THE ROLE AND IMPORTANCE OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN BANKS

Rajaboyev Shahboz Shodio‘g‘li
Samarkand Institute of Economics and Service, Assistant of the Department of "Information Technologies"
ORCID: 0000-0002-0997-6689
Isroilov Akmal Anvar og‘li
Student of Samarkand Institute of Economics and Service

Annotation:
This article describes the role and importance of information and communication technologies (ICT) services in modern banking systems. Types of software used in bank information complexes, their functional capabilities, security mechanisms, and operating technologies are deeply analyzed.

Keywords: Information and communication technologies (ICT), bank information systems, software, information security, data processing, automation of banking operations, remote banking services, electronic payment systems.

Introduction.

Information and communication technologies (ICT) today play an important role in all fields, particularly in the finance and banking sector. The effective operation of banking systems depends on many factors, and one of their most essential components is advanced information systems and software. Modern banks widely use ICT solutions to provide their services quickly, safely, and with high quality. This, in turn, expands opportunities for remote interaction with customers, automates electronic payment and settlement systems, and ensures reliable data storage.

Bank information complexes are important infrastructure that not only automate daily operations but also help make strategic decisions, analyze financial processes, and implement digital transformation. Modern software and technologies provide banks with high efficiency, stable operation, and data security. At the same time, they enable offering customers convenient and fast services, which increases competitiveness.

However, there are several major challenges in the introduction and use of ICT services in banks:

1. **Cybersecurity threats** – the need to protect information systems from hacking attacks and data theft.

2. **Adaptation to technological updates** – frequent software updates and the issue of training bank employees to use new systems.
3. **Financial costs** – implementing advanced information systems and providing technical maintenance requires high expenses.
4. **Data integration** – difficulty in combining different software products and coordinating data flow.
5. **Regulatory and normative requirements** – bank information systems and software must comply with local and international legal requirements.
6. **Development of technical infrastructure** – problems ensuring stable operation of servers, network infrastructure, and other technical devices.

The article provides a detailed analysis of the role of ICT services in the banking sector, types of software used in bank information complexes, and their operating technologies. In addition, the advantages of technological solutions and software products used in modern banks, their integration, and effective operating mechanisms are described. The research results help form scientific-practical recommendations for the effective use of information technologies in banking systems.

The growing role of ICT services in the banking sector and the strategic importance of bank information complexes in the conditions of the digital economy are also emphasized. This topic is relevant today not only for scientific research but also for practical banking activities.

Main part.

Information and communication technology services are one of the main pillars of the modern banking system. ICT services enable banks to carry out transactions in real-time, provide customers with mobile and internet banking services, ensure data security, and automate internal processes. Their implementation increases the efficiency of banking activities, improves service quality, and strengthens competitiveness.

Bank information complexes are important infrastructure that integrate all financial, technological, and management processes into a single system. These complexes perform such tasks as customer account management, automatic execution of payment orders, management of credit portfolios, risk analysis, preparation of various reports, and monitoring the security of banking operations. The complexes usually operate based on software modules, and each module serves a separate function.

Principles of Bank Information Systems and ICT Services

Principle Name	Description
Continuity	Ensuring the uninterrupted, continuous operation of the

	system, with services available to customers 24/7.
Security	Protecting data, encrypting it, managing access rights, and applying measures against attacks.
Speed	Processing transactions in real-time and carrying out banking operations without delays.
Reliability	Error-free and stable operation of software, and accuracy of results.
Flexibility	The ability to add new functions, modernize the system, and enable integration.
Modularity	Building the system based on modules, with each module serving a separate function.
Transparency	Automation of internal bank processes and the ability to monitor them.
Integration	Interoperability of systems with other banking applications, payment platforms, APIs, and fintech services.
Data Integrity	Ensuring data remains unchanged, not lost, and stored correctly.
User Convenience	Making interfaces simple and understandable, preventing errors with convenient controls.

Banks use various types of software in their operations. Core Banking System applications centrally manage the bank's main operations. Payment systems such as SWIFT, Uzcard, and Humo help process payments in real time. Security systems include antivirus software, firewalls, DDoS-protection tools, and data-encryption algorithms. Additionally, analytical and management software allows bank leadership to rely on comprehensive data in decision-making processes.

Bank software is based on data-processing technologies. Databases such as Oracle, PostgreSQL, and Microsoft SQL Server allow large volumes of operations to be processed quickly and securely. Cloud technologies are also widely used in modern banking activities. They allow remote management of services, rapid system updates, and increased security. API and integration technologies play an important role in connecting banking services with mobile applications, payment systems, and fintech platforms. Artificial intelligence systems automate customer service, identify fraud, and assist in determining credit scores.

Security requirements in bank information systems hold special importance and include confidentiality, integrity, authentication, access control, backup, and system monitoring. Ensuring these requirements protects banking systems from internal and external threats and increases customer trust.

Threats to Banking Services Posed by Information and Communication Technologies

Information and communication technologies have become the main foundation of banking operations, enabling fast and convenient execution of

payments, settlements, lending, customer service, and many other processes. However, along with the widespread use of ICT services, various threats have also increased. These threats may cause interruptions to the banking system, endanger customer financial security, and damage the bank's reputation. Therefore, ensuring information security is considered one of the most crucial tasks in the banking sector.

One of the most common threats to the banking system is cyberattacks. Hackers attempt to gain unauthorized access to systems, steal customers' personal or financial data, or alter transactions. Such attacks can disrupt the bank's operations or cause major financial losses. DDoS attacks also pose serious danger for banks. During these attacks, a high volume of requests is sent to bank servers, causing systems to malfunction and preventing customers from using internet banking services.

Another major threat to the banking system is phishing and social engineering. These threats aim to deceive customers into handing over their card information or online banking login details. Fake SMS messages, emails, and fraudulent links cause users to unknowingly give their data to criminals, resulting in illegal transfers of funds.

Malicious software (malware) is also highly dangerous for the banking system. Ransomware viruses may block bank servers and demand a payment to restore access. Spyware secretly monitors computer activities and steals user information. Trojan malware can create hidden access points into the system.

Another significant threat is data-base breaches. Since banks store large amounts of confidential information, such a breach can lead to major disasters. Leakage of customer data, illegal use of cards, and loss of bank trust may occur. Network security weaknesses—such as weak passwords, unsecured Wi-Fi networks, and outdated servers—also create opportunities for hackers.

Internal threats also pose serious risks. Irresponsibility or intentional misconduct by employees can cause data leaks or system failures. In many cases, failure to adhere to internal security protocols leads to major problems.

Threats to ICT services do not arise only from human actions. Natural disasters—fires, floods, earthquakes, or power outages—can also negatively affect banking systems. In such cases, data loss or temporary system shutdowns may occur. Therefore, banks implement backup servers, additional power sources, and disaster-recovery centers.

Overall, threats to ICT services in the banking sector are numerous, and each of them plays a crucial role in the continuous operation of the banking system. To reduce these threats, banks must constantly strengthen information-security measures, use modern protection systems, and improve employee qualifications.

Strategies for Ensuring ICT Services in the Banking System

To ensure the safe and uninterrupted operation of information and communication technology (ICT) services in the banking system, several effective strategies are used. First of all, controlling user access rights and applying strong authentication are essential. Two-factor authentication and biometric systems help increase system security. Data encryption and secure transmission through SSL/TLS protocols and AES or RSA algorithms are also key strategies.

Banks use antivirus software, firewalls, IDS/IPS systems, and other cybersecurity tools to protect against malware and attacks. Training employees in information security, establishing password policies, and providing phishing-awareness training strengthen internal security. Backup systems and disaster-recovery centers, along with cloud-storage services, ensure system continuity.

To strengthen network security, protected LAN and Wi-Fi networks, segmentation, and API security are applied. The banking system is constantly monitored, audited, and compliance with security standards is ensured. International and national standards such as ISO/IEC 27001, PCI DSS, and local legislative requirements help maintain high-level information security.These strategies enhance the reliability of banking ICT services, guarantee data security, and ensure uninterrupted customer service.

Conclusion

Information and communication technologies (ICT) play an essential role in the efficient operation of the banking system and the provision of digital financial services. Through ICT services, calculations, payments, lending, customer service, and many other processes are carried out quickly, conveniently, and securely. At the same time, these systems face various threats and risks, including cyberattacks, malware, phishing, insider threats, and technical failures, all of which endanger service continuity and data confidentiality.

To combat these threats, banks use numerous strategies: strong authentication and access control, data encryption, cybersecurity systems, employee training, backup and disaster-recovery mechanisms, network security enhancement, and continuous monitoring and audits. By adhering to international and national security standards, banks keep their systems updated and stable.

Overall, the development of ICT services ensures the digitalization of banking activities, increases service speed and efficiency, and strengthens customer trust. Proper and continuous application of security strategies guarantees system stability, data confidentiality, and uninterrupted operation of the banking sector.

List of References

1. Боронов , Б., и З. Мухаммадиев. «ПУТИ РАСШИРЕНИЯ ИНФОРМАЦИОННОГО ОБЪЕМА УЧЕТА КАПИТАЛЬНЫХ ВЛОЖЕНИЙ В ХОЗЯЙСТВУЮЩИЕ СУБЪЕКТЫ». *Передовая*

экономика и педагогические технологии, т. 2, вып. 2, апрель 2025 г., сс. 444-50, https://inlibrary.uz/index.php/aept/article/view/80274.
2. Ражабоев Ш. Ш. ЦИФРОВИЗАЦИЯ И ЗЕЛЕНЫЙ СЕКТОР В УСТОЙЧИВОМ РАЗВИТИИ //ББК 65.05 П 78. – С. 596.
3. Боронов , Б., & Саломов , Ш. (2025). ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ РАЗВИТИЯ ДЕЯТЕЛЬНОСТИ НЕГОСУДАРСТВЕННЫХ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ. Экономическое развитие и анализ, 3(2), 268–274. извлечено от https://inlibrary.uz/index.php/eitt/article/view/80115
4. Rajaboev S. S. Technologies of Using Multimedia Tools in Teaching Economic Sciences //Spanish Journal of Innovation and Integrity.
5. Боронов Б.Ф., Ахмедов М.А., and Худайназарова Д.Г.. "КОРХОНАЛАРДА ДАРОМАДЛАР ВА ХАРАЖАТЛАРНИ БОШҚА УМУМЛАШГАН ДАРОМАДЛАР ТЎҒРИСИДАГИ ҲИСОБОТДА АКС ЭТТИРИШ МАСАЛАЛАРИ" Экономика и социум, no. 3-2 (118), 2024, pp. 547-556.
6. Боронов Б.Ф., and Мустафоев А.Ф.. "НОДАВЛАТ ТАЪЛИМ ХИЗМАТЛАРИНИ РИВОЖЛАНТИРИШНИНГ ТАШКИЛИЙ МАСАЛАЛАРИ" Экономика и социум, no. 5-2 (120), 2024, pp. 926-929.
7. Ражабоев Ш. Ш. РОЛЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ТЕХНОЛОГИЧЕСКОМ ПРЕДПРИНИМАТЕЛЬСТВЕ //ББК 65.29 я43 Т384. – 2022. – С. 54.