применялась только до выплат, не превышающих пороговое значение, выше которого взносы взимались по ставке 0%; с 2025 г. страховые взносы 7,6% взимались вне зависимости от величины выплаты.

Налоговые преференции, максимум которых был установлен в 2022 г. постепенно снижаются. С 2026 г. усиливается системность косвенной поддержки развития ИТ-сектора в России с привлечением образовательной компоненты. Для сохранения льгот (по налогам, по льготным кредитам, отсрочки от призыва) аккредитованным ИТ-компаниям будет необходимо оказывать финансовую и нефинансовую помощь в подготовке кадров в рамках высшего образования в рамках разработки и реализации образовательных программ и отдельных учебных дисциплин. Это позволит дать дополнительный импульс для импортозамещения и ИТ-трансформации экономики России.

Список использованных источников

1. Механизмы и эффекты преференциального налогообложения юридических лиц / под ред. И.А. Майбурова. М.: Издательство Юнити-Дана, 2024. 352 с.
2. Киреева Е. Ф., Понкратов В.В. Налоговые льготы в стимулировании инноваций: мировой опыт и актуальные тренды // Финансы. 2025. № 5. С. 22-29.
3. Sinenko O. A. Tax expenditures of territories with special economic status of the russian Far East: performance assessment and ways to improve it // Vestnik of Institute of Economic Research. 2024. No. 1(33). P. 120-139.
4. Вылкова Е. С. Инструменты налоговой политики по борьбе с последствиями чрезвычайных ситуаций // Экономика. Налоги. Право. 2020. Т. 13, № 3. С. 136-143.

УДК 004.891.2

A.M. Veremeichik, N.N. Perepechko
Belarusian National Technical University
Minsk, Belarus

BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE IN THE FIGHT AGAINST FINANCIAL FRAUD: NEW CHALLENGES AND OPPORTUNITIES

Abstract. *Analyzing the synergistic effect of the use of blockchain technologies and artificial intelligence in the fight against financial fraud, highlighting key opportunities and identifying new challenges facing financial institutions and regulators*

А.М. Веремейчик, Н.Н. Перепечко
Белорусский национальный технический университет
Минск, Беларусь

БЛОКЧЕЙН И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В БОРЬБЕ С ФИНАНСОВЫМ МОШЕННИЧЕСТВОМ: НОВЫЕ ВЫЗОВЫ И ВОЗМОЖНОСТИ

***Аннотация**. Анализ синергетического эффекта от использования блокчейн-технологий и искусственного интеллекта в борьбе с финансовым мошенничеством, выделение ключевых возможностей и выявление новых вызовов, стоящих перед финансовыми институтами и регулирующими органами.*

The purpose of this study is to study the combined impact of blockchain and artificial intelligence technologies on the fight against financial fraud, identify their potential and identify new challenges faced by financial institutions and regulators.

The financial sector, being vital for the functioning of the economy, has always attracted the attention of fraudsters. According to the Association of Russian Banks, annual losses from fraudulent activities in Russia reach hundreds of billions of rubles. Traditional methods of defense based on pre-defined rules are no longer able to effectively resist sophisticated and constantly changing attack patterns. Cybercriminals actively use methods of psychological influence (social engineering), phishing, as well as advanced technologies, including artificial intelligence (AI), to automate and expand the scale of their activities.

In this situation, the key factor of technological progress in the financial industry is the combination of two innovative information and communication technologies: blockchain and artificial intelligence. If AI acts as an "intelligence" that can process huge amounts of data and detect deviations in real time, then the blockchain plays the role of an "incorruptible witness", ensuring the immutability, transparency and security of financial transactions. Together, these technologies form a new concept of security, shifting the focus from incident response to incident prediction and prevention [1].

Modern systems built on the basis of AI and machine learning (ML) are radically changing approaches to fraud detection.

Predictive analytics and real-time behavior analysis: unlike simple rules (for example, "prohibit transfers over a certain amount"), ML models analyze hundreds of parameters around the clock: the client's transaction history, location, device and browser used, as well as behavioral features (typing speed, mouse movements). For example, if a customer who usually makes payments from Moscow suddenly initiates a large transfer from another region from a new device, the system will assign a high level of risk to this operation and may request additional verification or block it until the circumstances are clarified.

Instead of simple rules such as transfer limits, predictive analytics and real-time behavioral analysis use machine learning to analyze hundreds of parameters around the clock. The client's transaction history, current location, data about the device and browser used, as well as features of his behavior when working with the system, such as typing speed and mouse movements, are taken into account. For example, a sudden large transfer from an unfamiliar region from a new device, if the client usually performs transactions from Moscow, will be marked by the system as high-risk and will require additional verification or blocking.

Deep learning and graph analysis algorithms are used to identify complex network anomalies. Fraudulent activities are often carried out by groups of linked accounts or companies. These algorithms are able to identify hidden connections by visualizing entire criminal schemes that are invisible when analyzing individual transactions [2].

In the fight against social engineering, natural language processing (NLP) models are used that analyze the contents of emails, SMS messages and instant messengers for signs of phishing, warning users about potential threats before transmitting confidential information.

Blockchain represents a revolutionary approach to ensuring the reliability and authenticity of data and ensures immutability and transparency: each transaction is cryptographically secured and linked to previous records, creating a transparent and immutable history. This provides the control authorities and auditors with a reliable verification environment.

In the field of identification (KYC), blockchain allows you to create a decentralized digital identity. After a single check with a reliable service provider, the user's digital ID is recorded in the registry and can be used in various financial institutions without re-submitting documents, simplifying the process for the client and reducing the risk of fraud.

Smart contracts for automatic rule compliance: Smart contracts are self-executing programs whose conditions are encoded. They can be configured to automatically meet regulatory requirements. For example, a contract can be programmed to make a payment only after receiving several digital signatures or when certain conditions are met (for example, confirmation of delivery of goods via an IoTsensor), which eliminates the human factor and the risk of fraud on the part of partners.

The true potential is revealed when they are used together:

AI analyzes the data, and the blockchain guarantees its authenticity. Machine learning models work with "pure", undistorted data from the blockchain, which significantly improves the accuracy of their forecasts.

Blockchain as a data source for AI training. The distributed ledger provides an extensive, anonymized and structured database of legitimate and fraudulent transactions, which is essential for training and continuous improvement of AI models [3].

Preemptive defense. Imagine a situation: Artificial intelligence detects something wrong on an account. Instead of the standard lock, it is able to launch, through a smart contract, an in-depth authentication procedure using biometric data contained in a decentralized digital identity of the user.

Despite its significant potential, the integration of blockchain and AI faces a number of serious challenges.

Scalability and performance issues: Public blockchain networks (for example, Ethereum) can be limited in data processing speed and have significant transaction costs, which makes it difficult to perform a large number of financial transfers. This requires the creation of more productive mechanisms for reaching agreement and using mixed (private) blockchains.

Regulatory ambiguity: the legal status of smart contracts, digital signatures on the blockchain, and operations involving crypto assets is still under discussion in many countries. Regulators need to develop clear rules that do not stop the development of technology, but at the same time ensure that the interests of users are protected.

Confidentiality of information: The openness of the blockchain may conflict with the requirements for the protection of personal data (such as GDPR in the European Union or 152-FZ in Russia). The solution may be to use technologies that allow you to prove the accuracy of data without disclosing its content (Zero-Knowledge Proofs).

"Attacks of the future": the use of AI by attackers: criminals are also beginning to use generative AI models (such as deepfakes) to bypass biometric identification systems and create convincing phishing messages. This creates the risk of an" arms race " between defenders and attackers [4].

Integration complexity and high cost: the implementation of these technologies requires significant investment in IT infrastructure, retraining of personnel, and overcoming resistance to existing processes within large financial institutions.

Blockchain technology and artificial intelligence technologies are no longer theoretical concepts and are becoming practical tools that can significantly increase the financial industry's resilience to fraudulent activities. Their interaction allows us to move from protecting borders to creating a reliable digital environment where every transaction is transparent, verifiable and analyzed in real time [5].

The key benefits of the Blockchain + AI combination are:

– Preventative measures (forecasting abnormal situations);

– Transparency (immutable control log);

– Automation (smart contracts and know your customer).

However, for widespread distribution, it is necessary to solve complex problems – legal, technological and organizational. Further development of this area requires close cooperation between financial institutions, IT development companies, and government regulators to develop standards, ensure system compatibility, and create an adaptive legal space.

Thus, blockchain and artificial intelligence are not just tools for combating fraud, but powerful factors that transform the entire financial system and lead to a safer, more efficient and more open economy.

Список использованных источников

1. Антонопулос, А. Осваивая Биткойн: Программирование открытого блокчейна 2-е изд./ А. Антонопулос. – Москва: Альпина Паблишер, 2023 – 450 с.;

2. Закс, Д. Децентрализованная цифровая идентичность и ее применение в финансовых услугах / Д. Закс // Журнал «Банковские технологии». – 2022. – № 5. – С. 34-41. – [сайт]. – Москва, 2018-2025 – URL: https://www.banktech.ru/ – (дата обращения: 15.11.2025);

3. Декрет Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» // Национальный правовой Интернет-портал Республики Беларусь. – [сайт]. – Минск, 2003-2025. – URL: http://pravo.by/document/?guid=3871&p0=Pd1700008 – (дата обращения: 15.11.2025);

4. Рассел, С. Искусственный интеллект: современный подход 4-е изд./ С. Рассел, П. Норвиг. – Москва, Вильямс, 2021 –743 с;

5. Отчет IBM «AI и машинное обучение в борьбе с финансовым мошенничеством».– [сайт]. – Нью Йорк 1991-2025 – URL: https://www.ibm.com/downloads/cas/8QZJXJ3A – (дата обращения: 15.11.2025).