2. Зайнидинов Х.Н., Турапов У.У. Информатив параметрларнинг мажмуасини шакллантиришда кўп мезонли дисперсия усули. //Форғона политехника институти.Илмий техника журнали. ISSN 2181-7200, Форғона шаҳри, 2017,Том 21, №2, стр.145-148

3. Турапов У.У.,Маллаев О.У. Алгоритм идентификации информативных меридианов по методу “Риодораку”.Научно-аналитический журнал “Научная перспектива” №5(75). Технические науки. г.Уфа 25.05.2016.,стр. 149-153.

4. Турапов У.У.,Маллаев О.У.,Позилова Ш.Х. Статистическая оценка информативности количественных признаков по локальным и многокритериальным методам для сложного процесса. Научно-аналитический журнал “Научная перспектива” №5(75).Технические науки.г.Уфа 25.05.2016.,стр. 145-148.

DETECTING FINANCIAL FRAUD IN UZBEKISTAN’S DIGITAL ECOSYSTEM: A COMPARATIVE ANALYSIS OF MACHINE LEARNING AND DATA BALANCING TECHNIQUES

Zairova R.Sh.
2nd-year student, Economics
Almalyk Branch of National University of Science and Technology «MISIS», Republic of Uzbekistan rushanashzairova@gmail.com

Annotation: The report discusses the growing risk of financial fraud within Uzbekistan’s digital banking ecosystem, focusing on unauthorized loans obtained through stolen personal information. Conventional rule-based detection frameworks fail to deliver reliable results, generating excessive false alarms and struggling to adapt to evolving scam tactics. By deploying machine learning models such as Random Forest, XGBoost, neural networks, and anomaly detection algorithms that paired with data balancing techniques like SMOTE, the research achieves significant improvements in fraud identification accuracy.

Keywords: digital banking ecosystem, unauthorized loans, machine learning, data balancing techniques, financial fraud, false alarms, personal data, anomaly detection algorithms.

ОБНАРУЖЕНИЕ ФИНАНСОВОГО МОШЕННИЧЕСТВА В ЦИФРОВОЙ ЭКОСИСТЕМЕ УЗБЕКИСТАНА: СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ И БАЛАНСИРОВКИ ДАННЫХ

Заирова Р.Ш.
Студентка 2-курса, направление «Экономика»
Алмалыкский филиал Национального исследовательского технологического университета «МИСИС», Республика Узбекистан
rushanashzairova@gmail.com

Аннотация: В статье рассмотрен растущий риск финансового мошенничества в цифровой банковской экосистеме Узбекистана, при этом особое внимание уделяется проблеме несанкционированного получения кредитов с использованием украденных персональных данных. Традиционные системы обнаружения, основанные на правилах, не дают надежных результатов, генерируя избыточное количество ложных срабатываний и с трудом адаптируясь к эволюционирующим тактикам злоумышленников. Благодаря внедрению моделей машинного обучения, таких как Random Forest, XGBoost, нейронные сети и алгоритмы обнаружения аномалий,

в сочетании с методами балансировки данных (например, SMOTE), исследование достигает значительного повышения точности идентификации мошенничества.

Ключевые слова: цифровая банковская экосистема, несанкционированные кредиты, машинное обучение, методы балансировки данных, финансовое мошенничество, ложные срабатывания, персональные данные, алгоритмы обнаружения аномалий.

O'ZBEKISTON RAQAMLI EKOTIZIMIDA MOLIYAVIY FIRIBGARLIKNI ANIQLASH: MASHINADA O'QITISH VA MA'LUMOTLARNI BALANSLASH USULLARINI QIYOSIY TAHLIL QILISH

Zairova R.Sh.
2-kurs talabasi, «Iqtisodiyot» yo'nalishi
Milliy texnologik tadqiqotlar universiteti «MISIS»ning Olmaliq shahridagi filiali,
O'zbekiston Respublikasi
rushanashzairova@gmail.com

Annotatsiya: Ushbu maqolada O'zbekiston raqamli bank ekotizimida moliyaviy firibgarlik xavfi ortib borayotgani ko'rib chiqilib, bunda o'g'irlangan shaxsiy ma'lumotlardan foydalangan holda ruxsatsiz kredit olish muammosiga alohida e'tibor qaratilmoqda. Qoidalarga asoslangan an'anaviy aniqlash tizimlari ishonchli natijalar bermaydi, ortiqcha yolg'on ishlanmalarni keltirib chiqaradi va tajovuzkorlarning evolyutsion taktikalariga zo'rg'a moslashadi. Random Forest, XGBoost, neyron tarmoqlar va anomaliyalarni aniqlash algoritmlari kabi mashinada o'qitish modellarini joriy etish orqali ma'lumotlarni muvozanatlash usullari (masalan, SMOTE) bilan birgalikda tadqiqot firibgarlikni identifikatsiyalash aniqligini sezilarli darajada oshirishga erishmoqda.

Kalit so'zlar: raqamli bank ekotizimi, ruxsat etilmagan kreditlar, mashinada o'qitish, ma'lumotlarni balanslashtirish usullari, moliyaviy firibgarlik, yolg'on ishga tushirishlar, shaxsiy ma'lumotlar, anomaliyalarni aniqlash algoritmlari.

Introduction. The rapid growth of digital financial transactions is accompanied by a corresponding increase in fraudulent activities, which intensifies existing challenges within the financial sector. The expansion of banking services, mobile payment systems, and digital platforms enhances accessibility and creates new vulnerabilities that are actively exploited by fraudsters to implement increasingly sophisticated schemes. This has a direct impact on the security of banks and payment systems, resulting in financial losses, a decline in customer trust, and elevated risk levels. In recent years, Uzbekistan has experienced a notable rise in cases where loans are issued by commercial banks in the names of individuals without their knowledge. The misuse of personal data has become a key factor contributing to the increase in such incidents, which has exceeded 40%[7].

Traditional fraud detection systems relying on rigid rules and predefined patterns falter under evolving threats. They lack adaptability to emerging attack vectors and cannot evolve with shifting financial behaviors, rendering them obsolete. As digital transactions surge in volume and complexity, these inflexible systems generate excessive false positives, strain operational capacity, and hinder real-time response. Analysts spend disproportionate time investigating non-issues, delaying accurate risk assessments and weakening overall decision quality. Each advancement in financial digitization introduces new vulnerabilities, demanding a fundamental reevaluation of current defenses and the adoption of dynamic

[7] Ombudsman.uz (2025), "In 2024, fraud cases related to the issuance of loans increased by 42% - Ombudsman", official news portal of the Authorized Person of the Oliy Majlis for Human Rights, available at: https://ombudsman.uz/ru/news/2025/01/27/2024-yilda-kredit-rasmiylashtirishga-oid-firibgarlik-holatlari-42-foizga-oshgan-ombudsman.

countermeasures. Machine learning-driven systems, powered by big data analytics and artificial intelligence, now offer a responsive alternative. These tools supersede static rule sets, uncovering concealed fraud patterns even in anonymous user activity by identifying subtle behavioral anomalies. The shift moves security from reactive remediation to preemptive defense: detecting risks early prevents losses before they materialize and strengthens financial systems against disruptive external pressures.

The study focuses on identifying the role of intelligent technologies in combating fraud. The analysis shows that they are more effective than traditional methods: they respond faster, detect suspicious patterns more accurately and reduce the error rate in fraud detection.

Legal framework and classification of cybercrime. Liability for the misappropriation of property through deception or abuse of trust is established under Article 168 of the Criminal Code of the Republic of Uzbekistan. In the context of the digital transformation of the financial sector, particular attention is given to fraud schemes carried out using information technologies. Such offenses are prosecuted under Article 168-1 of the Criminal Code of the Republic of Uzbekistan. Unauthorized access to computer information, including interference with the functioning of information systems, is punishable under Article 278-1 of the Criminal Code of the Republic of Uzbekistan. All these provisions form a unified legal framework aimed at countering threats in the field of financial transactions[8].

The main types of financial fraud include bank card fraud, which involves the unauthorized use of card details and the execution of illegal transactions. Credit fraud is also widespread, where loans are obtained in the names of third parties using their personal data. In addition, significant threats come from fraud schemes in online payments and phishing attacks aimed at obtaining users' confidential information. Criminals often persuade clients through advertisements that falsely present guaranteed success and claimed effectiveness. They also use referral schemes, place urgent calls with time-limited offers, and promote «exclusive» conditions. In some cases, they manipulate displayed income data so that false profit figures appear in user interfaces. All these methods are designed to exploit trust and trigger quick, impulsive decisions.

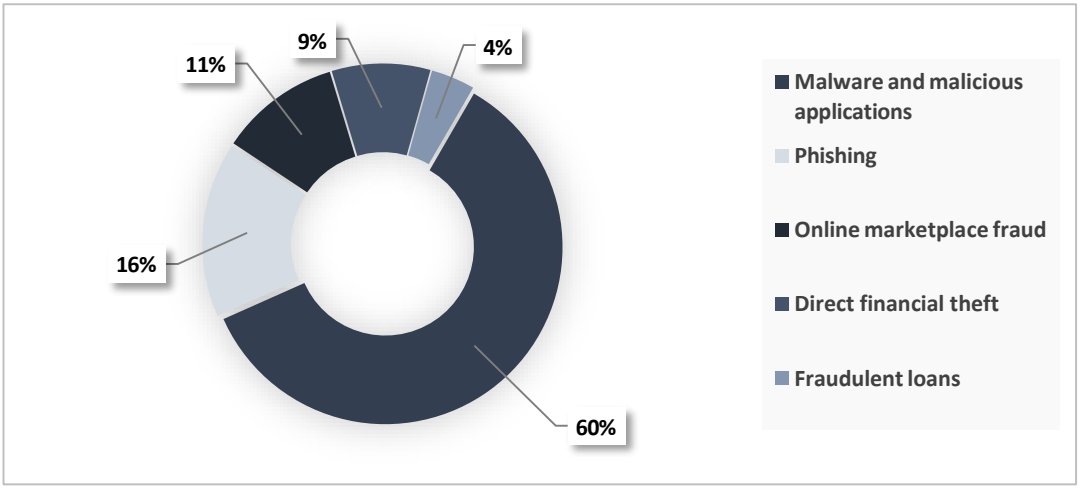

Fig. 1. Structure of cybercrime by type[9]

The majority of incidents are associated with malware and malicious applications, accounting for 60%, which reflects a persistent trend in the spread of malicious software. Phishing, aimed at obtaining personal data, represents 16% of cases. Online fraud accounts for 11%, while direct financial theft makes up 9%. The smallest share, 4%, is related to loans issued under another person's name. Despite their relatively low frequency, such attacks pose a serious threat to financial stability.

[8] Criminal Code of the Republic of Uzbekistan (1994), adopted by the Law of the Republic of Uzbekistan No. 2012-XII, Lex.uz national database of legislation, available at: https://www.lex.uz/acts/111457.

[9] Spot.uz (2025), "The structure of cybercrime in Uzbekistan: statistics and key trends for the current period", business and technology news portal, available at: https://www.spot.uz/ru/2025/05/30/cyber-crime/.

Materials and methods. Traditional methods for identifying financial fraud rely on rigid rule-based systems and manual transaction scrutiny. When predefined thresholds set by experts are met, these systems flag transactions for review, leaving human analysts to assess anomalies and detect signs of deceit. However, their lack of adaptability hampers effective responses in the fast-evolving landscape of digital finance. As fraudsters continuously evolve their techniques, introducing novel schemes at speed, updating detection rules remains slow and dependent on expert intervention. The result is a high volume of false positives, overwhelming investigators and delaying critical actions. Worse still, conventional frameworks fail to uncover sophisticated, multi-layered frauds that have no prior pattern by leaving institutions vulnerable to attacks they cannot anticipate. In light of the accelerating shift toward digital financial ecosystems, these shortcomings render outdated detection models inadequate for safeguarding modern economic systems.

Machine learning is widely used for fraud detection. Its ability to analyze large volumes of transactions and identify non-obvious patterns makes this approach highly effective. The main task is to classify an operation as either «fraud» or «non-fraud». In such scenarios, logistic regression is often applied: it estimates the probability of a fraudulent transaction based on features such as transaction amount, frequency of actions, and the user's geolocation. Decision trees are also used in practice: they build a sequence of conditions, making the decision-making process transparent. The accuracy of these models can reach 85-95%, but only under conditions of class balance and careful data preparation.

International experience in fraud mitigationэ The implementation of intelligent systems in several countries has demonstrated high effectiveness. In the United States, financial institutions have long been using machine learning algorithms to monitor transactions in real time. Such solutions quickly detect suspicious operations and block them before completion. For example, the company PayPal processes billions of transactions in real time, taking into account user behavior, transaction history, and payment context. Thanks to intelligent algorithms, the level of fraudulent transactions has decreased to 0.32% of the total volume. This is almost four times lower than the industry average of 1.32%. As a result, the platform becomes more secure, and customer trust increases[10].

Performance evaluation and analysis. In the course of the study, it was analyzed how different approaches to dataset balancing affect the performance of Random Forest and XGBoost models. The F1-score metric was used to evaluate the results [1].

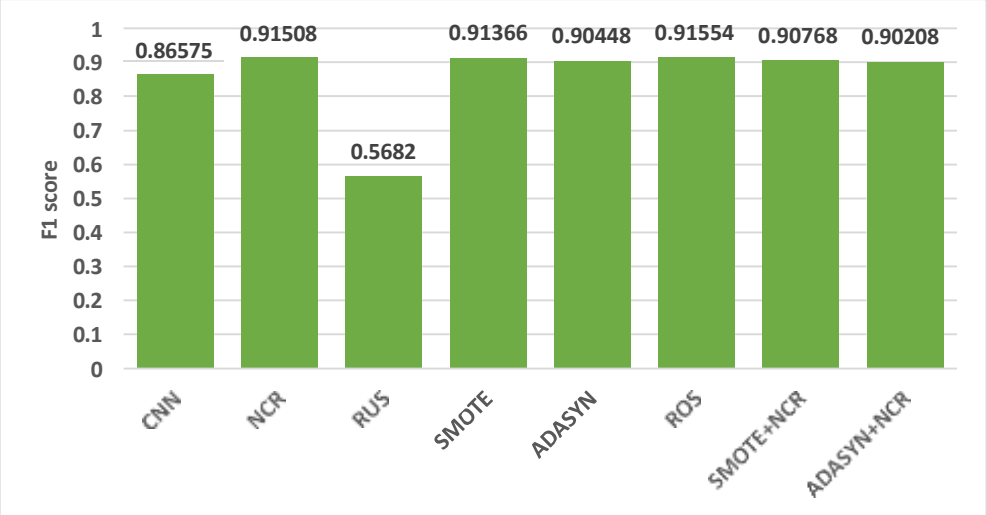

Fig. 2. Evaluation of data balancing techniques in Random Forest using F1-score

[10] Harvard Business School (2024), "PayPal vs. Fraud: Have no fear, Machine Learning is here!", Digital Innovation and Transformation, available at: https://d3.harvard.edu/platform-rctom/submission/paypal-vs-fraud-have-no-fear-machine-learning-is-

here/.

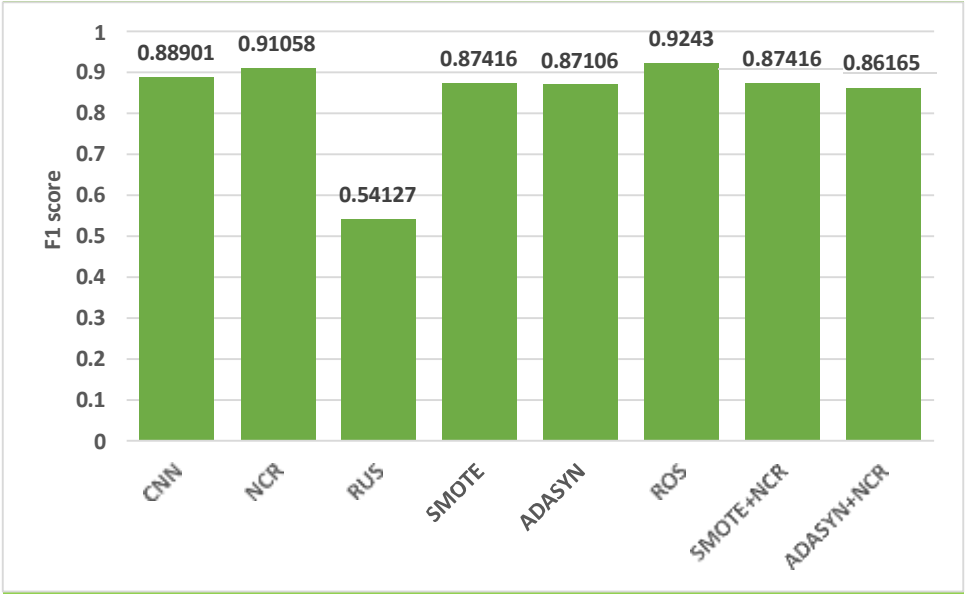

Fig. 3. Evaluation of data balancing techniques in XGBoost using F1-score

Challenges and constraints

The results of the analysis showed that oversampling methods such as ROS, SMOTE, and ADASYN, as well as hybrid approaches combining oversampling and undersampling (e.g., SMOTE+NCR and ADASYN+NCR), are more effective than traditional undersampling strategies. Simple undersampling methods lead to the loss of important information, which results in decreased classification accuracy. This outcome confirms that such approaches are unsuitable for problems with a strong class imbalance.

Neural networks and deep learning methods analyze sequences of operations, identifying hidden patterns in customer behavior that are not accessible to traditional approaches. Recurrent neural networks and LSTM-based architectures are effective in processing time series data, tracking changes in transaction dynamics. Convolutional neural networks work with structured data, detecting unusual combinations of features characteristic of fraudulent scenarios. Real-time data processing can reach up to 100 milliseconds. Such high-speed operation ensures an immediate response in modern banking systems, where delays may lead to financial losses [2].

Anomaly detection methods focus on identifying deviations in behavior without requiring labeled data. Approximately 70-80% of new fraud schemes have no historical analogues. In this context, unsupervised learning algorithms are effective, including clustering methods (k-means, DBSCAN) and isolation-based models such as Isolation Forest. These methods detect outliers in customer behavior, such as a sudden increase in transaction volume, unusual locations, or irregular transaction timestamps. For example, if a user typically spends between 100 and 500 currency units, a sudden transaction of 5000 units is immediately flagged as suspicious [3].

Modern platforms process between 1,000,000 and 10,000,000 transactions per day. Because of machine learning, risks associated with human factors are reduced, as personnel errors and subjectivity in incident assessment are eliminated. The integrated use of these capabilities increases the resilience of systems to emerging forms of financial fraud [4].

Detecting fraudulent transactions is challenging. Their proportion is extremely small compared to regular transactions. Even highly accurate systems that correctly classify the majority of operations face an excessive number of false positives. As a result, many actions are flagged as suspicious, while only a small fraction of them are actually fraudulent. This requires manual verification, which leads to increased time consumption and higher staffing costs. Reducing fraud levels is possible, but only through stronger control measures, which implies a significant increase in security expenses. Organizations are forced

to choose

between the cost of protection and the economic benefit of preventing losses. The situation is further complicated by reputational risks: public disclosure of fraud incidents can negatively affect a company's image. Aggressive blocking of legitimate users, even in the absence of confirmed fraud, undermines trust in the service and damages its reputation [5].

Conclusion. The development of financial technologies directly contributes to the improvement of security methods and the increased reliability of transactions. Intelligent technologies detect suspicious operations with high accuracy, reducing the number of false alarms. Unlike rigid rule-based systems, machine learning algorithms are capable of identifying hidden patterns that previously remained undetected. Such systems adapt to changing conditions by continuously updating behavioral patterns. However, their implementation requires significant computational resources and high-quality data. Without these, their effectiveness decreases. By combining multiple approaches, banks enhance their resilience to attacks. As a result, users gain greater confidence in the security of their transactions.

List of references

1. Doe, J. [et al.] (2024), "Performance evaluation of data balancing techniques in financial fraud detection using machine learning", Procedia Computer Science, Vol. 235, pp. 124-133, doi: 10.1016/j.procs.2024.03.1028.

2. Akhilomen, M. A. [et al.] (2018), "A comparative study of machine learning techniques for credit card fraud detection", Expert Systems with Applications, Vol. 110, pp. 350-362, doi: 10.1016/j.eswa.2018.05.032.

3. Fawcett, T. (2006), "An introduction to ROC analysis", Pattern Recognition Letters, Vol. 27 No. 8, pp. 861-874, doi: 10.1016/j.patrec.2005.10.010.

4. Ngai, E. W. T., Hu, Y. and Wong, Y. H. (2011), "The application of data mining techniques in financial fraud detection: a classification framework and an academic review of literature", Decision Support Systems, Vol. 50 No. 3, pp. 559-569, doi: 10.1016/j.dss.2010.08.006.

5. Prasad, S. S. P. [et al.] (2017), "Deep learning for financial fraud detection", 2017 IEEE International Conference on Computing, Communication and Automation (ICCCA), pp. 1297-1302, doi: 10.1109/CCAA.2017.8229994.

TRANSPORT MASALASINI YECHISHDA MS EXCEL DASTURINING IMKONIYATLARIDAN FOYDALANISH

Ergashev Muzaffar Abdukasimovich
Texnika fanlar doktori (Phd)
Abdirazzoqova Farangiz Haqqul qizi
Abdulla Qodiriy nomidagi Jizzax Davlat Pedagogika Universiteti

Annotatsiya: Ushbu maqolada transport masalasini yechishda Microsoft Excel dasturining imkoniyatlaridan foydalanish usullari ko'rib chiqilgan. Transport masalasining matematik modeli, uning chiziqli dasturlash bilan bog'liqligi hamda MS Excel dasturining "Solver" (Yechuvchi) qo'shimchasidan foydalanib masalani optimallashtirish bosqichlari batafsil yoritilgan. Tarmoq transport masalasiga doir amaliy misol keltirilgan va uning MS Excel muhitida qo'llanilishi ko'rsatilgan. Maqola natijalaridan matematika va informatika o'qituvchilari, logistika mutaxassislari va tadqiqotchilar foydalanishi mumkin.

Kalit so'zlar: transport masalasi, MS Excel, Solver qo'shimchasi, chiziqli dasturlash, optimallashtirish, matematik model, logistika, simplex usul, ta'minot, talab, minimal xarajat.