТИ В ЗАДАЧЕ РАСПОЗНАВАНИЯ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ С КРЕДИТНЫМИ КАРТАМИ

[1)] ООО "ЯНДЕКС", ул. Льва Толстого, 16, г. Москва, 119021, Россия
[2)] Белгородский государственный национальный исследовательский университет, ул. Победы, 85, г. Белгород, 308015, Россия
[3)] Белгородский университет кооперации, экономики и права, ул. Садовая, 116а, г. Белгород, 308023, Россия

e-mail: sozonova@bsuedu.ru, belov_as@bsuedu.ru

Аннотация
Задача распознавания мошеннических операций с кредитными картами является в настоящее время актуальной, поскольку наблюдается значительный рост их использования населением. В то же время, методы и алгоритмы, используемые организациями, обслуживающими кредитные карты далеки от совершенства. В настоящее время для решения данной задачи используются методы и алгоритмы машинного обучения. В данной работе представлено исследование по использованию для решения задачи распознавания мошенничества с кредитными картами нейронной сети. Рассмотрены проблемы наличия обучающих датасетов, имеющихся в открытом доступе и проблемы настройки нейронной сети исходя из политики организации.
Ключевые слова: машинное обучение; нейронные сети; бинарная классификация; обеспечение безопасности данных
Для цитирования: Абрамов К.В., Балабанова Т.Н., Белов А.С., Новиков А.Г. Нейронные сети в задаче распознавания мошеннических операций с кредитными картами // Научный результат. Информационные технологии. – Т.10, №4, 2025. – С. 61-69. DOI: 10.18413/2518-1092-2025-10-4-0-5

Abramov K.V.[1]
Balabanova T.N.[2]
Belov A.S.[2]
Novikov A.G.[3]

NEURAL NETWORKS IN THE TASK OF RECOGNIZING CREDIT CARD FRAUD

[1)] YANDEX, 16 Lev Tolstoy St., Moscow, 119021, Russia
[2)] Belgorod State National Research University, 85 Pobedy St., Belgorod, 308015, Russia
[3)] Belgorod University of Cooperation, Economics and Law, 116a Sadovaya St., Belgorod, 308023, Russia

e-mail: sozonova@bsuedu.ru, belov_as@bsuedu.ru

Abstract
The problem of recognizing credit card fraud is currently relevant due to the significant increase in the use of credit cards by the population. At the same time, the methods and algorithms used by credit card companies are far from perfect. Machine learning methods and algorithms are currently being used to solve this problem. The paper presents some current research being conducted in this area. This paper presents a study on the use of a neural network for credit card fraud detection. The availability of publicly available training datasets and the challenges of configuring a neural

network based on organizational policies are discussed. It demonstrates ways to tune the neural network under consideration to better recognize fraudulent transactions as such, while observing a greater number of legitimate transactions classified as fraudulent, and vice versa. It also demonstrates ways to tune the neural network to minimize the classification of legitimate transactions as fraudulent, while observing the omission of fraudulent transactions.
Keywords: machine learning; neural networks; binary classification; data security
For citation: Abramov K.V., Balabanova T.N., Belov A.S., Novikov A.G. Neural Networks in the Task of Recognizing Credit Card Fraud // Research result. Information technologies. – T.10, №4, 2025. – P. 61-69. DOI: 10.18413/2518-1092-2025-10-4-0-5

В настоящее время задача обнаружения мошенничества с кредитными картами является довольно актуальной, поскольку все большее количество людей предпочитают не использовать денежные средства в наличном виде, а пользоваться различного вида картами. Одной из задач организации и управления информационной безопасностью предприятий, предоставляющих населению услуги по выпуску и обслуживанию кредитных карт, является обеспечение безопасности их использования и, тем самым, обеспечение сохранности финансовых активов и персональных данных клиентов.

Для предотвращения хищения средств клиентов организации используют различные средства информационной безопасности:

- Программные средства защиты от внутренних и внешних угроз электронной коммерции, к которым можно отнести многофакторную аутентификации, различного рода экраны, антивирусные программы и т.д.
- Аудит информационной безопасности (ИБ) и мониторинг сети, что позволяет минимизировать риски утечки информации и совершения мошеннических операций с кредитными картами.
- Антифрод-системы, которые позволяют предприятиям отслеживать мошеннические операции.

С развитием методов и алгоритмов машинного обучения в целом и нейронных сетей в частности и их использованием в различных областях жизнедеятельности человека, появилась возможность их использования для более качественного распознавания мошеннических операций с кредитными картами [1, 2].

Кредитные карты используются для различных транзакций по всему миру. Онлайн-покупки товаров и услуг стали всё более распространёнными в повседневной жизни. Интернет-платежи становятся все более распространённым типом онлайн-транзакций. Банковская система предлагает электронные деньги, электронную коммерцию и электронные услуги посредством интернет-транзакций.

По мере расширения использования кредитных карт во всем мире увеличивается также вероятность того, что злоумышленник может украсть данные кредитной карты и использовать их для совершения мошенничества [3].

Мошенничество определяется как любое действие, предпринятое с целью обмана с целью получения денег без ведома держателя карты или банка-эмитента. Для совершения мошенничества с кредитными картами может быть использовано множество методов. Теряя или крадя карты, изготавливая поддельные или фальшивые карты, копируя фишинг, скимминг или крадя данные у продавца, удаляя или заменяя магнитную полосу на карте, на которой хранится информация пользователя [4].

В современном мире бизнеса проблема мошенничества с кредитными картами представляет собой одну из наиболее острых и актуальных угроз. Для разработки действенных стратегий противодействия этому явлению, ключевым является глубокое понимание способов и методов, используемых злоумышленниками. Мошеннические действия с кредитными картами осуществляются различными путями. В сущности, под мошенничеством с кредиткой подразумевается несанкционированное использование чужой кредитной карты в личных интересах, без ведома и согласия законного владельца карты и выпустившего ее банка. Важно отметить, что

лицо, совершающее данное деяние, не имеет никаких законных прав или связей ни с держателем карты, ни с финансовым учреждением, выпустившим ее, и не планирует вступать в контакт с владельцем карты или возмещать понесенные расходы.

Махинации с кредитными картами реализуются различными способами:

- Преднамеренное использование чужой учетной записи или персональных данных для обмана.
- Неправомерное применение кредитной карты в корыстных целях без разрешения владельца.
- Предоставление ложных сведений о карте для получения товаров или услуг.

Операции без физического предъявления карты, например, онлайн-покупки, становятся все более опасными, так как продавец (интернет-магазин) лишается преимуществ очной верификации, таких как проверка подписи или удостоверения личности с фотографией. Практически невозможно осуществить какие-либо проверки в "реальном мире", необходимые для идентификации личности, совершающей транзакцию. Это делает интернет привлекательной средой для мошенников. Исследования показывают, что уровень онлайн-мошенничества в 12-15 раз превосходит показатели "офлайн" мошенничества. Однако технологические инновации предлагают перспективы для предотвращения мошеннических операций.

Для защиты от мошеннических операций с кредитными картами банки и платежные системы внедряют многоуровневые системы безопасности. К ним относятся: использование сложных алгоритмов шифрования данных, двухфакторная аутентификация, мониторинг транзакций в режиме реального времени для выявления подозрительной активности и гео-ограничения, позволяющие блокировать операции из определенных стран или регионов.

Развитие технологий машинного обучения также играет ключевую роль в борьбе с мошенничеством [5, 6]. Алгоритмы машинного обучения способны анализировать огромные объемы данных и выявлять закономерности, которые могут указывать на мошеннические операции [7]. Это позволяет банкам и платежным системам оперативно реагировать на угрозы и предотвращать неправомерные транзакции.

Так, для распознавания мошеннических операций используются методы классического машинного обучения [8, 9], представленные в различных работах, например, такие как случайный лес [10-12], логистическая регрессия [13], генетические алгоритмы [14], анализ главных компонент [15], а так же различные комбинации методов [16-18],

Нейронные сети, благодаря своей способности к обучению на больших объемах данных и выявлению сложных взаимосвязей, могут обнаруживать мошеннические схемы, которые остаются незамеченными при использовании традиционных методов, основанных на простых пороговых значениях [19, 20]. В отличие от правил, заданных вручную, нейронные сети способны адаптироваться к изменяющимся тактикам мошенников, постоянно совершенствуя свои алгоритмы обнаружения. Одним из ключевых преимуществ нейронных сетей является их способность учитывать множество факторов одновременно, а не просто опираться на отдельные переменные счета.

Например, нейронная сеть может анализировать частоту транзакций, суммы покупок, географическое местоположение, время суток и даже тип продавца, чтобы выявить аномальное поведение, которое может указывать на мошенничество. Объединив эти данные, сеть может создать более полную картину поведения пользователя и точнее оценить вероятность мошеннической активности.

Более того, нейронные сети могут обучаться на данных, содержащих информацию о различных типах мошенничества, что позволяет им выявлять не только известные схемы, но и новые, еще не зафиксированные случаи. Это особенно важно в условиях, когда мошенники постоянно разрабатывают новые методы обмана, стремясь обойти стандартные системы защиты. Внедрение нейронных сетей в системы обнаружения мошенничества требует значительных инвестиций в инфраструктуру и экспертизу, однако потенциальные выгоды в виде снижения убытков от мошенничества и повышения лояльности клиентов оправдывают эти затраты. В конечном итоге, использование передовых технологий, таких как нейронные сети, становится

необходимым условием для эффективной борьбы с мошенничеством в современном банковском секторе.

Все чаще ряд проблем в сфере финансовых услуг рассматривается с точки зрения задач распознавания образов, для которых могут быть разработаны решения на основе нейронных сетей [21].

Обнаружение мошенничества включает в себя мониторинг действий групп пользователей с целью оценки, выявления или предотвращения нежелательного поведения, которое включает в себя мошенничество, вторжение и невыполнение обязательств. Это очень актуальная проблема, требующая внимания таких направлений исследований, как машинное обучение и наука о данных, где решение этой проблемы может быть автоматизировано.

Проблема обнаружения мошенничества с кредитными картами особенно сложна с точки зрения обучения, поскольку она характеризуется различными факторами. Наиболее значащими факторами являются:

- недостаток информационного обеспечения в виде датасетов для тренировки моделей;
- дисбаланс классов (количество действительных транзакций значительно превышает количество мошеннических.

Существует определенная проблема наличия именно открытых наборов данных для обучения и тестирования алгоритмов обнаружения мошенничества с кредитными картами, построенных на основе машинного обучения.

Данная проблема обусловлена тем, что компании, которые осуществляют выпуск и поддержку использования кредитных карт, стремятся не раскрывать методы и алгоритмы машинного обучения, которые ими используются для принятия решения об одобрении или отклонении платежей. Данная мера принимается с целью повышения безопасности в сфере обслуживания клиентов, но ведет к тому, что открытых наборов данных для разработки и тестирования алгоритмов машинного обучения для обнаружения мошенничества с кредитными картами практически нет.

В открытых источниках на данный момент удалось найти только один набор данных, пригодный для обучения и тестирования алгоритмов машинного обучения при решении задачи обнаружения мошенничества с кредитными картами. Набор данных можно найти по адресу https://oreil.ly/hljvo.

Данные в наборе являются анонимизированными. Для анонимизации данных использовался метод, который называется анализ главных компонент (principal component analysis, PCA).

В наборе данных представлено 284807 транзакций, среди которых только 492 являются мошенническими. Таким образом, набор данных является сильно несбалансированным. Следовательно, если осуществлять тренировку алгоритмов машинного обучения без предварительной обработки данных, то следует ожидать, что модель будет гораздо лучше определять легитимные операции, а не мошеннические. С одной стороны, это может удовлетворять компании, которые занимаются кредитными картами, поскольку их деятельность направлена на позитивное отношение клиентов ним. То есть, для компании лучше пропустить ряд мошеннических операций, чем ошибиться в классификации легитимной операции, что вызовет негодование клиента. Однако, с другой стороны, правильное определение мошеннических операций является важным аспектом для деятельности компании в целом.

Общий вид используемого набора данных представлен на рисунке 1.

	Time	V1	V2	V3	V4	V5	V6	V7	V8	V9	...	V28	Amount	Class
0	0.0	-1.359807	-0.072781	2.536347	1.378155	-0.338321	0.462388	0.239599	0.098698	0.363787	...	-0.021053	149.62	0
1	0.0	1.191857	0.266151	0.166480	0.448154	0.060018	-0.082361	-0.078803	0.085102	-0.255425	...	0.014724	2.69	0
2	1.0	-1.358354	-1.340163	1.773209	0.379780	-0.503198	1.800499	0.791461	0.247676	-1.514654	...	-0.059752	378.66	0
3	1.0	-0.966272	-0.185226	1.792993	-0.863291	-0.010309	1.247203	0.237609	0.377436	-1.387024	...	0.061458	123.50	0
4	2.0	-1.158233	0.877737	1.548718	0.403034	-0.407193	0.095921	0.592941	-0.270533	0.817739	...	0.215153	69.99	0

Рис. 1. Фрагмент набора данных легитимных и мошеннических операций с кредитными картами
Fig. 1. A fragment of a dataset of legitimate and fraudulent credit card transactions

Основной интерес для решения задачи распознавания мошеннических операций с кредитными картами представляет столбец Class. Именно в нем содержится информация о легитимности операции с кредитной картой. Если операция законная метка Class = 0, если операция мошенническая метка Class = 1.

В данной работе для решения задачи обнаружения мошенничества с кредитными картами, которая представляет собой бинарную классификацию, используются методы глубокого обучения.

Основные аспекты построения нейронной сети:

1. Архитектура: полносвязная нейронная сеть

2. Входной слой нейронной сети должен принимать исходные параметры операций с кредитными картами, представленные в наборе данных (в данном случае это 29 значений).

3. Первый слой представляет собой полносвязный слой с N нейронами и функцией активации ReLU (Rectified Linear Unit). Данная функция активации возвращает максимум из входного значения и нуля, позволяет избежать проблемы затухания градиента и ускоряет обучение. Количество нейронов N = 128, 256, 512.

4. На выходе необходимо получить ответ о принадлежности данных к одному из двух классов. Для этого в разрабатываемой сети в последнем слое используется функция активации sigmoid. По факту, эта функция активации дает вероятность принадлежности объекта к классу. В данном случае вероятность принадлежности транзакции к мошеннической.

5. Используемая функция потерь – Binary Cross-Entropy (BCE), которая измеряет эффективность модели классификации, выход которой — вероятностное значение между 0 и 1. Математическое представление функции потерь BCE:

$$BCE = -(yln(p) + (1 - y)\ln(1 - p)), \quad (1)$$

где y – фактическая метка (0 или 1),

p – предсказанная вероятность того, что образец принадлежит положительному классу (классу 1).

Формула вычисляет потери для каждого отдельного образца, а затем усредняет их по всем образцам.

Архитектура построенной нейронной сети представлена на рисунке 2.

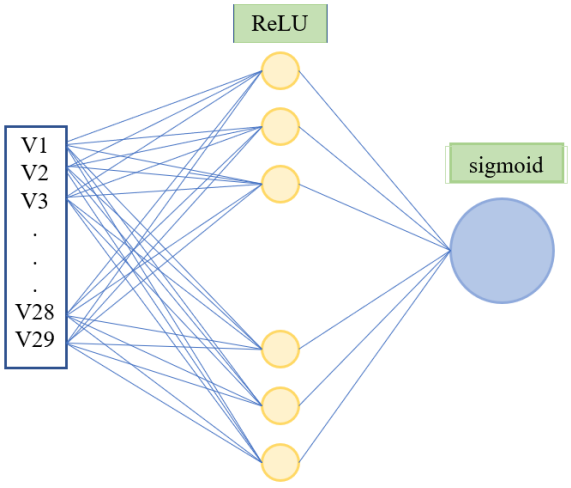

Рис. 2. Архитектура нейронной сети для бинарной классификации
Fig. 2. Neural network architecture for binary classification

Для обучения сети все данные разделялись на две подвыборки: 20% тестовая выборка, 80% обучающая. В процессе обучения был использован оптимизатор adam. В процессе обучения модель проходила 10 эпох по всему обучающему набору данных при этом каждый пакет состоит из 100 образцов.

Построенная нейронная сеть является относительно простой с точки зрения архитектуры, однако она имеет значительное количество обучаемых параметров. В таблице 1 представлено количество обучаемых параметров в зависимости от количества нейронов N.

Таблица 1

Количество обучаемых параметров сети

Table 1

Number of trainable network parameters

№	N	Количество обучаемых параметров
1	128	3969
2	256	7937
3	512	15873

Учитывая особенность набора данных, который используется в эксперименте, заключающуюся в том, что данные являются сильно несбалансированными (мошеннических операций гораздо меньше, чем легитимных), большинство распространенных метрик качества работы сети не будут показательными, так как если нейронная сеть просто будет давать результат «легитимная операция» для всех операций, то точность составит 99,8%.

Более показательным видом оценки в данном случае является матрица ошибок. На рисунке 3 представлены матрицы ошибок для трех реализаций нейронной сети: N = 128, 256, 512.

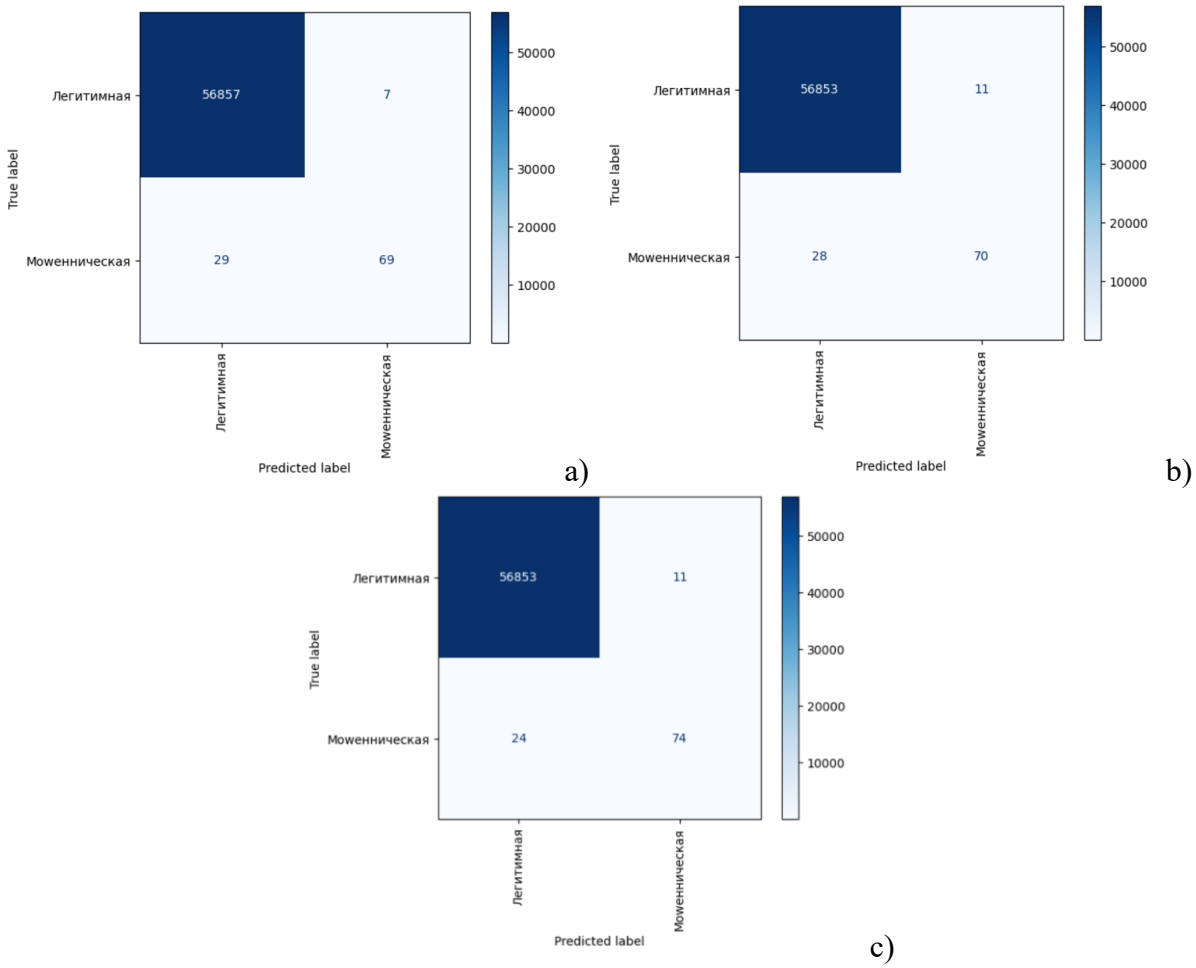

Рис. 3. Матрицы ошибок решения задачи: a) N=128, b) N=256, c) N=512
Fig. 3. Error matrices of the problem solution: a) N=128, b) N=256, c) N=512

По результатам эксперимента видно, что наибольшее количество мошеннических операций распознала нейронная сеть с N=512 (74, что меньше 70 при N=256 и 69 при N=128). Таким образом, представляется целесообразным использовать сеть с N=128.

Однако, следует заметить, что при решении данной задачи важным является политика организации, которая обслуживает кредитные карты. Большинство организаций склоняются к тому, чтобы минимизировать количество ошибок принятия легитимной операции в качестве мошеннической. Это связано с сохранением лояльности клиентов, поскольку блокировка легитимных операций, как правило, хуже сказывается на общем впечатлении клиентов о компании, нежели пропуск мошеннической операции. В этом случае представленная нейронная сеть может быть настроена таким образом, чтобы минимизировать ошибку принятия легитимной операции в качестве мошеннической. В этом случае целесообразно использовать сеть при N=128, так как она меньше всего легитимных операций отнесла к мошенническим (7, по отношению к 11 при N=256 и N=512).

Еще одним способом настройки нейронной сети является задание относительной значимости всех классов при обучении. В этом случае веса классов задают разную важность при расчёте функции потерь. Это позволит минимизировать влияние несбалансированности классов при обучении сети. В данном случае настройка должна быть выполнена таким образом, чтобы нейронная сеть ориентировалась в большей степени на минимизацию отнесения легитимных операций к мошенническим.

Результаты эксперимента при увеличении значимости для одного класса в 100 раз представлены на рисунке 4.

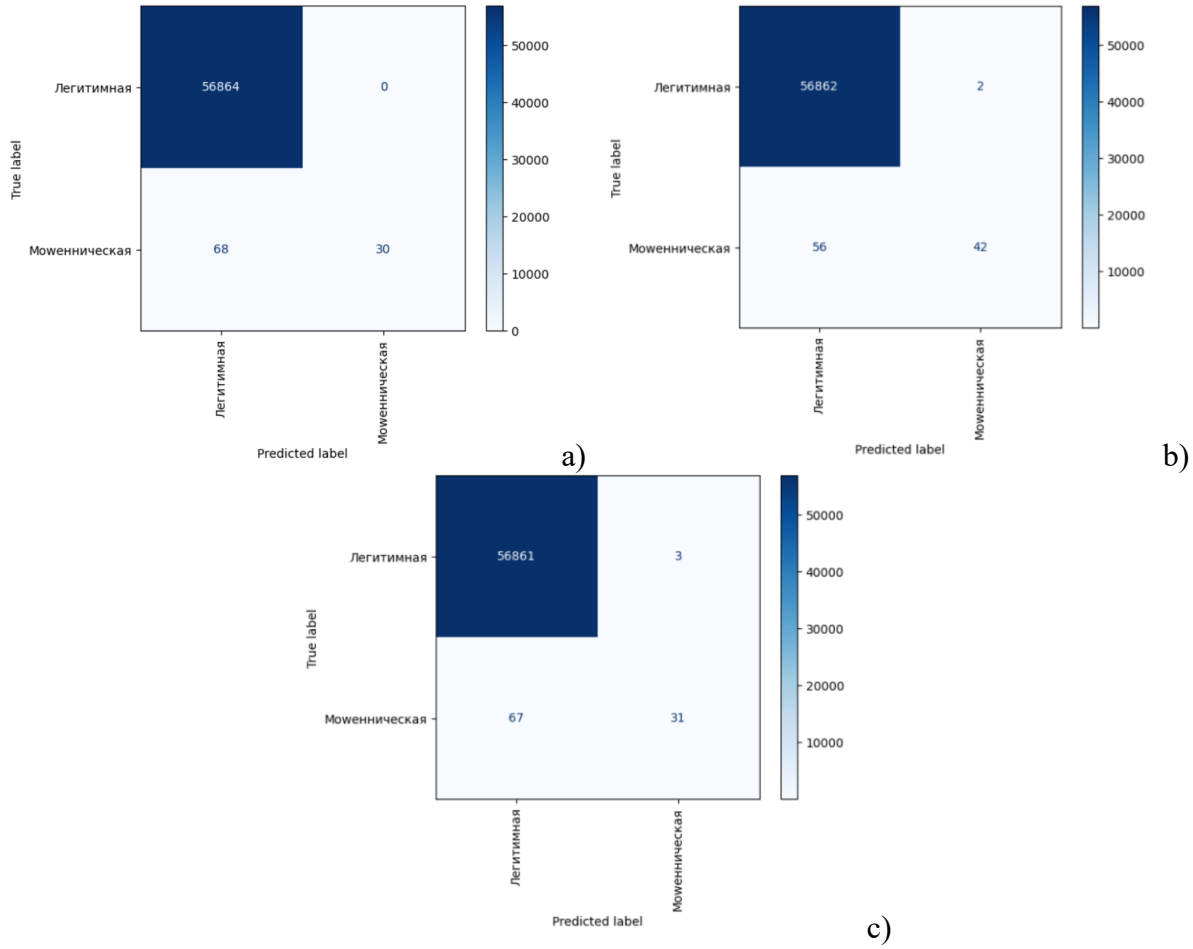

Рис. 4. Матрицы ошибок решения задачи при задании относительной значимости классов при обучении: a) N=128, b) N=256, c) N=512

Fig. 4. Error matrices for solving the problem when the relative importance of classes is set during training: a) N=128, b) N=256, c) N=512

По результатам эксперимента видно, что во всех трех случаях резко уменьшилось количество легитимных транзакций, которые были приняты мошенническими. При N=128 таких оказалось 0, при N=256 всего 2, при N=512 только 3. Однако, следует заметить, что и количество мошеннических операций, которые были распознаны как мошеннические, так же значительно уменьшилось.

Таким образом, настройка представленного нейросетевого решения для распознавания мошеннических операций с кредитными картами во многом зависит от политики компании и акцентах при ее использовании. В целом, представленное решение позволяет осуществлять поставленную задачу с достаточно высоким качеством.

Список литературы

References

1. Benchaji I., Douzi S., El Ouahidi B. Credit card fraud detection Model Based on LSTM recurrent neural networks. Journal of Advances in Information Technology. Vol. 12. no. 2. 2021. Pp. 113–118. DOI: 10.12720/jait.12.2.113-118

2. Credit Card Fraud Detection: 2025 Trends and Interventions, FICO, 2025.

3. Ali M.A., Azad M.A., Centeno M.P., Hao F., van Moorsel A. Consumer-facing technology fraud: Economics, attack methods and potential solutions. Future Generation Computer Systems, 100, 2019. Pp. 408-427.

4. Budhram T. Lost, stolen or skimmed: Overcoming credit card fraud in South Africa. South African Crime Quarterly, 40, 2012. Pp. 31-37.

5. "Credit card fraud detection and risk management strategies" (2024/2025).

6. "Credit Card Fraud Data Analysis and Prediction Using Machine Learning" (2024/2025).

7. Kasongo S.M. An advanced intrusion detection system for IIoT based on GA and tree based algorithms. IEEE Access. 2021; 9: 113199–113212

8. Khatri S., Arora A., Agrawal A.P. Supervised machine learning algorithms for credit card fraud detection: a comparison. In: 10th international conference on cloud computing, data science & engineering (Confluence); 2020. p. 680-683.

9. Serzhan Y. Fraud Detection in Credit Card Transactions using Machine Learning: A Comparative Analysis. 2025.

10. Sundaravadivel P. et al. Optimizing credit card fraud detection with random forests and deep learning techniques. 2025.

11. Ghiasi M.M., Zendehboudi S. Application of decision tree-based ensemble learning in the classification of breast cancer. Comput in Biology and Medicine. 2021; 128: 104089.

12. Lingjun H., Levine R.A., Fan J., Beemer J., Stronach J. Random forest as a predictive analytics alternative to regression in institutional research. Pract Assess Res Eval. 2020; 23(1): 1

13. Robles-Velasco A., Cortés P., Muñuzuri J., Onieva L. Prediction of pipe failures in water supply networks using logistic regression and support vector classification. Reliab Eng Syst Saf. 2020; 196: 106754.

14. Seera M., Lim C.P., Kumar A., Dhamotharan L., Tan K.H. An intelligent payment card fraud detection system. Ann Oper Res 2021; 1–23

15. Hemavathi D., Srimathi H. Effective feature selection technique in an integrated environment using enhanced principal component analysis. J Ambient Intell Hum Comput. 2021; 12(3): 3679–3688.

16. Saheed Y.K., Hambali M.A., Arowolo M.O., Olasupo Y.A. Application of GA feature selection on Naive Bayes, random forest and SVM for credit card fraud detection. In: 2020 international conference on decision aid sciences and application (DASA); 2020. p. 1091–1097

17. Li Y., Jia M., Han X., Bai X.S. Towards a comprehensive optimization of engine efficiency and emissions by coupling artificial neural network (ANN) with genetic algorithm (GA). Energy. 2021; 225: 120331.

18. Ahmed K.H. A credit card fraud detection approach based on ensemble learning. 2025.

19. Trippi R.T., Turban E. (eds), Neural Networks in Finance and Investing, Probus Publishing Company. 1993.

20. Bhuiyan M. "Enhancing Credit Card Fraud Detection: A Comprehensive Study of Machine Learning Approaches" (2024).

21. Mienye I.D., Sun Y. Improved heart disease prediction using particle swarm optimization based stacked sparse autoencoder. Electronics. 2021;10(19):2347

Абрамов Кирилл Владиславович, Аналитик-разработчик, ООО "ЯНДЕКС", г. Москва, Россия
Балабанова Татьяна Николаевна, кандидат технических наук, доцент, заведующий кафедры автоматизированных систем и технологий, Белгородский государственный национальный исследовательский университет, г. Белгород, Россия
Белов Александр Сергеевич, кандидат технических наук, доцент, доцент кафедры автоматизированных систем и технологий, Белгородский государственный национальный исследовательский университет, г. Белгород, Россия
Новиков Алексей Геннадиевич, магистрант кафедры информационной безопасности, Белгородский университет кооперации, экономики и права, г. Белгород, Россия

Abramov Kirill Vladislavovich, Analytik Developer, YANDEX, Moscow, Russia
Balabanova Tatyana Nikolaevna, Candidate of Technical Sciences, Associate Professor, Head of the Department of Automated Systems and Technologies, Belgorod State National Research University, Belgorod, Russia
Belov Alexander Sergeevich, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Automated Systems and Technologies, Belgorod State National Research University, Belgorod, Russia
Novikov Aleksey Gennadievich, Master's Student of the Information Security Department, Belgorod University of Cooperation, Economics and Law, Belgorod, Russia