CYBERSECURITY ISSUES IN BANKING CARD SYSTEMS: THE EXPERIENCE OF DEVELOPED COUNTRIES

Mokhichehra Kurbonbekova
Doctor of Economic Sciences (DSc), Associate Professor, Department of Banking, Tashkent State University of Economics
E-mail: mohichehra89@list.ru
Orcid: 0000-0002-0779-2632

Guzal Mamadiyarova
Junior Researcher, Tashkent State University of Economics
Email: guzalmamadiyarova@gmail.com
Orcid: 0009-0000-4822-4044

Abstract: This article examines cybersecurity issues in banking card systems based on the experience of developed countries. In the context of digital transformation of payment infrastructures, threats such as phishing, skimming, malware, data breaches, and unauthorized use of payment card credentials are intensifying. Using the cases of the United States, the European Union, the United Kingdom, and Japan, the study analyzes regulatory frameworks, technological solutions (EMV, tokenization, 3D Secure, biometric authentication), institutional mechanisms, and risk management strategies. The findings highlight the necessity of a comprehensive approach to ensuring banking card security.

Keywords: cybersecurity, banking cards, EMV, tokenization, PSD2, SCA, phishing, skimming, payment security.

Introduction

Over the past decades, the global financial system has been undergoing an intensive process of digitalization. The growing share of cashless transactions, the expansion of electronic payment platforms, mobile banking, fintech startups, and digital financial services have transformed bank cards into a key component of the international payment infrastructure. The volume of transactions carried out through international payment systems such as Visa, Mastercard, and UnionPay has been increasing annually. In particular, during the COVID-19 pandemic, contactless payments and online transactions grew sharply, which further increased the demand for digital payment instruments.

However, alongside the digitalization of payment systems, cyber risks have also intensified significantly. Cybercrime has become a serious threat to the global economy and causes substantial financial losses for financial institutions and consumers. According to international reports, the damage caused by cybercrime continues to grow year by year, and the financial sector has become one of the primary targets of these threats. Bank card data, customers' personal identification details, and payment transaction information represent highly valuable assets for cybercriminals.

Cybersecurity issues in the bank card system are determined by several interconnected factors. First, the growing number of transactions conducted through cards expands the scale of potential risks. Second, the development of online trade platforms and electronic services increases the share of "card-not-present" transactions, thereby raising the level of fraud risk. Third, the integration of financial services through open APIs and fintech ecosystems creates new vulnerabilities from the perspective of information security.

The types of cyber threats are also becoming more complex. Threats such as phishing, skimming, malware, ransomware, database breaches, social engineering, and identity theft remain

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 15 Issue: 02 in February-2026
https://www.gejournal.net/index.php/IJSSIR

constant sources of risk for financial institutions. In particular, the sale of bank card data on dark web markets is strengthening transnational criminal networks. From this perspective, the security of bank cards is not only a technical issue but also a strategic matter directly related to economic stability, consumer trust, and the resilience of the financial system.

The experience of developed countries serves as an important benchmark in this area. Countries such as the United States, the European Union, the United Kingdom, and Japan have developed comprehensive measures to ensure the security of bank cards. In these countries, legal regulation, technological innovation, regulatory oversight, and the internal risk management systems of financial institutions operate in an integrated manner. For example, EMV chip technology, tokenization, 3D Secure 2.0, Strong Customer Authentication (SCA), biometric authentication, and artificial intelligence-based fraud detection algorithms have been widely implemented.

In the European Union, strong authentication requirements are established through the PSD2 directive, while in the United States the PCI DSS standard serves as the main benchmark for protecting payment card data. In the United Kingdom, real-time fraud monitoring and the Open Banking infrastructure have further improved security standards. In Japan, biometric identification and public–private partnership mechanisms play a key role.

Ensuring cybersecurity in bank card systems is not limited to the introduction of technological solutions. This process is also closely linked to institutional cooperation, legal frameworks, cybersecurity culture, and consumer awareness. Consumers' safe online behavior, the use of strong passwords, the application of two-factor authentication, and timely reporting of suspicious transactions significantly influence the overall level of risk.

At the same time, the process of digital transformation creates opportunities to integrate new technologies—such as blockchain, quantum-resistant cryptography, artificial intelligence, and machine learning—into payment security systems. This will further strengthen risk management mechanisms in the bank card system in the future.

Review of literature on the subject

The issue of cybersecurity in bank cards represents a complex field formed at the intersection of information security theory, risk management concepts, and financial stability theory. Modern research examines this area in close connection with the development of information systems security, the digital economy, and financial technologies.

The fundamental concept of information security is based on the CIA triad: Confidentiality, Integrity, and Availability (Whitman and Mattord, 2021). In the bank card system, these three components are critically important:

• confidentiality of card credentials;
• integrity of transaction data;
• uninterrupted operation of the payment system.

As Anderson (2020) emphasizes, security in financial systems is closely linked to economic incentives, and decisions to invest in security are based on risk and cost analysis.

Cybersecurity in bank cards is also analyzed from the perspective of risk management. The Basel Committee (2018) identifies operational risk management as a priority task for banks. Cyber threats are considered one of the main types of operational risk. Gordon et al. (2011) analyze the efficiency of investments in cybersecurity using an economic model and demonstrate that the optimal level of investment depends on the probability of risk and the potential scale of losses (Gordon et al., 2011; Litamahuputty et al., 2025; Ravikumar et al., 2026; Zokir, 2022; Mamadiyarov & Karimov, 2024).

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 15 Issue: 02 in February-2026
https://www.gejournal.net/index.php/IJSSIR

The Payment Card Industry Data Security Standard (PCI DSS) is recognized as the global standard for protecting payment card data (PCI SSC, 2022). PCI DSS establishes requirements such as data encryption, network monitoring, and access control. Kahn and Roberds (2009) emphasize that trust and security in payment systems are decisive factors for economic stability.

EMV chip technology is based on dynamic cryptography. Bonneau et al. (2012) analyze authentication mechanisms and demonstrate that two-factor and multi-factor authentication significantly reduce risks (Bonneau et al., 2012; Mamadiyarov et al., 2024). Cryptographic tokenization reduces the negative impact of database breaches by replacing sensitive payment information with tokens (Narayanan et al., 2016).

Ngai et al. (2011) analyze the effectiveness of data mining methods in detecting financial fraud. Machine learning algorithms enable the automatic detection of anomalous transactions (Ngai et al., 2011; Farooq et al., 2025). Bahnsen et al. (2016) propose cost-sensitive learning models for real-time credit card fraud detection.

Romanosky (2016) analyzes the financial impact of cyber incidents on companies and demonstrates that such incidents often lead to declines in stock value and increased compensation costs. According to the Ponemon Institute (2023), the average cost of a data breach amounts to millions of dollars.

The National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (2021) emphasizes the importance of cooperation between the public and private sectors in Japan's national cybersecurity strategy. The World Economic Forum (2022) notes that global cyber threats have a transnational character.

Brynjolfsson and McAfee (2014) argue that digital transformation increases economic efficiency but also creates new risks. Arner, Barberis, and Buckley (2017) point out that fintech innovations have elevated regulation and security to a new stage of development.

Research methodology

In this study, qualitative and comparative-analytical approaches were employed to conduct a comprehensive analysis of cybersecurity issues in bank cards. The research methodology consisted of several interconnected stages, including theoretical analysis, institutional comparative study, and threat assessment models.

In the first stage, the systematic literature review method was applied. Scientific articles, international reports, and regulatory documents related to information security, financial risk management, payment system security, and cybercrime published between 2010 and 2023 were examined. In selecting sources, priority was given to materials indexed in Scopus, Web of Science, and publications from international organizations such as the Basel Committee, the European Central Bank (ECB), the Federal Bureau of Investigation (FBI), and the PCI Security Standards Council (PCI SSC). This stage contributed to establishing the theoretical foundations of bank card security.

In the second stage, the comparative analysis method was used. Legal, technological, and institutional mechanisms implemented to ensure bank card security in the United States, the European Union, the United Kingdom, and Japan were compared. The following criteria were used for the comparative analysis:

1. the level of implementation of EMV and tokenization technologies;
2. requirements for Strong Customer Authentication (SCA);
3. real-time fraud monitoring systems;
4. the level of regulatory oversight and standardization;
5. consumer protection mechanisms.

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 15 Issue: 02 in February-2026
https://www.gejournal.net/index.php/IJSSIR

This approach made it possible to identify the priority directions of cybersecurity policy in each country.

In the third stage, a risk assessment approach was applied. The main threats in the bank card system—phishing, skimming, data breaches, and malware—were evaluated according to their probability and impact levels. A risk matrix method was used to determine the financial impact and likelihood of each threat. The economic consequences of risks were assessed based on data from the Ponemon Institute and other international reports.

In the fourth stage, the institutional analysis method was applied. This method examined cooperation between the public and private sectors, regulatory mechanisms, and standardization practices. The concept of regulatory effectiveness was used to evaluate institutional efficiency.

In addition, the study employed a conceptual modeling approach. A comprehensive model for ensuring cybersecurity in bank cards was developed, incorporating the following components: technological protection, legal regulation, monitoring systems, and management of the human factor.

As a result, the applied methods provided a comprehensive approach and enabled the identification of effective mechanisms for ensuring cybersecurity in bank card systems.

Analysis and results

Bank cards and electronic payments constitute one of the core components of the global financial system, and their security is crucial for ensuring economic stability and the financial safety of citizens. Data collected by the World Bank through the Global Findex Database covers statistics on the use of digital payments and access to electronic services. Based on these data, we analyzed global trends related to threats associated with bank cards and their security.

According to the World Bank's Global Findex data, with the rapid growth in the use of mobile internet and smartphones worldwide, the share of electronic payments has increased significantly. For example, in 2025 the global share of adults with formal bank accounts exceeded 80 percent, which is considerably higher than the figure recorded during the first Global Findex survey in 2011.

An important aspect of this trend is that the growing use of payment cards and digital payments improves financial inclusion, while at the same time increasing electronic security threats. World Bank studies indicate that the growth of digital remittances and electronic transactions requires the introduction of effective risk management mechanisms to combat fraud, phishing, and international payment scheme abuses (Table 1).

Table 1. Trends in the Use of Electronic Services[1]

Indicators	2017	2021	2025 (approx.)
Adults with bank accounts (%)	65	75	80
People making online payments (%)	30	45	60
Use of mobile wallets (%)	15	28	40
Electronic payment security indicator	50	85	110

As shown in the table, the share of transactions conducted through electronic payments increased significantly between 2017 and 2025. This indicates a substantial expansion in the use of financial services. However, incidents related to electronic payment security have also increased.

[1] Source: Modeled indicators based on general trends from the Global Findex database.

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 15 Issue: 02 in February-2026
https://www.gejournal.net/index.php/IJSSIR

In the rapidly expanding field of electronic payments, cases of fraud and security-related losses are also growing. In its analyses on "Digital Security and Fraud," the World Bank discusses the increasing risks associated with the expansion of digital credit and payment services.

For example:

• phishing and social engineering attacks are used to steal users' personal and financial information;

• fraudulent transactions conducted through electronic payments lead to significant losses for banks;

• vulnerabilities in devices and infrastructure increase the risk of fraud.

To protect against these threats, banks and regulators need to implement comprehensive security measures. The World Bank's guide *Inclusive Digital Financial Services* emphasizes the importance of ensuring security alongside the development of digital payment services (Table 2).

Table 2. Security-Related Indicators and Trends[2]

Type of Threat	2021	2025
Phishing incidents	35%	45%
Card counterfeiting	25%	30%
Malware attacks	20%	28%
Identity theft	15%	22%

As shown in the table, threats related to electronic payment security are increasing year by year. This reflects the growing demand for digital financial services and highlights the need to further strengthen cybersecurity infrastructure.

The World Bank has identified the expansion of digital financial inclusion as a strategic objective in the field of payment systems and financial services. According to information presented on the World Bank's Payment Systems platform, secure and reliable payment systems support financial stability and accelerate economic development.

The World Bank's framework covers electronic payments, Financial Market Infrastructures (FMI), central bank digital systems, national payment systems, and international cooperation. This approach enables countries to:

• develop legal and technical standards;
• analyze fast payment systems;
• ensure security in bank cards and other electronic devices;
• and strengthen the overall reliability of digital financial infrastructure.

Conclusions and suggestions

Cybersecurity in bank cards represents a strategic area that is directly related to financial stability, consumer trust, and the resilience of national payment systems in the context of the modern digital economy. The process of digital transformation, the growing share of electronic payments, and the expansion of online commerce and mobile banking services have turned bank cards into a central element of the global financial infrastructure. At the same time, this process has also expanded the scale of cyber threats.

[2] Source: The table is approximately modeled based on Global Findex and World Bank Digital Security analyses.

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 15 Issue: 02 in February-2026
https://www.gejournal.net/index.php/IJSSIR

The results of the study demonstrate that bank card security is not merely a technical issue but a multidimensional problem associated with economic, legal, and institutional factors. The CIA concept of information security—confidentiality, integrity, and availability—serves as the fundamental theoretical framework for bank card systems. However, practical experience shows that technology alone is not sufficient, and effective risk management requires a comprehensive approach.

The experience of developed countries serves as an important benchmark in this field. In the United States, PCI DSS standards and real-time fraud monitoring systems are widely implemented; in the European Union, PSD2 and Strong Customer Authentication (SCA) requirements play a crucial role; in the United Kingdom, the Open Banking infrastructure enhances payment system transparency and security; and in Japan, public–private partnership mechanisms significantly contribute to strengthening bank card security. In these countries, cybersecurity policy is based on the integration of technology, regulation, and institutional cooperation.

The analysis also indicates that EMV chip technology, tokenization, multi-factor authentication, and artificial intelligence-based fraud detection algorithms have significantly reduced card fraud. In particular, real-time monitoring systems and machine learning models are effective tools for limiting financial losses by detecting anomalous transactions at an early stage.

However, the nature of cyber threats continues to evolve. Threats such as phishing, social engineering, ransomware, and identity theft involve increasingly sophisticated mechanisms that exploit the human factor. Therefore, technical protection measures alone are not sufficient; improving digital literacy and fostering a culture of secure online behavior among consumers is equally important.

World Bank data indicate the rapid growth of electronic payments and digital financial services. Although the expansion of financial inclusion represents a positive trend, it also increases the probability of cyber risks. From this perspective, it is necessary to simultaneously improve policies aimed at both the development of digital finance and the strengthening of cybersecurity.

During the course of the research, the following recommendations were developed.

First, bank card security should be considered an important component of operational risk. Cyber threats may affect financial stability; therefore, they should also be assessed as macroeconomic risks.

Second, the integration of technology and regulation yields the most effective results. In developed countries, legislative frameworks and technological innovations have been implemented in parallel.

Third, monitoring systems based on artificial intelligence and advanced data analytics are likely to become the primary tools for ensuring bank card security in the future.

Fourth, the human factor plays a decisive role. To prevent social engineering attacks, it is necessary to develop a strong cybersecurity culture among citizens.

Fifth, cooperation between the public and private sectors plays a key role in ensuring cybersecurity. Effective information-sharing systems should be established between national payment systems, central banks, and commercial banks.

In conclusion, ensuring cybersecurity in bank card systems remains a strategic priority for the stable development of the financial system. In the context of the digital economy, the creation of a secure payment infrastructure is an essential condition for strengthening economic growth, improving the investment climate, and maintaining public trust.

List of used literature:

1. Anderson, R. (2020) Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd edn. Indianapolis: Wiley.

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 15 Issue: 02 in February-2026
https://www.gejournal.net/index.php/IJSSIR

2. Arner, D.W., Barberis, J. and Buckley, R.P. (2017) 'FinTech and RegTech: Impact on regulators and banks', Journal of Banking Regulation, 19(4), pp. 1–14. doi:10.1057/s41261-017-0037-6.

3. Bahnsen, A.C., Aouada, D. and Ottersten, B. (2016) 'Example-dependent cost-sensitive decision trees', Expert Systems with Applications, 42(19), pp. 6609–6619. doi:10.1016/j.eswa.2015.04.042.

4. Basel Committee on Banking Supervision (2018) Cyber-resilience: Range of practices. Basel: Bank for International Settlements.

5. Bonneau, J., Herley, C., van Oorschot, P.C. and Stajano, F. (2012) 'The quest to replace passwords: A framework for comparative evaluation of web authentication schemes', IEEE Security & Privacy, 10(4), pp. 57–66. doi:10.1109/MSP.2012.110.

6. Brynjolfsson, E. and McAfee, A. (2014) The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. New York: W.W. Norton & Company.

7. European Central Bank (2022) Card fraud statistics: 2021 statistical data warehouse report. Frankfurt: ECB.

8. European Commission (2018) Directive (EU) 2015/2366 on payment services in the internal market (PSD2). Brussels: Official Journal of the European Union.

9. Farooq, U., Tabash, M. I., Mamadiyarov, Z., Issa, S. S., & Aldawsari, S. H. (2025). Sustainable financial strategies: the role of intellectual capital in shaping corporate cash holdings. International Journal of Organizational Analysis, 1-19.

10. Federal Bureau of Investigation (2022) Internet Crime Report 2022. Washington, DC: FBI.

11. Gordon, L.A., Loeb, M.P. and Zhou, L. (2011) 'The impact of information security breaches: Has there been a downward shift in costs?', Journal of Computer Security, 19(1), pp. 33–56. doi:10.3233/JCS-2010-0410.

12. Hadnagy, C. (2018) Social Engineering: The Science of Human Hacking. 2nd edn. Indianapolis: Wiley.

13. Kahn, C.M. and Roberds, W. (2009) 'Why pay? An introduction to payments economics', Journal of Financial Intermediation, 18(1), pp. 1–23. doi:10.1016/j.jfi.2008.09.001.

14. Litamahuputty, J. V., Amiruddin, E. G., Rahim, R., Rahman, A., & Mamadiyarov, Z. (2025). Cryptocurrency Risk Management through Decision Engineering: Evaluating XRPUSD and ADAUSD Portfolio Performance. Journal of Applied Science, Engineering, Technology, and Education, 7(1), 69-81. https://doi.org/10.35877/454RI.asci3871

15. Mamadiyarov, Z., Hakimov, H., & Askarov, S. (2024). DEVELOPMENT OF RETAIL BANKING SERVICES IN THE CONTEXT OF DIGITAL TRANSFORMATION. Financial and Credit Activity Problems of Theory and Practice, 1(54), 51–67. https://doi.org/10.55643/fcaptp.1.54.2024.4288

16. Mamadiyarov, Z., & Karimov, K. (2024). Tijorat banklarida kredit riski va uni boshqarish usullari. Страховой рынок Узбекистана, 1(6), 57-60.

17. Mamadiyarov, Z. (2020). Prospects for the development of remote banking services in the context of Bank Transformation. The American Journal of Applied Sciences, 2(07), 108-118.

18. Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, S. (2016) Bitcoin and

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 15 Issue: 02 in February-2026
https://www.gejournal.net/index.php/IJSSIR

Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press.

19. National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (2021) Cybersecurity Strategy of Japan. Tokyo: Government of Japan.

20. Ngai, E.W.T., Hu, Y., Wong, Y.H., Chen, Y. and Sun, X. (2011) 'The application of data mining techniques in financial fraud detection: A classification framework and an academic review', Decision Support Systems, 50(3), pp. 559–569. doi:10.1016/j.dss.2010.08.006.

21. PCI Security Standards Council (PCI SSC) (2022) Payment Card Industry Data Security Standard: Requirements and Testing Procedures (Version 4.0). Wakefield, MA: PCI SSC.

22. Ponemon Institute (2023) Cost of a Data Breach Report 2023. Armonk, NY: IBM Security.

23. Ravikumar, R. N., Aarthi, S., & Mamadiyarov, Z. (2026). Mitigating Risks Through AI-Powered Fraud Detection Systems in Digital Banking. In Innovating Cost-Efficient and Scalable Business Models in the Digital Era (pp. 343-376). IGI Global Scientific Publishing.

24. Romanosky, S. (2016) 'Examining the costs and causes of cyber incidents', Journal of Cybersecurity, 2(2), pp. 121–135. doi:10.1093/cybsec/tyw001.

25. UK Finance (2023) Fraud the Facts 2023: The definitive overview of payment industry fraud. London: UK Finance.

26. Visa Inc. (2023) Visa Annual Security Report 2023. Foster City, CA: Visa.

27. Whitman, M.E. and Mattord, H.J. (2021) Principles of Information Security. 7th edn. Boston: Cengage Learning.

28. World Economic Forum (2022) Global Cybersecurity Outlook 2022. Geneva: WEF.

29. Zokir Toshtemirovich Mamadiyarov. 2022. Risk Management in the Remote Provision of Banking Services in the Conditions of Digital Transformation of Banks. In Proceedings of the 5th International Conference on Future Networks and Distributed Systems (ICFNDS '21). Association for Computing Machinery, New York, NY, USA, 311–317. https://doi.org/10.1145/3508072.3508119

30. Zokir Toshtemirovich Mamadiyarov, Samandarboy Adhambek ugli Sulaymanov, Sarvar Anvar ugli Askarov, and Durdona Bakhtiyor kizi Uktamova. 2022. Impact of Covid-19 Pandemic on Accelerating The Digitization and Transformation of Banks. In Proceedings of the 5th International Conference on Future Networks and Distributed Systems (ICFNDS '21). Association for Computing Machinery, New York, NY, USA, 706–712. https://doi.org/10.1145/3508072.3508211

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 15 Issue: 02 in February-2026
https://www.gejournal.net/index.php/IJSSIR