AMERICAN JOURNALS
Open Access, Peer Reviewed Journals

American Journal of Business Management, Economics and Banking
ISSN (E): 2832-8078 Volume 43, December - 2025

ENSURING INFORMATION SECURITY WITHIN THE BANK MANAGEMENT SYSTEM: KEY STRATEGIC APPROACHES

Kobiljon Isroiljonov,
Student of Tashkent International University Major: Economics
Phone: +998994616355
e-mail: isroiljonov.k55@gmail.com

ABSTRACT

The rapid digital transformation of the banking system of the Republic of Uzbekistan, conditioned by the systemic introduction of innovative information and communication technologies and supported by state strategies, has created a secure, efficient, and modern national payment infrastructure. However, while this kind of transformation increases the efficiency, transparency, and competitiveness of financial operations, it has also given a boost to the demand for relevant advanced information security measures. Ensuring the reliability, integrity, and confidentiality of banking data can be reached only via proactive, multilevel approaches that integrate technological innovations, robust cybersecurity frameworks, and effective management of digital risks, which in turn will let the banking sector provide safe, convenient, and high-quality remote financial services both to domestic and international users.

KEYWORDS

Digital banking, national payment system, information and communication technologies, electronic payments, remote banking services, information security, cybersecurity, electronic digital signature, banking infrastructure, and protection of financial data.

Introduction

Through the systematic and broad introduction of innovative information and communication technologies into the banking system of the Republic of Uzbekistan, it became possible to establish, in a relatively short period of time, a modern national payment infrastructure. Currently, an integrated interbank payment system involving all commercial banks is fully functional, offering reliable mechanisms for cashless settlement at the national level. Its operation provides for the high accuracy, transparency, and timeliness of both domestic and international payment transactions and, at the same time, contributes to the effective implementation of monetary and credit policy and the optimization of general cash flow management in the economy.

In this regard, the strategic approach of the state leadership is very important. As noted by the President of the Republic of Uzbekistan Sh. Mirziyoyev: “Whichever sector produces high-value products, we will support that sector first. Therefore, we must develop and apply a strategy for sectors that can give a serious impetus to economic development.” He underlined the need to focus on technology-intensive

and highvalue sectors, such as digital banking, for further development as key drivers of economic modernization and sustainable development.

The accelerated digitalization of the banking sector, coupled with consistent government support, not only strengthens the national payment system but also enhances the competitiveness of Uzbekistan's financial infrastructure in the global economic environment. The creation of such integrated systems testifies to the country's determination for the formation of an efficient, secure, and innovative banking ecosystem able to meet contemporary international standards.

The telecommunications network of the banking system of the Republic of Uzbekistan has been developed as an integrated complex of closed corporate communication infrastructures of the Central Bank, commercial banks, and other organizations operating in different sectors of the national economy. Basically, the given system relies on the telecommunication capabilities of the main operator "Uzbektelecom" JSC, while the channels of communication from other providers are used as auxiliary or backup resources for continuity and stability of processes.

Basic aims of this banking telecommunication infrastructure are to create a highly reliable and secure transport environment for interbank electronic payment processes, closed virtual corporate networks for protected data exchange, continuous operation of the interbank electronic mail system, and special communication channels allocated in accordance with needs formulated by various network users. All these functions position the telecommunication network as a vital technological backbone that allows conducting financial transactions efficiently, accurately, and securely within the country.

One can hardly deny that the financial and banking sector is currently one of the most technically equipped fields when it comes to issues of information security. Yet, the rapid and disruptive changes in modern information technologies-to wit, extensive virtualization of data resources, wider utilization of cloud platforms, and expansion of mobile broadband access-significantly reshape the demands for ensuring cybersecurity. In these conditions, participants of the financial market, alongside government bodies, private organizations, and even individual users, need to move toward the use of next-generation information protection tools and modern security models.

These technological shifts necessitate a proactive approach toward strengthening cybersecurity frameworks, as emerging digital ecosystems introduce new vulnerabilities alongside new opportunities. Financial institutions are thus compelled to implement improved security architectures, advanced authentication systems, and comprehensive risk-mitigation mechanisms that can help maintain the integrity, confidentiality, and availability of critical financial data.

Nowadays, one of the most serious problems in the sphere of information security is the intentional disturbance of automated systems, which process banking data. This problem becomes extremely urgent for those countries whose information and communication infrastructures are highly developed and deeply integrated into economic and social processes. While electronic payment mechanisms, plastic cards, and large computer networks are being developed, they more and more become the object of various types of information attacks and cyber-invasions. In these conditions, when access to a computer connected to the Internet is enough to try unauthorized interference in financial processes, this threat becomes substantially broader and more complicated. In such a context, this problem is not only extremely urgent but also remains poorly investigated in contemporary scientific and practical research.

Nowadays, most commercial banks have established channels for performing remote payment operations. Performing financial transactions over the Internet has become routine, and clients can pay

bills, transfer money, or conduct any other bank operations from almost any place in the world. To undertake such operations, they need an apparatus connected to the global network and a digital signature key duly registered with the bank. While these technological conveniences significantly enhance customer experience and operational efficiency, they also raise the stakes in terms of strong authentication, sound cryptographic protection, and close monitoring to prevent unauthorized access and financial fraud.

Through remote banking services, many advantages are offered to customers, which greatly enhance the efficiency and comfort of financial interactions.

• Time efficiency: Clients can perform all payment operations at any convenient moment, without the need to physically go to bank branches, which drastically reduces time expenditures and raises operational flexibility.

• Ease of usage. All monetary transactions are performed via personal computer or other electronic devices, and users can manage their accounts from any place that has access to the Internet.

• High transaction processing speed. Remote banking technologies guarantee rapid execution of payment orders, thereby enhancing overall effectiveness concerning financial operations and reducing delays typical for traditional channels of service provision.

Real-time document status monitoring. Your users can keep track of every stage in the processing of their payment documents, thus making it a highly transparent process wherein they can also identify potential issues in real time.

• Immediate access to account information: Customers can have quick access to all detailed data about all movements of funds in their accounts, thus allowing better financial planning, control, and decision-making.

However, in spite of the significant benefits brought about by remote banking technologies, complete reliance on absolute security provided by electronic means of paying has not been instilled into people. This situation partially arises from frequent and increasingly sophisticated hacker attacks targeting computer networks and digital infrastructures of financial systems. Such attacks outline the current drawbacks of information systems and prove that even the most advanced technological solutions need ongoing care and development.

Within the contemporary digital landscape, the EDS operates as a basic means of security that serves to guarantee authenticity and integrity for banking transactions. Every EDS key is legally and functionally equal to a manually written signature by an authorized person, hence being a secure means of confirmation of identity in the electronic environment. EDS considerably increases the advantages of electronic payments compared with traditional banking services by guaranteeing document authenticity, prevention of unauthorized interference, and enabling legally binding relations in electronic interaction.

With this, banks periodically inform customers about the rules for the proper use, protection, and storage of EDS keys. Strict adherence to these recommendations significantly enhances reliability and security in electronic payment transactions, since the compromise of a digital signature is fraught with the most serious consequences for clients and financial institutions alike.

In any case, the development of automated large-scale information processing systems is a very dynamic process that has been changing and continues to change in line with technological progress. As a result, the speed of development of new system vulnerabilities and errors exceeds in many instances the speed of their detection and complete elimination. Every new software platform or

technological component may create new risks that require substantial redevelopment or strengthening of the existing security architecture. This is a constant process that calls for proactive, adaptive, and multilevel security approaches within the banking sector.

From our point of view, reaching information security in the banking system involves consideration of the following specific factors:

1. Banking systems comprise data on actual and processed information related to monetary funds. Payments are made, loans issued, and funds transferred based on that very data. Thus, unauthorized use of information causes severe damage and increases the number of criminals wanting to attack banking data.

2.Bank data covers the interests of customers. This information is usually secret, and the bank is responsible for keeping it confidential.

3. A bank's competitiveness is determined by the scope of services provided, including remote ones. It should be possible for customers to take care of their money at any time and place. On the other hand, the more accessible the system is, the higher is the probability that the criminals will also be able to get access to it.

4. Information security requires ensuring the reliability even of computer systems in emergency situations. At the same time, however, even strict measures to regulate the use of confidential information today are not able to prevent its leakage fully through other channels.

A systematic approach to information security, therefore, means treating the tools and activities that are undertaken by the bank as one comprehensive set of interrelated, complementary, and coordinated measures. In a nutshell, development of information systems should be supplemented with technologies of data transfer and protection. These technologies are to ensure security of data transfer. Reliability should be understood on the logical level (information).

References:

1. Commentary on the Information Security Concept of the Central Bank of the Republic of Uzbekistan, Commercial Banks, and Non-Bank Credit Institutions - https://cbu.uz/uz/documents/3332/37539/
2. CERT-CBU (Cybersecurity Center) — Functions and Mechanisms for Ensuring Information Security in the Banking System - https://cbu.uz/uz/about/central-office/divisions/markaziy-bank-cert-cbu-kiberxavfsizlik-markazi
3. “Minimum Requirements for Banks’ Information Security Established” — Regulation on the Obligation to Establish an Information Security Service in Each Commercial Bank - https://yuz.uz/uz/news/banklarining-axborot-xavfsizligiga-doir-minimal-talablar-belgilandi