Spanish Journal of Innovation and INTEGRITY
ISSN: 2792-8268
Volume: 42, May-2025
http://sjii.indexedresearch.org

Types of Threats Affecting the Security of the Payment System

Babaeva Guzal Yashinovna
Associate Professor of the Department "Banking Accounting and Audit" Tashkent State University of Economics

Rasulova Parizoda, Akbarova Zarina
1st year Master's students of the Tashkent State University of Economics

Abstract: *With the rapid digitalization of financial services, modern payment systems have become integral to global economic infrastructure, offering fast and reliable fund transfers. Specific Background: As the usage of online and electronic payment methods increases, so do the risks associated with cyber threats, fraud, and internal system vulnerabilities. Despite global advances in payment security, there remains a need for focused research on the unique threat landscape and risk management practices in national systems like Uzbekistan's. This study analyzes the main types of threats affecting the security of payment systems legal, credit, liquidity, operational, and especially cyber risks and evaluates international best practices for mitigating such risks in both centralized and decentralized systems. The analysis identifies cyberattacks (e.g., phishing, DDoS, malware), internal misconduct, and technological obsolescence as major vulnerabilities. The study further highlights discrepancies between Uzbekistan's current risk management practices and global standards, suggesting enhancements through instant payment technologies, AI-based monitoring, and regulatory reforms. By integrating technical, legal, and procedural perspectives with comparative analysis of international and Uzbek systems, the study presents a holistic framework for evaluating and improving payment system security. The findings underline the necessity of continuous technological upgrades, enhanced cybersecurity awareness, and strengthened institutional oversight to ensure the stability and trustworthiness of financial systems in the digital era. This research offers actionable insights for policymakers, financial institutions, and payment system operators to adapt resilient and future-ready risk management strategies.*

Keywords: *payment system, cyber threats, security, fraud, internal threat, financial infrastructure.*

Introduction

Modern payment systems have become a key element of the global financial infrastructure. They provide fast, reliable, and efficient methods of transferring funds between individuals, firms, and financial institutions. In the era of financial digitalization, the emergence of new technologies, and the increasing use of online payments, the security of payment systems has become particularly relevant. Protecting user data, combating fraud, complying with regulatory norms, and reducing risks associated with cyber threats are just some of the tasks facing payment system operators. Maintaining the security of these systems not only safeguards the interests of end users but also directly impacts the stability of the entire financial sector of a country. The threats faced by payment systems can originate from diverse sources and manifest in various ways [1].

In contemporary scientific literature, the analysis of threats arising in the functioning of payment systems and the development of effective methods for their prevention and risk mitigation are particularly relevant. Many studies are dedicated to the functioning of payment systems and payment instruments. Payment instruments can include plastic cards, "electronic wallets" in open networks, or

accounts in electronic interactive banking systems. Banking payment systems can be defined from the perspective of their economic essence. From this standpoint, banking payment systems represent a part of the non-cash settlement system, based on their own principles, payment methods, and forms of settlement, actively interacting with the entire non-cash settlement system. In a narrower sense, the term "payment system" is sometimes used as a synonym for "interbank money transfer systems [2]."

However, in general, the term "payment system" refers to the complete set of tools (intermediaries, rules, procedures, processes, and interbank money transfer systems) that facilitate the circulation of money within a country or currency zone. At the same time, the practice of building and developing national payment systems varies from state to state, heavily dependent on numerous national factors, including the level of economic development, cultural and legal traditions, education levels, and more [3].

As a result, national payment systems differ in payment structure, quality and quantity of payment services, degree of integration, etc. An integral element is also the consideration of issues related to their security. In detail, the monographs "Security of Financial Technologies" and "Cyber Threats in Payment Systems: Current Challenges" thoroughly analyze the current landscape of cyberattacks and fraud in the financial sector [4].

Methodological Basis of the Research

The methodological foundation of this research comprises both general scientific and specific research methods aimed at a comprehensive study of processes related to the operation and security of payment systems. During the work, a comparative analysis of various approaches to ensuring the security of payment systems was conducted, applied both in the Republic of Uzbekistan and in countries with developed financial structures. This made it possible to identify key differences in protection strategies, determine factors contributing to the resilience of payment systems, and outline potential paths for adapting global best practices into national practice.

Results and Discussion

Payment systems are exposed to a number of major risks. Risks that are particularly significant for payment systems include, but are not limited to: legal risk, credit risk, liquidity risk, and operational risk [5].

Legal Risk. The presence of a solid legal foundation is of paramount importance for the operation of a payment system.

Credit Risk. Credit risk typically arises when a central bank or settlement institution provides credit to participants during an operational day to facilitate payments.

Liquidity Risk. Liquidity risk can also emerge in a payment system, especially in the event of a participant's failure to meet obligations.

Operational Risk. Operational aspects are especially critical for payment systems due to the pivotal role they play in the financial system. A payment system's inability to function normally can create or exacerbate existing risks between the payment system and its participants. In such cases, disruptions can propagate through the system and threaten the stability of the financial system as a whole. This also includes various risks related to physical and information security.

Modern payment systems actively employ internet technologies to enhance the security and convenience of transactions. However, as technology advances, so does the number of threats emerging in the virtual environment [6].

Cyber Threats. The most dangerous among these are cyberattacks aimed at disrupting the functioning of payment systems, stealing data, and manipulating financial transactions.

"Hacking and Data Leaks." One of the main threats to payment systems is the risk of their servers and databases being hacked. Malicious programs or hackers who gain access to these systems can steal confidential information, including credit card numbers, login credentials, passwords, and details of customers' financial transactions.

"DDoS Attacks (Distributed Denial of Service)." DDoS attacks are attempts to overload the resources of a payment system to render it unavailable to users. This is achieved by sending a massive number of fake requests to the system's server, causing overload and temporary unavailability of its services. These attacks can last from several hours to several days and are often aimed at undermining user trust in the payment system.

"Malware." Malware, such as viruses, trojans, and spyware, represents another significant threat to payment systems. It can be used to infect devices through which users make payments or to interfere with the operation of payment platforms.

Fraud and Fake Transactions. Fraudulent activities are one of the most common threats to payment systems. They can take various forms and affect both end users and the operators of the payment systems themselves.

Phishing is a deception method in which criminals seek to obtain personal data, including login credentials, passwords, and bank card details, by impersonating legitimate organizations. Fraudsters create fake websites that mimic the official pages of payment systems or banks and redirect users to these resources through fake emails or messages. By entering their data, users unknowingly hand it over to the fraudsters [7].

"Skimming." Skimming involves installing special devices on ATMs or point-of-sale terminals to extract data from the magnetic strips of cards. These devices can collect user information, which can then be used to create counterfeit cards or conduct criminal transactions. This method remains one of the oldest but still effective forms of fraud [8].

"Manipulation of Payment Details. "Criminals can also tamper with payment details to redirect money to their own accounts. This can be achieved by altering information during the transfer process, such as changing the recipient's account number in the payment system or in the documents used to execute the transfer [9].

Not all threats come from external sources. Internal risks can arise from employees of payment systems, banks, or other participants in the financial ecosystem. The significance of this type of threat lies in the fact that employees interacting with payment systems may have access to confidential information and resources, making various forms of abuse possible [10].

"Unauthorized Access to Information." Employees with access to users' personal data may use this information for personal gain. For example, they may sell the data, use it for unauthorized transactions, or engage in other forms of fraud [11].

"Dishonest Employee Actions." Additionally, some employees may participate in transaction manipulation. This can include altering transfer information, creating fake payments, or transferring funds to their personal accounts. To minimize such threats, it is necessary to implement systems for monitoring employee actions, as well as conduct audits and monitoring [12].

Currently, Uzbekistan operates centralized interbank and payment systems organized by the Central Bank, which function on the basis of an automated settlement system and allow for both urgent and non-urgent payments. Despite the system's stable operation, certain problems remain, such as:

- Low transaction processing speed in some segments
- Vulnerabilities of outdated technological platforms

- Insufficient development of tools for instant payments.

An analysis of international practices shows the active implementation of instant payment technologies (Instant Payments), distributed ledger technology (blockchain), and the transition to fully automated risk management systems. In a number of countries, real-time 24/7 protocols are successfully applied, significantly enhancing the resilience of payment systems and reducing operational risks [13].

Figure 1 presents the key elements that ensure the reliability and security of payment systems: clear documentation, disclosure of design and risk management procedures, open access to information, legal certainty of the roles of parties, clear decision-making procedures in crisis situations, and defining the capabilities of system participants [14].

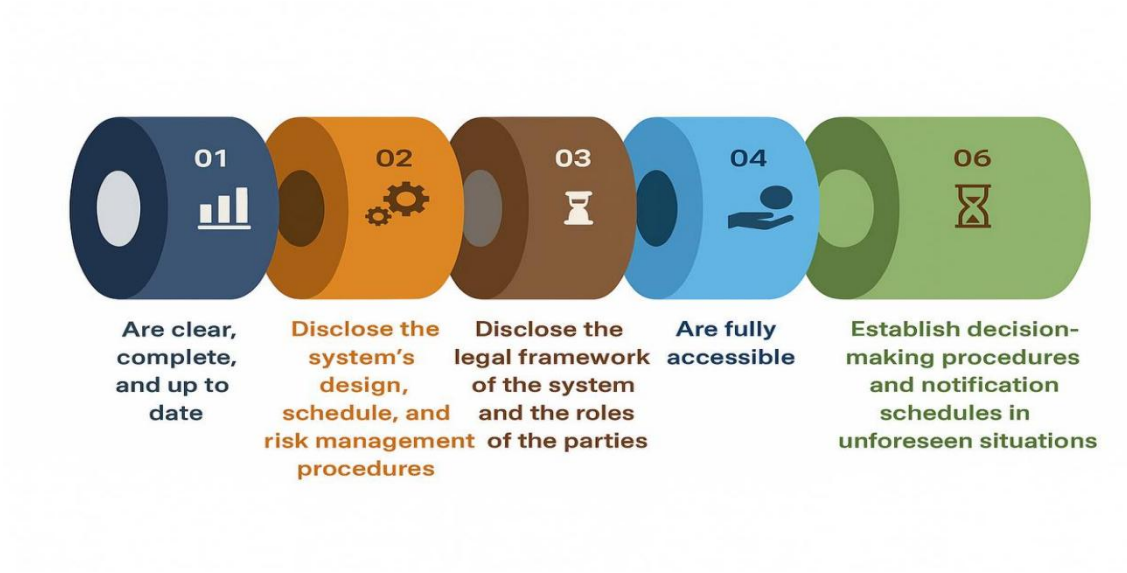

Figure 1. Key Characteristics of an Effective Payment System

These principles contribute to reducing internal and external risks and increase the level of trust among payment system participants. Moreover, a key aspect of ensuring the security of payment systems is the proper organization of the risk management process, the structure of which is illustrated in Figure 2.

Fig.2. Algorithm for organizing the risk management process

Figure 2. Algorithm for Organizing the Risk Management Process in Payment Systems.

In the context of growing cyber threats amid global digitalization, risk management has become an integral part of the functioning of an effective payment system [15].

In recent years, the digital sector of the country's economy has expanded, with key growth drivers e-commerce platforms and digital services, as well as financial technologies related to the high-quality and secure processing of payments on marketplaces and digital services developing rapidly. At the same time, the recent increase in cases of theft or fraud involving bank cards indicates insufficient digital financial literacy among the population and the qualifications of law enforcement personnel, the lack of modern systems for preventing offenses in commercial banks and payment organizations, and among payment system operators. To address these issues, the following laws and regulations have been enacted in the country: the Law of the Republic of Uzbekistan "On Cybersecurity" dated April 15, 2022, No. ЗРУ-764; the Regulation on Information Protection in Automated Systems of Commercial Banks of the Republic of Uzbekistan dated March 10, 2020, No. 3224; and the Regulation of the Central Bank of the Republic of Uzbekistan on Ensuring Information Security in Payment Systems of Payment System Operators and Payment Service Providers dated June 30, 2020, No. 3268. Additionally, increasing the level of cyber literacy among employees of financial institutions and regularly updating security standards in accordance with international recommendations (BIS, PCI DSS, SWIFT) are of particular importance.

Conclusion

The security of payment systems in the era of digitalization of financial infrastructure has become one of the key aspects of both state regulation and the private sector. A comprehensive approach to combating threats includes technical solutions, legislative support, and raising awareness among all participants in payment processes. It is necessary to account for the dynamic emergence of new threats and quickly adapt to the changing conditions of the digital economy. The application of predictive

analytics for cyber threats, the active use of artificial intelligence, and deepening international cooperation in cybersecurity represent promising directions.

List of References

1. A. Murugova and G. Y. Babaeva, Payment System and Banking Security: Textbook, Tashkent: Iqtisod – Moliya, 2019, p. 5.
2. T. Kokkola, Ed., the Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem, Frankfurt am Main, Germany: European Central Bank, 2010, p. 25.
3. S. Voronin, Ed., National Payment System. Business Encyclopedia, Moscow: KNORUS: TsIPSIR, 2013, p. 8.
4. I. Ivanov, Security of Financial Technologies, 2020.
5. V. Petrova, Cyber Threats in Payment Systems: Modern Challenges, 2022.
6. D. P. Sidorov, Electronic Payment Systems, 2021.
7. Zh. Gaipov, "Main Types of Risks in Payment Systems of the Republic of Uzbekistan and Methods of Managing Them," CentralAsianStudies, [Online]. Available: https://issuu.com/centralasianstudies/docs/113-122_.
8. G. Ya. Babaeva, "Measures to Reduce Fraud Risks in Payment Systems," Int. J. Educ., Social Sci. Humanit., vol. 12, no. 6, p. 1361, 2022. [Online]. Available: https://scholar.google.com/citations?view_op=view_citation&hl=ru&user=4SpN3AgAAAAJ&citation_for_view=4SpN3AgAAAAJ:KlAtU1dfN6UC.
9. Law of the Republic of Uzbekistan, "On Cybersecurity," Apr. 15, 2022, No. ЗРУ-764.
10. Regulation on Information Protection in Automated Systems of Commercial Banks of the Republic of Uzbekistan, Mar. 10, 2020, No. 3224.
11. Regulation of the Central Bank of the Republic of Uzbekistan, "On Ensuring Information Security in Payment Systems of Payment System Operators and Payment Service Providers," Jun. 30, 2020, No. 3268.
12. G. Babayeva, "Issues of Developing Payment Services of Commercial Banks," Eurasian J. Law, Finance, Pract. Sci., vol. 5, no. 4, pp. 157–164, 2025. [Online]. Available: https://in-academy.uz/index.php/EJLFAS/article/view/50448.
13. C. Dewi, E. I. H. Ujianto, and R. Rianto, "Electronic payment threats and security: A systematic literature review," J. Nasional Pendidik. Tek. Informatika: JANAPATI, vol. 13, no. 2, pp. 301–315, 2024.
14. Galhotra, A. Jatain, S. B. Bajaj, and V. Jaglan, "Mobile Payments: Assessing the Threats, Challenges and Security Measures," in Proc. 2021 5th Int. Conf. Electron. Commun. Aerosp. Technol. (ICECA), 2021, pp. 997–1004.
15. V. Ramaiya, P. Goyal, and N. K. Dubey, "Cybersecurity Threats and Trust Dynamics in Digital Payment Systems: An Analysis of Domestic Fraud and User Perspectives," in Int. Conf. Advancements Smart Comput. Inf. Security, Cham: Springer Nature Switzerland, 2024, pp. 116–138.