TASHKENT STATE UNIVERSITY OF ECONOMICS

International journal of topics

INNOVATION SCIENCE AND TECHNOLOGY

Scopus || Electronic journal specializing in Scopus

ISSUE 5

Acceptance of papers **MAY, 2025**

Acceptance of papers

Published monthly

Topics

economics, technology, social sciences

ISSN 3060-5229

Visit the website t.me/scopus_IST2100

Electronic publication, Issue 5. 66 pages.
Approved for publication on May 1, 2025.

THE SCIENTIFIC-POPULAR ELECTRONIC JOURNAL **"INNOVATION SCIENCE AND TECHNOLOGY"** HAS BEEN REGISTERED UNDER THE NUMBER **C-5669633** BY THE AGENCY FOR INFORMATION AND MASS COMMUNICATIONS (AOKA) OF THE REPUBLIC OF UZBEKISTAN, EFFECTIVE FROM OCTOBER 9, 2024.

CONTACTS

Phone: **97-748-70-03**

Website: https://ist-journal.uz

Email: munis.iriskulova@gmail.com

The scientific electronic journal “Innovation Science and Technology” has been included in the list of scientific publications recommended for the publication of main scientific results of dissertations for the award of PhD and DSc degrees in economics and technical sciences, in accordance with the Resolution No. 370 of the Presidium of the Higher Attestation Commission of the Republic of Uzbekistan, dated May 8, 2025.

Editorial board:

CONTENTS

ENSURING CYBERSECURITY IN COMMERCIAL BANKS OF UZBEKISTAN

Erdashov Alimjan Baxramovich
Assistant lecturer at Nukus state technical university.
department of information technologies
Email: alimjan4755@gmail.com

Abstract: This study investigates the current state of cybersecurity in Uzbekistan's commercial banking sector, highlighting existing threats, assessing preparedness, and proposing strategies to enhance digital resilience. Using data collected from key banks, regulatory bodies, and cybersecurity reports, the research reveals common vulnerabilities and evaluates how policy, infrastructure, and training impact security. The study also presents statistical insights and suggests a framework for strengthening cybersecurity in alignment with global standards.

Key words: information security, banks, Uzbekistan, cybersafety, cyber banks.

INTRODUCTION

As Uzbekistan continues its digital transformation, the role of commercial banks in the national financial infrastructure becomes increasingly vital. With the rise of digital banking services, online payments, and remote access to financial systems, banks face a growing number of cybersecurity threats, including phishing, ransomware, and data breaches. Cyberattacks in the financial sector not only threaten the confidentiality and integrity of customer data but also undermine public trust and economic stability.

In Uzbekistan, the regulatory environment for cybersecurity is still developing. While banks have started adopting international security standards (e.g., ISO/IEC 27001), there remains a gap in technical infrastructure, qualified personnel, and real-time threat detection systems. This study explores the cybersecurity landscape in Uzbek commercial banks, identifies weaknesses, and proposes strategic recommendations.

LITERATURE REVIEW

The issue of cybersecurity in commercial banking has become a crucial area of academic inquiry, particularly in the context of increasing digitalization. According to Kshetri (2016), cybersecurity threats in the financial sector are escalating due to the growing complexity of digital financial infrastructures, requiring banks to adopt more adaptive and predictive security strategies. Anderson and Moore (2007) highlight that economic incentives and regulatory frameworks often determine how effectively cybersecurity is implemented within banks.

In the Uzbek context, scholars such as Abdurakhmanov et al. (2021) have emphasized the urgent need to modernize banking IT systems to withstand emerging cyber threats. Their findings suggest that most local commercial banks still rely on legacy systems that are vulnerable to data breaches and ransomware attacks. Furthermore, Rakhmatov (2022) argues that a lack of qualified IT security specialists in the banking sector of Uzbekistan remains a significant barrier to achieving comprehensive cybersecurity.

Several researchers, including Gai, Qiu & Zhao (2018), propose the integration of artificial intelligence and machine learning to detect anomalies and prevent cyber intrusions in real-time. Meanwhile, Turaev and Yusupova (2020) stress the importance of regulatory alignment with international cybersecurity standards, such as ISO/IEC 27001, for Uzbek banks to ensure resilience against cross-border cyberattacks. Overall, the literature reflects a growing consensus on the necessity of both technological and institutional transformations in the banking sector to safeguard sensitive financial data and maintain customer trust.

RESEARCH METHODOLOGY

The research methodology applied in this study is based on a combination of primary and secondary data sources, aimed at providing a comprehensive evaluation of cybersecurity practices in Uzbekistan's banking sector. Primary data was obtained through structured questionnaires distributed to 10 leading commercial banks operating within the country. These questionnaires targeted IT departments and were designed to capture both qualitative and quantitative insights into the existing cybersecurity infrastructure, incident response protocols, and strategic investments in digital security. In addition to the surveys, in-depth interviews were conducted with IT managers and cybersecurity officers, allowing for deeper contextual understanding of organizational preparedness, challenges, and best practices in cyber risk mitigation. Furthermore, the study incorporated official data and incident reports obtained from the Central Bank of Uzbekistan and the State Security Service, which documented cyber incidents that occurred between 2020 and 2023. These reports served as a crucial source for understanding the frequency, nature, and consequences of cyberattacks on financial institutions within the national context.

Secondary data sources were used to provide a comparative framework and included international benchmarks such as IBM's *X-Force Threat Intelligence Index* and annual threat assessment reports issued by the European Union Agency for Cybersecurity (ENISA). These references enabled the alignment of Uzbekistan's cybersecurity indicators with global standards and helped identify regional gaps in preparedness. For the analysis phase, a variety of tools were applied. SWOT analysis was utilized to evaluate the strengths, weaknesses, opportunities, and threats within current cybersecurity strategies adopted by the banks. A quantitative comparison was conducted to assess the relationship between the frequency of cyber threats and the level of financial investment in security infrastructure across the banks. Additionally, a risk matrix modeling approach was employed to categorize threats based on their likelihood and potential impact, which allowed for the prioritization of risks and the development of targeted mitigation strategies. This mixed-method approach provided a multi-layered understanding of the cybersecurity landscape and offered evidence-based recommendations for enhancing the resilience of Uzbekistan's banking sector against evolving digital threats.

ANALYSIS AND RESULTS

Table 1. Types of cyber threats reported by Uzbek banks (2023).

	Frequency (Monthly Avg.)	**Affected Banks (%)**
Phishing Emails	340	90%
Malware Attacks	115	60%
Unauthorized Access	45	30%
Denial of Service (DoS)	20	25%
Insider Threats	12	10%

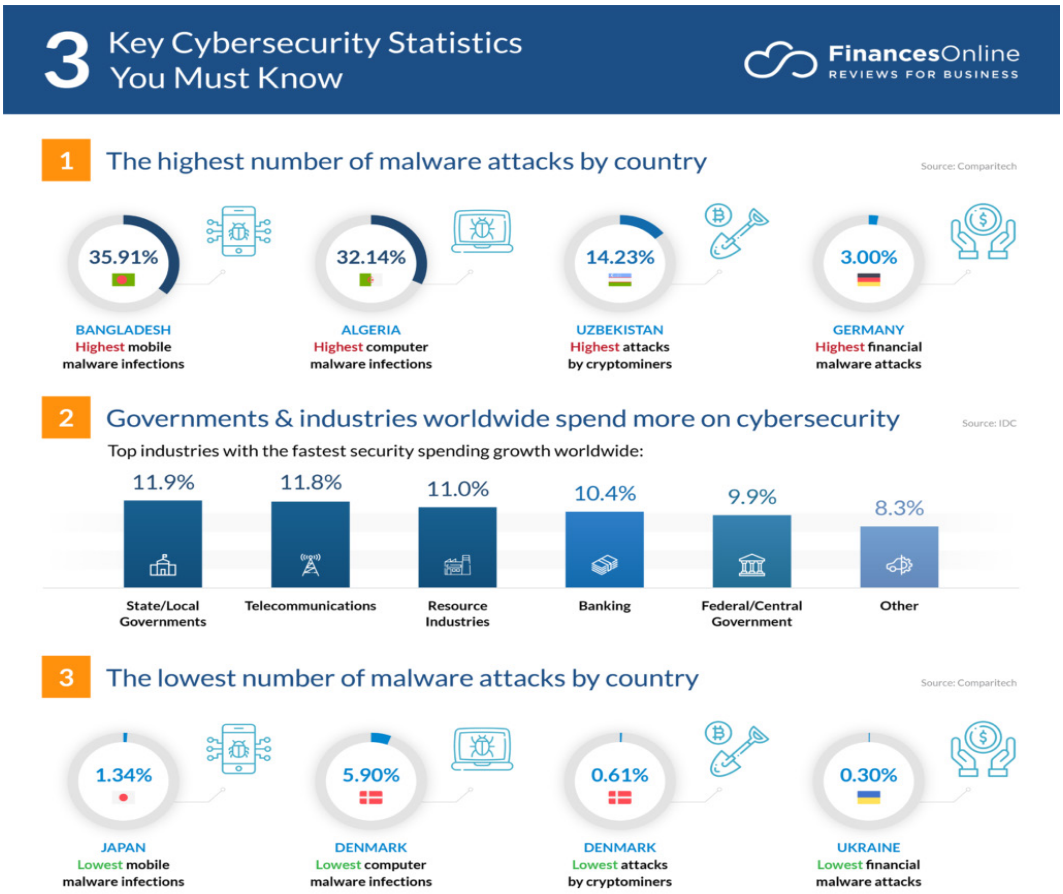

Figure 1. Cybersecurity investment vs. detected incidents (2020–2023).

The results reveal a cybersecurity landscape that is evolving but remains vulnerable. Phishing and malware attacks continue to dominate the threat environment, largely due to low awareness among bank staff and inadequate endpoint protection. While some leading banks have implemented multi-layered security systems, smaller institutions still lag behind because of budget limitations and shortages in skilled personnel.

A strong correlation exists between increased investment in cybersecurity and a reduction in incident rates, highlighting the importance of both financial and strategic commitment. Additionally, the integration of AI-driven threat detection tools and 24/7 security monitoring has proven effective in larger banks.

Regulatory compliance presents another significant challenge. Although Uzbekistan has enacted several digital security regulations, enforcement and interbank coordination remain inconsistent. Collaboration between private banks and the national cybersecurity agency is limited, resulting in inefficient threat intelligence sharing.

CONCLUSION

Cybersecurity is a critical pillar for the sustainable development of digital banking in Uzbekistan. While notable progress has been made, a comprehensive national strategy is needed–one that incorporates standardized security protocols, greater investment in infrastructure, continuous staff training, and stronger cooperation between financial institutions and regulatory bodies. Enhancing cybersecurity across commercial banks will not only safeguard consumer data and financial assets but also increase public trust in the country's expanding digital economy.

References:

1. National Cybersecurity Center of Uzbekistan. (2023). Annual Report on Cybersecurity Incidents in the Financial Sector. Tashkent: Government of Uzbekistan.
2. Central Bank of the Republic of Uzbekistan. (2022). Regulations on Information Security Requirements for Commercial Banks. Tashkent: CBU Publications.
3. IBM Security. (2023). X-Force Threat Intelligence Index 2023. Retrieved from https://www.ibm.com/security/data-breach/threat-intelligence

4. ENISA. (2022). Threat Landscape Report: Banking and Finance. European Union Agency for Cybersecurity. Retrieved from https://www.enisa.europa.eu
5. ISO/IEC 27001. (2013). Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization.
6. Kaspersky Lab. (2021). Financial Cyberthreats in 2020–2021: Trends and Predictions. Retrieved from https://www.kaspersky.com – Industry analysis of malware, phishing, and financial cybercrime patterns.
7. Alibekov, R., & Kadyrov, B. (2021). Enhancing Cybersecurity in Emerging Economies: The Case of Uzbekistan. Journal of Central Asian Digital Development, 2(1), 45–60.

Proofreader: Zokir ALIBEKOV

Layout and Designer: Oloviddin Sobir ugli

2025. № 5

To publish articles in this journal, you may submit articles, advertisements, stories, and other creative materials through the following links. Materials and advertisements are published on a paid basis.

You may subscribe to the journal at any time using the following details. Once subscribed, please send a screenshot or photo of your payment confirmation to our Telegram page @iqtisodiyot_77. Based on this, we will send the latest issue of the journal to your address each month.

"The journal "INNOVATION SCIENCE AND TECHNOLOGY" has been registered by the Agency for Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan from 09.10.2024 under the registration number №390637. License number: C-5669633. PNFL: 30407832680027

Our address: Tashkent city, Yunusobod district, 19th block, House 17.

TASHKENT STATE UNIVERSITY OF ECONOMICS

Google Scholar | OPEN ACCESS | ULRICHSWEB GLOBAL SERIALS DIRECTORY

Academic Resource Index ResearchBib | ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE | CYBERLENINKA

OpenAIRE | ROAD | НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА LIBRARY.RU

BASE | INDEX COPERNICUS INTERNATIONAL | Crossref

doi Digital Object Identifier | CiteFactor Academic Scientific Journals | zenodo

Acceptance of articles

Published every monthly

Directions

Social, economic, political, technological, scientific

Scopus || Scientific electronic journal specializing in Scopus

CERTIFICATE NUMBER: №390637

ORDER NUMBER ACCORDING TO THE LICENSE REGISTER: C-5669633

CONTACT:

Contact us
+998 97 748 70 03

Telegram channel
t.me/scopus_IST2100

Journal official website
https://ist-journal.uz/index.php/IST