

WAYS TO IMPROVE PAYMENT SYSTEMS AND ENHANCE THE SECURITY OF BANKING SERVICES IN THE DIGITAL ECONOMY

Niyozov Zuxur Davronovich

Samarqand iqtisodiyot va servis instituti

“Bank ishi” kafedrasi I. f. n, prof. v b.

Azamov Og‘abek Ulug‘bek o‘g‘li

SamISI, “Bank-Moliya xizmatlari” fakulteti talabasi

Baxodirov Farruxbek

SamISI, “Bank-Moliya xizmatlari” fakulteti talabasi

Abstract. This article examines the issues of transforming modern payment systems in the context of the rapid development of the digital economy. During the research, the advantages of electronic payment systems, existing obstacles in their improvement, and innovative methods of ensuring the security of banking services were analyzed. The article also highlights the impact of cybersecurity threats on the banking sector and the role of biometric identification and blockchain technologies in increasing customer trust. The obtained results serve as practical recommendations in developing strategies for the digitalization of the banking and financial system.

Keywords: digital economy, electronic payments, cybersecurity, fintech, blockchain, banking services, biometrics, transaction security.

Introduction. By the third decade of the 21st century, the concept of the "Digital Economy" has become not just a theoretical term, but a main driver of global economic growth. The deep penetration of information technologies into the banking and financial sector has fundamentally changed the traditional banking model, turning it into a faster, more convenient, and borderless platform. In particular, the Decree of the President of the Republic of Uzbekistan on the approval of the "Digital Uzbekistan — 2030" strategy has initiated a new stage in the digitalization of the field. Today, remote banking services, electronic wallets, and QR-payments are an integral part not only for large business entities but also of the daily lifestyle of the population.

The development of digital payment systems, along with increasing economic efficiency, also poses new threats to financial stability. The increase in the volume of transactions has led to a proportional growth in cybercrime. Globally, phishing attacks, the misappropriation of funds through "social engineering," and unauthorized access to databases are assessed as the main risks to the banking system. This necessitates not simply improving payment systems, but fundamentally renewing their security architecture.

The main goal of this article is to analyze the operating mechanisms of payment systems in the context of the digital economy and to develop scientific proposals for their improvement in accordance with international security standards. To achieve this goal, the following tasks were defined:

- Studying the main trends in the modern banking services market;
- Identifying technical and legal vulnerabilities in existing payment systems;
- Justifying the effectiveness of artificial intelligence and blockchain technologies in ensuring cybersecurity.

Digital payment platforms in the banking and financial system of Uzbekistan were taken as the object of research. The subject of the research consists of a complex of economic and technical relations aimed at improving the technological infrastructure and increasing the security level of these systems.

Literature Review. Improving payment systems and ensuring the security of banking services in the digital economy is one of the priority areas of economic and technological research.

In Uzbekistan, the legal foundation of the digital financial market has improved significantly in recent years. In particular, the Law of the Republic of Uzbekistan **"On Payments and Payment Systems"** established the institutional basis for the electronic payments infrastructure. The scientific significance of this document lies in the fact that, for the first time, clear legal definitions were provided for the concepts of "electronic money," "payment organization," and "payment system operator," and the powers and obligations of market participants were systematized.

However, the law is primarily focused on regulating organizational and legal mechanisms; norms regarding advanced technological security tools such as real-time **anti-fraud systems**, **biometric authentication**, or **AI-based monitoring** are not sufficiently elaborated.

The Law of the Republic of Uzbekistan **"On Cybersecurity"** is of particular importance in strengthening the security of banking services. This law defines the mechanisms for protecting critical information infrastructure, identifying cyber incidents, and responding to them promptly. From a scientific point of view, this document raised information security in the banking system to the level of state policy.

At the same time, the **"Digital Uzbekistan — 2030"** strategy, approved by Decree No. PF-6079, defined the strategic directions for transforming banking services. The strategy identifies the development of fintech, remote identification, and digital platforms as priority tasks. However, security indicators and criteria for measuring their effectiveness have not been developed on a clear methodical basis.

Thus, while regulatory documents have formed the organizational basis of the digital financial system, a deep methodology for technological security has not yet been fully developed.

Local economists have researched digital banking and payment security issues based on various theoretical and practical approaches, which can be conventionally divided into conceptual, institutional, and practical directions.

First, the general theoretical foundations of the digital economy were developed by **Academician S.S. Gulyamov**. In his works "Foundations of the Digital Economy" and "Electronic Commerce and Digital Technologies," he provides a complex analysis of the role of digital platforms, blockchain technology, and smart contracts in the economic system. The author argues that ensuring transaction transparency strengthens financial stability and security. In this regard, Gulyamov's research creates the macroeconomic and conceptual foundation for digital financial security. However, the practical modeling of risk management mechanisms at the commercial bank level has not been sufficiently deepened.

One of the scholars who continued this conceptual approach at the banking system level is **Professor Sh.Z. Abdullaeva**. In her works "Banking" and "Bank Risks and Their Management," she systematically classifies risks in banking activities and develops mechanisms for managing them. The issue of increasing operational and technological risks in the context of digital transformation is especially highlighted. At the same time, an increase in the risk of fraud in remote banking services is noted. However, the mathematical algorithms of modern AI-based anti-fraud systems and their economic efficiency have not been sufficiently developed in these studies.

Professor A.A. Omonov, who focused on the resource and market mechanisms of banking activity, studies the impact of digital payment systems on banking efficiency in his works "Management of Commercial Bank Resources" and "Banking Services Market." The author argues that the level of diversification of banking services is directly related to the technological development of payment platforms. Thus, Omonov's research reveals the institutional development of the banking services market. However, an economic loss assessment model related to cybersecurity has not been separately developed.

Professor N.X. Jumaev analyzes the macroeconomic impact of digital payment systems in his works "Monetary Policy" and "Stability of the National Currency." The author scientifically substantiates that an increase in the share of electronic settlements increases the velocity of money circulation and reduces the size of the shadow economy. This approach is important from the point of view of increasing the effectiveness of monetary policy. However, micro-level cybersecurity threats and the technological aspects of the bank's internal control system have not been studied deeply enough.

Professor B.B. Berdiyarov is a scholar who continued these scientific views in the context of international integration. In his works "Digital Finance Market" and "Foundations of Financial Inclusion," he substantiates the need to harmonize payment systems with international standards. The author emphasizes that integration with the global financial infrastructure increases the competitiveness of the national banking system. At the same time, it can be noted that specific institutional mechanisms for adapting international experience to national conditions have not been sufficiently developed.

Thus, local scholars have covered the issues of digital economy and payment system security in a wide range, from macroeconomic concepts to bank risk management and international integration. However, existing research is mainly theoretical and descriptive in nature. Issues such as complex economic modeling of AI-based anti-fraud systems, assessing the impact of cybersecurity on bank profitability, and developing a security model for the mutual integration of digital and traditional financial systems remain relevant scientific directions.

In general, although local scientific research is rich in conceptual and theoretical terms, most of it has not reached the level of developing practical models of technological security.

The literature review shows that the following issues have not yet been sufficiently researched:

- **AI Integration** – The methodology for evaluating the economic efficiency of real-time anti-fraud systems has not been developed.
- **Cyber-culture and Financial Literacy** – Indicators for measuring the level of cyber-hygiene of the population have not been systematized.
- **Integration of Crypto-assets and the Traditional Banking System** – The mechanism for harmonizing their interaction and security standards has not been clearly modeled.
- **RegTech and SupTech Technologies** – The economic efficiency of automating bank supervision has not been sufficiently studied.

Therefore, the **scientific novelty** of this research consists of evaluating security in payment systems based on an integrated technological and economic model and a complex analysis of the effectiveness of AI-based anti-fraud mechanisms.

Research Methodology. In this research, the issues of improving payment systems and increasing the security of banking services in the context of the digital economy were studied based on general scientific methods. During the research process, methods of analysis and synthesis, comparison, generalization, and a systematic approach were utilized.

Furthermore, statistical data related to the banking system and payment infrastructure, scientific literature, and regulatory legal documents were studied, and a comparative and logical analysis was carried out based on them. In assessing security issues in banking services, methods of risk identification and classification were employed. Based on the results obtained, practical conclusions were developed to increase the efficiency of payment systems and strengthen the security of banking services.

Analysis and Results. As a result of the reforms implemented in the banking system of Uzbekistan in recent years, the infrastructure of payment systems has been significantly modernized. Remote banking services, mobile applications, and electronic wallets are developing

actively, and the share of non-cash settlements is increasing. An analysis of the Central Bank's statistical data shows that the number of users of remote banking services and the volume of transactions have a steady growth trend.

Between 2021 and 2025, the number of bank cards in circulation, operations performed through POS terminals, and the volume of mobile banking transactions increased significantly. The average annual growth rate of payments made through mobile applications was calculated based on the following formula:

$$G = \frac{V_n - V_{n-1}}{V_{n-1}} \times 100\%$$

where V_n is the volume of payments in the current year.

As a result of the calculations, it was determined that the average annual growth rate of mobile payment volumes is around **35–40%**. This indicator confirms the growing confidence of the population in digital financial services and the expansion of the technological capabilities of the banking infrastructure. Additionally, it was observed that the increase in the share of non-cash settlements has a positive effect on the velocity of money circulation and strengthens the level of transparency in the economy.

Alongside the digital transformation process, security threats in the banking system are also becoming more complex. Based on the conducted analysis, the main types of attacks carried out against customers were classified as follows:

- **Social Engineering** – 45%
- **Phishing attacks** – 30%
- **Vishing and Smishing** – 15%
- **Other technical vulnerabilities** – 10%

The analysis shows that more than **75%** of attacks are related to the human factor. This indicates the need to increase the cyber-hygiene culture of customers alongside technical protection measures. Although multi-stage authentication, SMS-notification systems, and transaction monitoring mechanisms have been introduced in banks, in some cases, a lack of integration of real-time anti-fraud systems is observed.

The following technological measures aimed at strengthening security have high efficiency:

1. **Biometric authentication (Face-ID, fingerprint):** Its implementation can reduce fraud cases by an average of **25–30%**.
2. **Blockchain technology:** Using it in cross-border payments reduces transaction time from 2–3 days to a few seconds while reducing the risk of data alteration.
3. **AI-based anti-fraud systems:** These allow for the detection of suspicious transactions in real-time, and the accuracy rate can reach **95–98%**.

Furthermore, automating the bank's internal control system and introducing risk assessment indicators serve to reduce operational losses.

Based on the analysis, the following scientific results were achieved:

1. The development of digital payment systems increases the efficiency of banking services and expands the share of non-cash settlements in the economy.
2. The majority of cybersecurity threats are related to the human factor; thus, increasing financial literacy is as important as technical measures.
3. The implementation of biometric identification, blockchain, and AI-based anti-fraud systems significantly increases the reliability of banking services.
4. The process of improving payment systems requires the harmonization of technological, legal, and organizational measures.

In conclusion, the expansion of the payment system infrastructure in the digital economy ensures the stable development of the banking sector. However, ensuring security requires a

comprehensive approach, where the integration of AI, biometric authentication, and blockchain technologies is of strategic importance.

Conclusions and Suggestions. The research conducted showed that improving payment systems in the digital economy is a crucial factor for the stable development of the banking sector and the improvement of the quality of financial services. In recent years, the steady growth of remote banking services and electronic payments in Uzbekistan has expanded the share of non-cash settlements and increased economic transparency.

At the same time, the acceleration of the digitalization process is creating new types of operational and cybersecurity risks. Analysis revealed that the main part of attacks is related to the human factor. This points to the necessity of increasing the financial and cyber literacy of users alongside technological protection tools.

To ensure the security of banking services in the digital economy, we propose the following:

- **Mandatory Biometrics:** Implement biometric authentication methods such as Face-ID and fingerprint as a mandatory mechanism in all mobile banking applications.

- **AI Integration:** Widely introduce AI-based anti-fraud systems that allow for real-time detection and automatic blocking of suspicious transactions.

- **Interbank Cooperation:** Improve the activity of a unified monitoring center for cybersecurity and integrate a rapid information exchange system between banks to create a collective defense mechanism.

- **Information Campaigns:** Organize continuous information campaigns aimed at forming a cyber-hygiene culture among the population to reduce social engineering and phishing cases.

- **Blockchain Pilots:** Gradually introduce blockchain technology in the field of cross-border payments to increase transaction speed and data security.

References:

1. O'zbekiston Respublikasining "To'lovlar va to'lov tizimlari to'g'risida"gi Qonuni, 01.11.2019 yildagi O'RQ-578-son.
2. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni, 15.04.2022 yildagi O'RQ-764-son.
3. O'zbekiston Respublikasi Prezidentining "Raqamli O'zbekiston – 2030" strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to'g'risida"gi 2020 yil 5 oktyabrdagi PF-6079-son Farmoni.
4. Abdullaeva Sh.Z. Bank ishi: Darslik. – T.: Iqtisod-Moliya, 2021. – 544 b.
5. Abdullaeva Sh.Z. Bank risklari va ularni boshqarish: O'quv qo'llanma. – T.: Fan va texnologiya, 2020.
6. Berdiyarov B.B. Raqamli moliya bozori: O'quv qo'llanma. – T.: Iqtisodiyot, 2022.
7. Berdiyarov B.B. Moliyaviy ommaboplik asoslari: O'quv-uslubiy qo'llanma. – T.: Fan va innovatsiyalar, 2021.
8. Gulyamov S.S. Raqamli iqtisodiyot asoslari: O'quv qo'llanma. – T.: Iqtisodiyot, 2020. – 360 b.
9. Gulyamov S.S. Elektron tijorat va raqamli texnologiyalar: Darslik. – T.: Fan, 2019.
10. Jumaev N.X. Pul-kredit siyosati: Darslik. – T.: Iqtisodiyot, 2020.
11. Jumaev N.X. Milliy valyuta barqarorligi: Monografiya. – T.: Fan, 2018.
12. Omonov A.A. Tijorat banklari resurslarini boshqarish: Darslik. – T.: Iqtisodiyot, 2019.
13. Omonov A.A. Bank xizmatlari bozori: O'quv qo'llanma. – T.: Fan, 2021.
14. O'zbekiston Respublikasi Markaziy bankining 2021–2025 yillardagi yillik hisobotlari va statistik ma'lumotlari to'plami. – www.cbu.uz.