MODERN CYBER THREATS IN THE BANKING SECTOR: CLASSIFICATION, ANALYSIS AND COUNTERMEASURES

Akbarova Zarina
Tashkent State University of Economics
"Uzmilliybank" JSC, Methodology Specialist
https://doi.org/10.5281/zenodo.19631210

Abstract. The banking sector continues to be the main target of cyber attacks throughout the worldwide cybersecurity landscape. This article examines the principal categories of cyber threats confronting contemporary financial institutions and analyses the methodological frameworks used in academic literature to classify and evaluate those threats and presents a combined comprehension of effective countermeasures which derives from regulatory technical and organizational elements. The results demonstrate that organizations need to implement multiple security layers because no defense system can protect them against all threats and organizations must use a complete security strategy which combines legal requirements with technical solutions and workforce development to achieve long-term cybersecurity protection in the financial sector.

Keywords: cybersecurity, banking sector, cyber threats, phishing, ransomware, DDoS attacks, digital banking, financial security, risk management.

Аннотация. Банковский сектор остаётся одной из наиболее уязвимых отраслей в глобальном пространстве кибербезопасности. В настоящей статье рассматриваются основные категории киберугроз, с которыми сталкиваются современные финансовые учреждения, анализируются методологические подходы, применяемые в научной литературе для классификации и оценки подобных угроз, а также предлагается синтезированное понимание эффективных мер противодействия, основанных на регуляторном, техническом и организационном измерениях. Результаты исследования свидетельствуют о том, что ни одна однослойная стратегия защиты не является достаточной, а комплексный адаптивный подход, сочетающий законодательные, технологические меры и меры по развитию человеческого капитала, является необходимым условием устойчивой кибербезопасности в финансовом секторе.

Ключевые слова: кибербезопасность, банковский сектор, киберугрозы, фишинг, программы-вымогатели, DDoS-атаки, цифровой банкинг, финансовая безопасность, управление рисками.

Annotatsiya. Bank sektori global kiberxavfsizlik makonida eng ko'p hujumga uchragan tarmoqlardan biri bo'lib qolmoqda. Ushbu maqolada zamonaviy moliya muassasalari duch keladigan kiber tahdidlarning asosiy toifalari ko'rib chiqiladi, ilmiy adabiyotlarda ushbu tahdidlarni tasniflash va baholash uchun qo'llaniladigan metodologik yondashuvlar tahlil qilinadi hamda tartibga solish, texnik va tashkiliy o'lchovlarga asoslangan samarali qarshi choralar borasida sintezlashtirilgan tushuncha taklif etiladi. Tadqiqot natijalari shuni ko'rsatadiki, hech qanday bir qatlamli mudofaa strategiyasi yetarli emas va moliya sektorida barqaror kiberxavfsizlikni ta'minlash uchun qonunchilik, texnologik va inson kapitali choralarini o'z ichiga olgan kompleks, moslashuvchan yondashuv zarurdir.

Kalit so'zlar: kiberxavfsizlik, bank sektori, kiber tahdidlar, fishing, ransomware, DDoS-hujumlar, raqamli banking, moliyaviy xavfsizlik, risklar boshqaruvi.

Introduction

The growing trend of digital banking has created new security risks which now pose unique risks to financial institutions operating in every country. The process of banks transforming their key functions to online systems while developing their mobile banking operations and connecting with external vendors has created new security risks which hackers can exploit [1]. The impact of successful cyberattacks on banking systems extends beyond single banks because they endanger entire financial systems and reduce public confidence in online banking while creating major economic effects in countries that rapidly adopt digital finance systems like Uzbekistan and Central Asian nations [2]. The academic and regulatory communities have dedicated many resources to create strong cyber threat taxonomies which assess threat severity and recommend evidence-based security solutions. The literature shows two main issues because it presents different methods to classify threats and their importance while developing countries have trouble executing theoretical security frameworks. The article presents a synthesis of existing research on cyber threats which affect banking systems and an evaluation of current threat classification systems to identify the most effective security solutions which financial organizations should adopt in today digital landscape [3].

Methodology and literature review

The researchers of this study implemented their research methods through a systematic review combined with a critical evaluation of scholarly articles, official regulations, and organizational documents. Russian scholars have made

significant progress in identifying banking cyber threats through their research which developed multi-dimensional classification systems that separate threats into internal and external origins and technical and social engineering attack methods and infrastructure and application and human attack targets [4]. The United States and European Union jurisdictions have established a research pattern which focuses on developing risk-quantification models and creating enterprise risk management systems that incorporate cybersecurity governance elements [5]. The national banking system of Uzbekistan has implemented digital transformation initiatives which face cybersecurity standard enforcement challenges according to existing academic literature that includes Central Bank of the Republic of Uzbekistan regulatory standards [6]. The banking cybersecurity field identifies six main threat types which appear consistently in multiple research studies: phishing and social engineering attacks, ransomware and malware deployment, distributed denial-of-service (DDoS) attacks, insider threats, advanced persistent threats (APTs), and third-party integration vulnerabilities with open banking interfaces [7].

Results and discussion

The examined literature produces a unified yet complicated understanding of the current cyber danger situation which banks face. Phishing attacks represent the most volumetrically prevalent threat category which accounts for a substantial proportion of all successful intrusions into banking systems worldwide because attackers use human cognitive weaknesses to execute these attacks instead of exploiting technical system flaws. Ransomware attacks serve as the most dangerous threat because they create operational disruptions which can disable complete banking systems for extended durations according to documented case studies from Eastern European financial institutions. DDoS attacks which do not result in data breaches create major reputational damage and operational disruption because attackers now use these attacks to create fake diversions while they access more secure system components. Institutional risk assessments fail to recognize the danger of insider threats because organizations underestimate both malicious insiders and negligent workers who create security breaches which occur more often than attacks which succeed.

APTs, associated predominantly with state-sponsored actors, represent the most technically sophisticated threat category and are of particular concern for systemically important financial institutions whose compromise could yield strategic intelligence of geopolitical value [3]. The analysis further reveals that the proliferation of open banking standards and application programming interfaces

(APIs), while enabling significant innovation in financial service delivery, has introduced structural vulnerabilities that existing security frameworks were not designed to address [7]. In evaluating countermeasures, the literature demonstrates broad consensus around several core principles. First, the adoption of a zero-trust security architecture — in which no user, device, or network segment is granted implicit trust regardless of its position relative to the network perimeter — is increasingly regarded as the foundational technical paradigm for banking cybersecurity [1]. Second, the deployment of artificial intelligence and machine learning systems for anomaly detection and behavioural analytics has demonstrated measurable effectiveness in identifying threat patterns that evade signature-based detection tools [9]. Third, and critically, the literature emphasises that technical solutions alone are insufficient without corresponding investment in cybersecurity culture, staff training, and organisational governance structures that assign clear accountability for information security outcomes [2].

At the regulatory level, frameworks such as the European Union's DORA regulation and analogous national-level instruments in Russia and Uzbekistan reflect a growing institutional consensus that systemic resilience requires not only firm-level compliance but coordinated cross-institutional and cross-border information sharing on emerging threats [6]. The Uzbek regulatory context is particularly instructive in this regard: the Central Bank's progressive digitalisation agenda has created both opportunity and urgency in the development of a nationally coherent cybersecurity framework, and scholarly analysis suggests that the current regulatory architecture, while improving, contains gaps particularly in the governance of third-party risk and incident response obligations [2].

Conclusion

The foregoing analysis establishes that cyber threats facing the banking sector are diverse, evolving, and increasingly sophisticated, resisting reduction to any single classification framework or countermeasure strategy. The scholarly literature, across Uzbek, Russian, and international traditions, converges on the conclusion that effective cybersecurity in banking requires the integration of technical, organisational, and regulatory dimensions within a coherent risk governance framework. The zero-trust architectural paradigm, AI-assisted threat detection, and mandatory cross-institutional information sharing represent the most substantiated technical and policy directions available to financial institutions at present. For developing financial markets, including Uzbekistan, the challenge is compounded by the simultaneity of rapid digitalisation and

institutional capacity-building, creating environments in which vulnerability and ambition coexist. Future scholarly work should continue to develop context-sensitive frameworks for cybersecurity governance that account for the specific regulatory, infrastructural, and human-capital conditions of emerging economies, contributing to a more globally equitable standard of financial system resilience .

References:

1. Stallings, W. Cryptography and Network Security: Principles and Practice. 8th ed. — New York: Pearson, 2022. — 768 p.
2. Yusupov, B. A. Raqamli iqtisodiyotda bank tizimining axborot xavfsizligi muammolari // O'zbekiston iqtisodiyoti. — 2023. — № 2. — S. 45–58.
3. Andress, J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. 2nd ed. — Amsterdam: Syngress, 2019. — 240 p.
4. Doroshenko, S. V., Zhuravlev, A. N. Klassifikatsiya kiberugroz v bankovskom sektore: teoreticheskie podkhody i prakticheskoe znachenie // Finansy i kredit. — 2021. — № 4. — S. 312–328.
5. Verizon. Data Breach Investigations Report 2023. — New Jersey: Verizon Communications Inc., 2023. — 87 p.
6. Toshmatov, Sh. R. O'zbekiston Respublikasi bank tizimida kiberxavfsizlikni tartibga solish: holati va istiqbollari // Huquq va boshqaruv. — 2022. — № 3. — S. 78–91.
7. European Banking Authority. Guidelines on ICT and Security Risk Management. — Paris: EBA, 2020. — 54 p.
8. Kaspersky Lab. Financial Cyberthreats in 2022: Annual Report. — Moscow: Kaspersky Lab, 2023. — 42 p.
9. Nicholson, A., Webber, S., Dyer, S. SCADA Security in the Light of Cyber-Warfare // Computers & Security. — 2020. — Vol. 31, № 4. — P. 418–436.
10. Petrov, M. V. Kiberriski v bankovskoy sisteme: sovremennye metody otsenki i upravleniya // Bankovskoe delo. — 2022. — № 7. — S. 22–35.