CONCEPTUAL APPROACHES TO BANK CYBERSECURITY

Iurie CAPRIAN, PhD student
Moldova State University
E-mail: iuriecaprian@gmail.com
ORCID: https://orcid.org/0000-0001-5484-3087

Abstract

Cybersecurity in banking is a multidimensional notion that brings together strategies, technologies, practices and processes aimed at protecting banks; systems, data and digital networks. The purpose of the research was to present the essence and trends in the development of cybersecurity within banks. The study was conducted by examining reports from specialized companies and expert opinions published in open form on the Internet. The materials thus accumulated allowed the creation of a complex picture of the current development of cybersecurity in banking activities. The main reasons that require bank cybersecurity management are: customer data protection; maintaining customer trust and reputation; compliance with regulations; preventing financial loss; protecting critical infrastructure; ensuring business continuity. It is clear that over the past few years the threat landscape has expanded in complexity and scope. Currently, banks are facing cybersecurity problems that have already become traditional, such as ransomware, unencrypted data, cloud-based cyber-attacks, social engineering, phishing attacks, malware, attacks on third-party providers, supply chain attacks, endpoint security. At the same time, we can talk about new challenges in strengthening the cybersecurity of banks: the evolution of zero trust security; regulatory pressures and compliance-driven security; quantum computing threats to cryptography; AI-powered fraud detection and financial crime prevention. Experts visions for the continued strengthening of cybersecurity in banking are linked to the evolution of advanced technologies and the improvement of regulatory frameworks. To this end, banks will develop innovations related to artificial intelligence, blockchain and quantum computing.

Keywords: *banking; cybersecurity; attack; threat; detection; prevention*
DOI: https://doi.org/10.59642/EDR.3.2025.27
JEL: G21 **UDC:** 336.7

Introduction

Cybersecurity in the banking system is a complex concept that refers to the totality of practices, measures, technologies and strategies implemented by banking institutions to protect digital systems, networks, data, their own networks, as well as customer information from the diversity of cyber threats, attacks and unauthorized access. It provides for the implementation of advanced technologies, strict policies and continuous monitoring to protect against cyber threats. This protection largely extends to sensitive financial information, such as account details, personal data and transaction records, against unauthorized access, theft or attack. Cybersecurity is an important component of the banking security system. (Backbase, 2024), (The Business Research Company, 2025), (Future Processing, 2024), (Claire dela Luna, 2024)

By implementing advanced security technologies, monitoring systems for vulnerabilities, and educating both employees and customers, banks can stay ahead of cybercriminals and maintain the integrity of their operations.

Experts at Backbase (2024) state: “Cybersecurity is important for banks due to their role as custodians of not only money, but also sensitive personal and financial information. The high value of this data means banks are prime targets for cyberattacks, making it essential for them to protect themselves in various ways. Customer trust is another valuable commodity that banks can’t afford to lose. Even a single breach can damage a previously solid reputation and erode customer confidence, leading to loss of business. And financial loss is, of course, another major consideration.”

The timeliness of the study was dictated by the seriousness of the situation regarding the dynamics of global losses from cyberattacks on banks.

According to the International Monetary Fund (2024), the global financial sector has lost $12 billion in the last 20 years due to over 20,000 cases of cyberattacks. This increase in the scale of cyberattacks is due to an increase in digitalization and geopolitical tensions.

Through a broader approach, data published by Embroker Team (2025) can be presented, according to which the global costs incurred by companies due to cybercrime amounted to 8 trillion dollars in 2023, and the prospect of this indicator increasing is 24 trillion dollars by 2027.

By implementing modern security technologies, monitoring systems for vulnerabilities, and educating both employees and customers, banks can create solid protection against cybercriminals and maintain the integrity of their business.

This article aims to present current approaches to cybersecurity within commercial banks.

MAIN CONTENT

1. Materials and Methods

The conducted study focused on the conceptual aspects of cybersecurity management within banking institutions. The information base of the research was created based on the examination of publications by experts in the field of banking cybersecurity and reports from specialized companies. The accumulated information allowed for the creation of a background image on the essence and dynamics of the global state of work in the field of banking cybersecurity. Then, a synthesis was created of current trends, future prospects, conclusions and recommendations for improving cybersecurity systems in banking institutions.

2. Results and Discussion

The cybersecurity system within banks is intended to ensure the fulfillment of the following functions (Claire dela Luna, 2024), (Darktrace):

- *Customer data protection*. Customer data, from social security numbers and addresses to sensitive financial details, is stored by banks and if compromised, can lead to identity theft, fraud and significant financial losses for individuals. In this area, cybersecurity plays a substantial role in defending this information against unauthorized access. Encryption, firewalls and secure access controls are some of the measures taken by banks to ensure that customer data remains protected.
- *Maintaining customer trust and reputation*. Cybersecurity has a significant impact on customer trust in the bank that serves them. To have a quality banking service, customers must have full confidence that their financial information is secure and that their transactions are carried out safely.

Security issues can reduce confidence in a bank's ability to protect sensitive personal and financial data. (Backbase, 2024) Studies by some specialized companies confirm this. For example, Centrify found that 65% of data breach victims lost trust in an organization as a result of the breach. IDC reported that 80% of consumers in developed countries are willing to leave a company if their information is compromised in a security breach. (Kenyon, 2021) According to the recent Accenture consumer banking survey, 58% of bank customers are concerned about the security of their personal

and financial data and the potential for being attacked by hackers when using their banks' personalized products. (Abend)

Robust cybersecurity measures are extremely important for maintaining bank customer trust, as well as ensuring that customers feel safe when conducting transactions and sharing sensitive information with their bank.

- *Compliance with regulations*. Banks are required to adhere to strict data protection standards, and cybersecurity compliance in the financial industry is heavily regulated. For example, legislation such as the General Data Protection Regulation in the European Union and the California Consumer Privacy Act in the US set strict guidelines on how banks must handle and protect customer data. Compliance with these regulations requires significant cybersecurity measures, including regular security audits, data encryption, and secure authentication processes. Failure to comply with the established regulations can result in significant fines and legal repercussions.
- *Preventing financial loss*. A successful cyberattack can lead to significant financial losses for banks. Criminals can steal money directly from bank accounts, manipulate transaction records, or use stolen credit card information to make fraudulent purchases. Also worth mentioning are the costs associated with system downtime or the high cost of repairing damaged systems. Furthermore, banks can be fined for violating regulations, incur legal fees, and pay compensation to compensate customers affected by cybercrime or identity theft due to a cyber breach. Implementing robust cybersecurity for financial services can minimize banks' financial risks associated with cybercrime by investing in advanced cybersecurity solutions.
- *Protecting critical infrastructure*. Banking infrastructure, including online banking platforms, ATMs, and payment processing systems, can become a target for cybercriminals. Attacks on these systems could lead to operational disruptions, affecting customer service.
- *Enhancing operational efficiency*. Effective cybersecurity practices not only protect banking institutions from cyberattacks, but also enhance their operational efficiency. When systems and data are secured, banks can ensure uninterrupted services and minimize downtime caused by cyber incidents.
- *Future-proofing against emerging threats*. As technology advances, so do the methods used by cybercriminals. Banks must stay one step ahead of these emerging threats by continuously updating their cybersecurity strategies. Strengthening cybersecurity efforts ensures that banks are prepared to deal with new and more sophisticated cyberattacks.

At the moment, we can talk about the formation of a global cybersecurity market in the banking sector, which, due to the impact of increasing cyber threats and the need for robust security measures, is showing rapid growth, which is presented differently through the evaluations of different specialized companies:

- In 2023, Allied Market Research valued the global banking cybersecurity market at $74.3 billion in 2022 and forecasted growth to $282 billion by 2032.
- According to Maximize Market Research (2024), the value of the banking cybersecurity market was $273.24 billion in 2023 and its size is estimated to grow to $623.17 billion in 2030. The main factor for this growth is considered to be the increasing adoption of new technologies, stimulated by digital transformations and large-scale migrations to the public cloud for multiple applications.
- Specialists from The Business Research Company (2025) estimate the size of the banking cybersecurity market at $317.98 billion in 2024, with a forecast growth to $359.88 billion in 2025

and $585.32 billion in 2029. This growth is attributed to risk management, sophistication of cyber threats, digital transformation, mobile banking security and cloud security.

According to a PYMNTS Intelligence report, "Protecting Accelerated Disbursements From Fraud", 71% of financial institutions are using artificial intelligence and machine learning to detect fraud, up from 66% in 2023. This is to detect anomalies and patterns those human analysts might not notice, enabling faster decisions. (PYMNTS, 2024)

The following features of the examined market are also noteworthy (Grant):

- It is forecasted that by 2025, 48% of banks will use blockchain technology for secure and transparent transactions;
- 75% of banks are preparing for quantum cybersecurity threats by 2030;
- By 2025, there will be a global shortage of qualified cybersecurity professionals of 3.4 million positions.

The increasing importance of banking cybersecurity is driven by many factors, including:

- *Increased cyber threats.* Banks are currently facing an increase in cyber threats, driven by the increasing number and sophistication of cybercrime and the widespread adoption of digital technologies.

Some experts say that artificial intelligence has changed the cyber threat landscape, as AI-powered cyberattacks use machine learning to rapidly scan security systems, identify and exploit vulnerabilities. Cybercriminals have become able to automate attack processes, making these attacks more sophisticated and more frequent. According to a 2023 survey by CFO.com, 85% of cybersecurity professionals believe that the increase in cyberattacks is due to the application of artificial intelligence. (Embroker, 2025)

- *Regulatory Compliance*. Regulatory bodies have set stricter cybersecurity standards, forcing banks to take more robust security measures.
- *Technological advancements*. The increasing application of emerging technologies such as artificial intelligence, blockchain, quantum computing and cloud computing is making cybersecurity systems more effective in protecting against emerging threats. Also worth noting is the implementation by banks of solutions such as multi-factor authentication, encryption and regular security audits.
- *Mobile banking growth*. With the increasing use of mobile devices, they are becoming even more vulnerable to cybersecurity threats. Mobile banking applications can be targeted by cyberattacks, infecting devices with malware or gaining access to customer accounts. Phishing is also practiced to convince users to download malicious applications or click on fraudulent links. Similarly, a person's banking credentials are stolen or financial transactions are intercepted. Furthermore, mobile devices can be lost or stolen and used in an unauthorized manner by third parties to access a person's sensitive information. (Jasińska, Dobosz, 2024)

The most common cyber threats to banks are (Backbase, 2024), (Future Processing, 2024), (Jasińska, Dobosz, 2024):

- *Phishing attacks* are a form of cybercrime in which attackers trick individuals into providing sensitive information, such as login credentials, credit card numbers, or other banking details. They often resort to impersonating trusted entities (such as the bank itself) using social engineering to trick victims into responding. Using fake login pages, fraudulent emails from the bank, or even fake text alerts (e.g., by cybercriminals), access to a bank's systems can be gained.

The most common phishing tactic is to create a sense of urgency or panic with the aim of getting users to act without thinking critically.

In 2023, 27.32% of total phishing attacks globally were linked to financial institutions, down from 36.3% in 2022. (Petrosyan, 2024)

Malware or malicious software is any program or file that is intentionally harmful to a computer, network, or server, and is used to disrupt operations or steal sensitive data. Malware attacks infect devices and networks for various criminal purposes.

Types of malwares include computer viruses, worms, Trojan horses, ransomware and spyware. These malicious programs steal, encrypt and delete sensitive data; alter or hijack core computing functions; and monitor end users' computer activity. (Yasar, Lutkevich, 2024)

- *Banking Trojan* is a type of malware designed to steal personal financial data, such as online banking credentials, credit card details, or account login information. Once infected, the Trojan can monitor online activity, capture keystrokes, display fake banking web pages, or redirect users to fraudulent sites. (Keepnet, 2024)
- *Ransomware attacks* are a type of malware-based cyberattack that targets a user's or organization's data and encrypts a victim's data or systems, making them inaccessible. Ransomware is one of the most widespread types of malwares.

In the banking sector, ransomware attacks disrupt financial operations and put confidential financial information at risk. Encryption makes data unreadable and inaccessible and blocks the bank’s access to its own data. Once critical data is locked, important operations such as processing transactions, accessing customer accounts, and even internal communications can become impossible. Attackers then demand a ransom in exchange for a decryption key. The potential reputational and financial losses force banks to pay the ransom in order to quickly resume their banking activities.

In 2025, expert Anthony M. Freed announced the documentation of 3,348 ransomware attacks on banking infrastructure globally, highlighting a shift in tactics expressed through complex, multi-stage operations. Typically, these attacks begin with reconnaissance, followed by lateral movement that exploits identity management flaws to gain preferential access. Once inside, attackers exfiltrate sensitive data before deploying encryption payloads.

In 2024, the average cost of a security breach was $6.1 million per incident, a 10% increase from the previous year. (Feed, 2025)

- *Distributed Denial of Service (DDoS)* attacks are a form of cyberattack that are aimed at disrupting operations within a bank’s online services, such as websites, mobile apps, or payment systems. Criminals use a network of computers known as a botnet to flood a bank’s servers with requests or data packets, overwhelming the server’s ability to process the requests. As a result of the attack, the system slows down, freezes, or becomes unresponsive. Given that banks present a large attack surface, hackers can use DDoS to distract security teams while they launch additional cyberattacks, allowing them to demand a substantial ransom.
- *Insider threats* are related to the involvement of individuals within the banking institution (employees, contractors, or business partners) who may abuse their access to sensitive information for malicious purposes. For example, a disgruntled bank employee might disclose sensitive customer data as an act of revenge or for financial gain.

- *Advanced persistent threat (APT)* is a sophisticated cyberattack in which an attacker establishes an undetected presence on a network to steal sensitive data over an extended period of time. An APT attack is carefully planned and executed to ensure infiltration of the bank, circumvent existing security measures, and remain undetected. APT execution requires a higher degree of customization and sophistication than a traditional attack. Criminals typically form well-funded and experienced cybercriminal teams that target high-value institutions. They typically spend significant time and resources examining and identifying vulnerabilities within the institution. (Baker, 2025)
- *Third party risk.* Banks benefit from the services of third-party providers, such as access to new technologies, risk management tools, cloud services and more. Each of these providers can be a target for cyber-attacks. In the event of a successful attack, the bank can be disconnected from work and, therefore, its customers can be affected. The greater the number of providers, the greater the possibility of attacks. A similar problem arises in connection with the use of remote employees. Each remote employee presents a new security challenge, as it involves an activity outside the bank's network or the use of unsecured public networks. Monitoring how employees comply with data security procedures or software updates is relatively complicated for the banking institution.

In international practice, the following cybersecurity solutions for banks have been developed: (Future Processing, 2024), (Harry Menear, 2024), (Infosecurity Europe, 2024):

- *AI-driven threat detection and response*. Artificial intelligence (AI) models have the ability to recognize patterns in large volumes of unstructured data, which can be applied to threat detection for cybersecurity systems. AI tools can flag subtle differences, anomalies, and patterns that could indicate a zero-day threat or the presence of a malicious actor in the system.
- *Encryption and secure data storage*. Encryption and secure storage methods are one of the foundations of cybersecurity in banking. Encryption is designed to ensure that, even if data is intercepted, it cannot be read without the decryption key. Banks are required to use high-performance encryption protocols and update them periodically to remain resilient to emerging threats. Secure data storage practices, such as using secure data centers and implementing redundancy, are also extremely important for protecting sensitive information.
- *Multi-factor authentication (MFA).* MFA is a security and identity protection standard for customers who bank, shop, and manage their lives entirely online. MFA is a multi-step account authentication process that requires more information than just a username and password before they can access their accounts. MFA can include something they know (password), something they have (smartphone), or something they are (biometrics). MFA can significantly reduce account hacking by allowing security teams to detect suspicious activity during sign-up processes.
- *Access controls and privileged account management*. Banks should use role-based access controls, and employees should only have access to the information necessary for their roles. Privileged accounts should be closely monitored, and access should be granted on a need-to-know basis. Regularly reviewing and updating access controls can help mitigate the risk of insider threats.
- *Secure software development lifecycle*. Integrating security into the software development lifecycle is intended to ensure that applications are designed with security as an initial priority and includes the use of best coding practices and regular updates to address security vulnerabilities.
- *Distributed Denial of Service (DDoS) mitigation.* Cybersecurity teams can perform DDoS attack mitigation by implementing a load balancer, restricting requests from certain locations, and blocking communication from outdated or unused ports, protocols, and applications.

- *Database activity monitoring.* Database's record and store information. An attacker who gains access to the database can then have write access to the entire set of tables, which means they can easily delete any activity rows associated with their presence and steal data. Database activity monitoring refers to a set of tools that monitor and analyze database activity. Its purpose is to flag and identify fraudulent, illegal, or unwanted behaviors that occur in a system. These tools run and function without any serious impact on the user experience. Given that most databases do not monitor or flag suspicious activities, unless there is a tool that handles activity monitoring, third-party solutions become a necessity in many cases.
- *SQL injection prevention.* SQL injection is a code injection technique used by attackers to steal, falsify, and manipulate data. Such an attack can led to attackers gaining unauthorized access to sensitive data, such as credit card information, PIN codes, or other private information. In banking, failure to prevent SQL injection can result in attackers altering balances, reversing transactions, and even transferring money to their bank accounts. Cyberattackers inject SQL code into the backend of a target system when they discover unprotected user data entries in a web application or web page. Hackers can then exploit this vulnerability to locate the IDs of other users in the database, impersonating these users (usually those with data privileges, such as the database administrator) to run malicious code on the system.
- *Secure payment gateways* are important for protecting online transactions. Banks should use payment gateways that comply with industry standards, such as the Payment Card Industry Data Security Standard. These gateways encrypt transaction data, ensuring that sensitive information, such as credit card details, is transmitted securely. They should also support tokenization, which replaces sensitive data with unique identifiers, reducing the risk of data exposure.
- *Real-time transaction monitoring* helps detect and prevent fraudulent activity by examining transaction patterns and flagging suspicious behavior. Banks can use machine learning algorithms to identify anomalies and take immediate action to mitigate risks.
- *Employee training and awareness*. Banks should implement ongoing training programs to inform employees about the latest threats and best practices. These include regular phishing simulations, workshops, and certifications. Encouraging employees to report suspicious activity can also help identify potential threats early.
- *Customer education*. Banks should provide resources and guidance on recognizing phishing attempts, using strong passwords, and avoiding public Wi-Fi networks for financial transactions. Regularly updating these educational materials and conducting awareness campaigns can help maintain a high level of customer vigilance.
- *Incident response planning*. Having a robust incident response plan is important to minimize the impact of security breaches. Banks should develop and regularly update incident response plans, setting out the steps to be taken in the event of a cyber-attack. This includes identifying key stakeholders, establishing communication protocols and conducting regular exercises.
- *Regular security audits*. Conducting regular security audits can help identify vulnerabilities and comply with banking industry standards. These audits should include penetration testing, vulnerability assessments, and code reviews. It is recommended that banks conduct these audits at least annually or whenever significant changes are made to their systems.

The future of cybersecurity in banking has the following features (Claire dela Luna, 2024):

- *AI-driven security*. By leveraging artificial intelligence technologies, banking institutions can improve their cybersecurity systems. At the same time, successfully implementing AI-based security solutions requires skilled specialists, strategic planning, and a commitment to continuous improvement. (Krakowczyk, 2024)
- *Quantum-resistant security*. Although quantum computing is still in its infancy, it will have a significant impact on encryption and security, either improving protection or introducing new vulnerabilities. As a result, banks will be required to develop security solutions that can deal with the threats posed by quantum computing.
- *Integrating blockchain with cybersecurity*. Many experts have high hopes for the integration of blockchain technology with advanced cybersecurity measures, which can create a more secure and efficient banking ecosystem. (Infosys BPM)
- *Compliance-centric approach*. The future of cybersecurity in banking will be driven by the evolution of advanced technologies and increasingly stringent regulatory frameworks. Banks will be required to align their operations with evolving regulatory requirements and compliance standards, which will force banks to be one step ahead in terms of compliance and data protection strategies.
- *Platformization*. Banks are increasingly using unified cybersecurity platforms to streamline security activities and improve efficiency. On the other hand, many companies operating in the field of banking cybersecurity are increasingly focusing their attention on developing advanced platforms, such as the Extended Detection and Response (XDR) platform. XDR is a cybersecurity platform that integrates and correlates information from multiple security products to provide a more comprehensive and contextualized picture of potential security threats in the banking institution's IT environment. (The Business Research Company, 2025)

Conclusions

With the expansion and deepening of banks' activity in cyberspace, the problems caused by cybercrime tend to become more acute, which implies the need to improve cybersecurity performance. It is a broad complex of technologies, protocols and methods designed to ensure protection against cyber-attacks, malware, viruses, hacking and unauthorized access. The purpose of cybersecurity activities is to prevent, detect and combat various types of cyber threats. The activity of improving the cybersecurity of banks takes place under the pressure of the need to reduce the operational, financial and legal impact of cyber-attacks and data breaches; strengthen customer trust; ensure compliance with existing regulations and anticipate their evolution; ensure the efficiency of banking activity by optimizing the use of resources. The increasing diversity of cybercrimes in the banking sector has necessitated the development of high-performance technologies and tools for managing banking cybersecurity worldwide. The continuous strengthening of cybersecurity in the banking sector is linked to the evolution of advanced technologies and the improvement of regulatory frameworks. This concerns the detection of cybercrimes and their prevention based on artificial intelligence, the application of cryptography represented by quantum computing, the application of blockchain technology.

References

1. Abend Valerie. Guardians of Trust: Navigating Cybersecurity in Banking. Available at: https://bankingblog.accenture.com/navigating-cybersecurity-banking. [Accessed 13.05.2025].

2. Allied Market Research, 2023. Cybersecurity in Banking Market Size, Share, Competitive Landscape and Trend Analysis Report, by Type, by Organization Size, by Deployment Mode: Global Opportunity Analysis and Industry Forecast, 2023-2032. Available at: https://www.alliedmarketresearch.com/cybersecurity-in-banking-market-A12738. [Accessed 14.05.2025].
3. Backbase, 2024. Cybersecurity in banking: the complete guide. Available at: https://www.backbase.com/blog/modernization/cybersecurity-in-banking-the-complete-guide. [Accessed 27.03.2025].
4. Baker Kurt, 2025. Advanced Persistent Threats (APT) Explained. Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/#:~:text=An%20advanced%20persistent%20threat%20(APT)%20is%20a%20sophisticated%2C%20sustained,Destruction. [Accessed 21.05.2025].
5. Claire dela Luna, 2024. Cybersecurity in Banking: Threats, Solutions & Best Practices. Available at: https://www.esecurityplanet.com/cloud/cyber-security-in-banking/. [Accessed 27.03.2025].
6. Darktrace. What is Financial Service Cybersecurity?. Available at: https://www.darktrace.com/cyber-ai-glossary/cybersecurity-for-financial-services. [Accessed 10.05.2025]
7. Embroker Team, 2025. Top 16 cybersecurity threats in 2025. Available at: https://www.embroker.com/blog/top-cybersecurity-threats/#:~:text=According%20to%20a%202023%20survey%20from%20CFO.com%2C,in%20cyberattacks%20is%20due%20to%20AI%20tactics. [Accessed 12.05.2025].
8. Embroker Team, 2025. Cyberattack statistics 2025. Available at: https://www.embroker.com/blog/cyber-attack-statistics/. [Accessed 12.05.2025].
9. Freed Anthony M., 2025. Ransomware Attack on Financial Institutions Average $6.08 Million in Losses. Available at: https://www.halcyon.ai/blog/ransomware-attack-on-financial-institutions-average-6-08-million-in-losses. [Accessed 12.05.2025].
10. Future Processing, 2024. Cybersecurity in banking: importance, threats and solutions. Available at: https://www.future-processing.com/blog/cybersecurity-in-banking/#what-is-cybersecurity-in-banking-and-why-is-it-important. [Accessed 29.04.2025].
11. Grant Ejimone. Banking Cybersecurity Statistics and Trends (2025). Available at: https://www.absrbd.com/post/banking-cybersecurity-statistics-and-trends#:~:text=Key%20Takeaways,for%20secure%20and%20transparent%20transactions. [Accessed 25.04.2025]
12. Infosys BPM. Securing the Future of Banking: Exploring the Synergy of Blockchain and Cybersecurity. Available at: https://www.infosysbpm.com/blogs/financial-services/securing-the-future-of-banking-exploring-the-synergy-of-blockchain-and-cybersecurity.html. [Accessed 02.06.2025].
13. International Monetary Fund, 2024. IMF: Cyberattacks Drain $12B from Financial Institutions in Two Decades. Available at: https://www.financemagnates.com/institutional-forex/imf-cyberattacks-drain-12b-from-financial-institutions-in-two-decades/. [Accessed 29.04.2025].
14. Jasińska Dorota, Dobosz Marcin, 2024. Cybersecurity in Banking: Threats and Mitigation Strategies. Available at: https://neontri.com/blog/cybersecurity-in-banking/#:~:text=Mobile%20vulnerabilities,gain%20access%20to%20user%20accounts. [Accessed 24.05.2025].
15. Kenyon Tilly, 2021. What causes the most damage, losing data or trust?. Available at: https://cybermagazine.com/cyber-security/what-causes-most-damage-losing-data-or-trust. [Accessed 17.05.2025].
16. Keepnet, 2024. What is a Banking Trojan?. Available at: https://keepnetlabs.com/blog/what-is-a-banking-trojan. [Accessed 17.05.2025].
17. Krakowczyk Tomasz, 2024. The Role of AI and Cybersecurity in the Financial Sector. Available at: https://softwaremind.com/blog/the-role-of-ai-and-cybersecurity-in-the-financial-sector/. [Accessed 02.06.2025].
18. Maximize Market Research, 2024. Banking Cyber Security Market – Global Industry Analysis And Forecast (2024-2030). Available at: https://www.maximizemarketresearch.com/market-report/global-banking-cyber-security-market/92354/. [Accessed 12.05.2025].
19. Menear Harry, 2024. Top 7 Cybersecurity solutions for financial institutions. Available at: https://www.fintechstrategy.com/blog/2024/08/07/top-7-cybersecurity-solutions-for-financial-institutions/. [Accessed 22.05.2025]
20. Petrosyan Ani, 2024. Share of financial phishing attacks worldwide from 2016 to 2023. Available at: https://www.statista.com/statistics/1319867/share-of-financial-phishing-attacks/#:~:text=In%202023%2C%20around%2027.32%20percent%20of%20total,phishing%20attacks%20worldwide%20from%202016%20to%202023. [Accessed 24.04.2025].
21. PYMNTS, 2024. 71% of Financial Institutions Turn to AI to Fight Faster Payments Fraud. Available at: https://www.pymnts.com/fraud-prevention/2024/71-percent-of-financial-institutions-turn-to-ai-to-fight-faster-payments-fraud/. [Accessed 24.04.2025].
22. The Business Research Company, 2025. Banking Cyber Security Global Market Report 2025. Available at: https://www.thebusinessresearchcompany.com/report/banking-cyber-security-global-market-

report#:~:text=What%20Is%20The%20Banking%20Cyber%20Security%20Market%20Growth%20Forecast?,orchestration%2C%20collaborative%20threat%20intelligence%20sharing. [Accessed 26.03.2025].
23. Yasar Kinza, Lutkevich Ben, 2024. What is malware? Prevention, detection and how attacks work. Available at: https://www.techtarget.com/searchsecurity/definition/malware. [Accessed 18.05.2025].