DOI: 10.55643/fcaptp.4.63.2025.4790

THE IMPACT OF DIGITALIZATION ON THE FINANCIAL INSTITUTIONS' ECONOMIC SECURITY IN THE FACE OF GROWING CYBER THREATS

Alina Kudinova
PhD in Economics, Associate Professor of the Department of Management and Logistics, National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine;
e-mail: alinachaikina@ukr.net
ORCID: 0000-0003-3821-2079
(Corresponding author)

Oleksandra Maslii
PhD in Economics, Associate Professor of the Department of Finance, Banking, and Taxation, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine;
ORCID: 0000-0003-2184-968X

Valerii Smokvina
PhD Student, Department of Finance, Banking and Taxation, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine;
ORCID: 0009-0009-2520-3764

Kyryl Tsyhanenko
PhD Student, Department of Finance, Banking and Taxation, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine;
ORCID: 0009-0004-1580-253X

Received: 03/04/2025
Accepted: 05/08/2025
Published: 31/08/2025

ABSTRACT

The primary objective of this study is to identify the various cyber threats that impact the operations of financial institutions, particularly their information and economic security. This is crucial for the sustainable growth of the country and has a direct effect on its economic security. The financial sector globally experiences the highest losses due to cyber incidents. On average, financial organizations around the world incur losses of approximately USD 5.9 million per incident, which is higher than the average loss across all industries, estimated at USD 4.45 million. Financial institutions incur losses not only from ransom payments to prevent the disclosure of stolen data and the costs associated with restoring infrastructure after ransomware attacks, but also from direct financial losses in certain situations.

This study identified the most common types of cyberattacks, examined their impact on the operations of financial institutions, and suggested ways to respond to and prevent such incidents. For the first time, an algorithm for the strategic management of digitalization in financial institutions was proposed, aimed at enhancing their economic and informational security. The algorithm can be implemented at all managerial levels to reduce the influence of subjective risk factors. Additionally, a multifactor predictive model has been developed and substantiated, which represents a further development of existing approaches to assessing information and economic security in financial institutions. This model integrates internal (organization-controlled) and external (environmental) factors and utilizes statistical methods and machine learning techniques to analyze data and forecast security levels. As digitalization continues to evolve in our country, financial institutions must adapt and embrace innovation to ensure sustainable development, even under martial law.

Keywords: economic security, cyber threats, information security, management, financial institutions, business strategy, digitalization, digital technologies

JEL Classification: G21, G28, O33, L86, K24, D81

INTRODUCTION

As of today, both domestic and foreign organizations (institutions) are subject to various types of hacker attacks aimed at disrupting business processes and obtaining illegal monetary benefits during these attacks. Certainly, each organization and institution must implement a set of measures that will enhance cybersecurity and establish a dependable strategic framework for actively countering these risks and external threats. The relevance of the topic for financial institutions operating in Ukraine has increased since martial law was introduced, many enterprises, institutions, and organizations have been relocated, and lost qualified personnel, while continuing to adhere to the strategic course that the President of Ukraine introduced for the full digitalization of various processes, the creation of the so-called "state in a smartphone." Research shows that those financial institutions that continued to invest in the implementation of digital technologies were able to quickly adapt to new conditions and provide access to financial resources to stabilize economic security during the war. An important role in this process

DOI: 10.55643/fcaptp.4.63.2025.4790

is played by the development of financial technologies (FinTech), which simplifies risk management and increases the transparency of financial transactions.

Recorded cases of cyberattacks in 2022 and 2023 pose a significant threat to the functioning of Ukraine's banking system, due to the high level of cybercrime and weak cybersecurity. In addition, there is an imbalance between the development of the digital economy and its integration into the financial sector, since although the IT sector provides about 4.5% of the country's GDP, to achieve the realization of its existing potential, investments in digital infrastructure, increasing digital skills among the population, and strengthening the research base are necessary.

That is why it is relevant to study the European experience in ensuring the economic security of financial institutions in the face of growing cyber threats. It is also relevant to develop practical recommendations for building a strategy to counter various cyber challenges based on identifying these risks and threats and exploring the possibilities of using digital technologies to ensure the sustainable functioning of the country's financial system.

LITERATURE REVIEW

An analysis of literary sources reveals various approaches to understanding the impact of digitalization on the cybersecurity levels of institutions and organizations. Specifically, some authors (Koibichuk V., Kurovska Yu., 2022) examine how integral indicators of socio-economic transformations driven by digitalization influence a country's digital development. They also suggest conducting research using various methodologies, including assessments of digital development levels, the national cybersecurity index, the Basel AML index, and others.

This approach is relevant, but it is designed to determine the level of the country's cybersecurity and does not reveal the specifics of the application of digital technologies in the financial sector. There is no list of types of cyber threats or possible strategies for countering them.

Other researchers (Barchenko N., Lubchak V., Lavryk T., 2022) suggest defining a set of indicators to measure a country's digital transformation progress, considering its capacity to combat cyber threats in the pursuit of sustainable development goals. They propose a series of formal mathematical models to assess the national level of digital development, factoring in the country's ability to counter cyber threats from a systems analysis perspective.

The authors emphasise the necessity of applying a systemic approach and the importance of determining indicators that ensure the country's cybersecurity. However, the study primarily focuses on the country's cybersecurity without placing sufficient emphasis on its impact on the economic security of financial institutions or the applicability of the proposed model.

Onyshchenko V., Yehorycheva S., Maslii O., and Yurkiv N. (2022) found that failing to address the negative impact of emerging threats, such as the cryptocurrency market, electronic payment services, cybercrime in the financial system, and the spread of misinformation, undermines financial security. The authors provide a comprehensive description of national financial security, considering the concept of the information society.

The authors have acknowledged risks and threats to the state's financial security in the context of digitalization. However, greater attention should also be given to the information, financial, and economic security of financial institutions. In their study, the authors (Yarovenko et al., 2024) examine the impact of digitalization on financial security, focusing on cashless transactions and cryptocurrency. The report analyzes both the benefits and challenges of digitalization, evaluates existing regulatory frameworks and cybersecurity measures, and identifies key policy implications for ensuring digital financial security.

The authors propose that to enhance economic security and trust in the digital economic ecosystem, policymakers should prioritize regulatory clarity, risk-based regulation, cybersecurity resilience, and consumer education. However, it is suggested that these measures should not only focus on the political aspect, such as the development of state policy, but also be implemented at the operational level. This includes training personnel within financial institutions to ensure competence in cybersecurity.

Some scholars (Blynda Yu., Kirkach O., 2024), analyzing the experiences of developed countries, argue that successful digitalization necessitates a holistic approach. This approach should encompass infrastructure development, personnel training, and legislative reforms. They emphasize the importance of collaboration between the government, private sector, and civil society to achieve optimal efficiency in public administration through digital technologies.

The authors' opinion is acknowledged; however, it should be noted that their approach is focused on increasing citizen participation in decision-making processes using e-democracy tools, such as online voting and public consultations. However, the impact of this approach on the financial sector is not addressed.

Other authors (Narboy G., Faridakhon A., Shakhzod S., Rano A., 2022; Zedgenizova I., Ignatyeva I., Zarubaeva E., Teplova D., 2021) emphasize that addressing issues of economic security has become increasingly urgent in the context of non-stationary processes in the modern world, with a focus on predicting threats and challenges. They also explore the technosphere's significant role in shaping the scientific, social, and economic order, citing positive examples from countries such as the United States, China, and Japan. Their research delves into the impact of economic digitalization on economic security, analyzing both the advantages and disadvantages of digitalization, the evolving requirements for economic security in the digital age, and the digitalization experiences of developed countries.

The authors' opinion is agreed with; however, their study focuses on the national level, considering the possibilities of enhancing information protection. It should be noted, though, that insufficient attention is given to the impact of cyberattacks on the financial sector and their subsequent effect on the country's economic security.

Efremova K. (2023) and Krupianyk A. (2023) explore the connection between economic security and digitalization, focusing on the influence of digital technologies on modern economic development. The study identifies cyber threats that necessitate assessment and analysis, along with the establishment of measures to mitigate their impact on Ukraine's economic security. It is noted that the current system of indicators for assessing security levels and the set of factors threatening the stability and development of economic security require substantial revision.

The author acknowledges the need to review cybersecurity indicators and identify opportunities for implementing digital technologies at various management levels. However, it is considered appropriate to further explore this research specifically in the context of assessing the impact of cyber threats on the financial sector, as it is particularly vulnerable to various types of hacker attacks today.

Garkavenko V., Grinko I. (2021) and Shkolnyk I., Frolov S., Orlov V., Datsenko V., Kozmenko Y. (2023) identified the key trends in financial technologies (fintech), including crypto-ecosystems, NFTs, and cybersecurity. They highlighted that the growing number of digital transactions is expected to lead to an increase in cyberattacks and ransomware. The authors demonstrated that cybersecurity has become a focal point for investors, particularly corporate ones, and that B2B services within fintech subsectors are gaining popularity. They also predicted a rise in partnerships between large financial and technology companies.

The proposed forecast for the development of the fintech sector and the key trends in financial technologies are noteworthy. However, it lacks details on the use of digital technologies for providing cybersecurity within financial institutions, and trends in cybersecurity systems to combat hacker attacks are not addressed.

Mehed A., Varnalii Z. (2021) state that the digital transformation process leads to the formation of a new structure characterized by new business process formats, digital products, and digital markets. This shift necessitates a reevaluation of approaches to enterprise security and the adaptation of the financial security mechanism to meet the demands of the digital environment. The authors developed a financial security mechanism for enterprises in the digital economy, consisting of a set of interrelated principles, tasks, and methods aimed at influencing the development of management decisions.

The financial security mechanism proposed by the authors in the digital economy concerns entrepreneurship and does not highlight the possibility of financial institutions applying this mechanism.

Some authors (Bochko O., Pihotska O., 2023) suggest the application of digital technologies in financial monitoring to enhance cybersecurity levels. According to the authors, digital systems can identify and prevent fraud and other financial threats, while digital solutions improve access to financial information for stakeholders, thereby increasing transparency and fostering trust in the enterprise's financial activities.

The authors' opinion regarding the importance of using digital technologies in financial monitoring to enhance cybersecurity is shared. However, it should be noted that this approach is proposed for application at the level of a private enterprise rather than a financial institution. As a result, some of the proposed measures may not be applicable, as the operational specifics of banking institutions differ significantly from those of private enterprises.

Korol M., Parlag S. (2020) conducted a thorough analysis of the impact of digitalisation on the development of Ukraine's banking system, considering existing financial technologies and implemented functional and process innovations. The authors note that many Ukrainian banking institutions tend to focus on dealing with the consequences of cybercrimes

DOI: 10.55643/fcaptp.4.63.2025.4790

rather than investing in measures to protect clients' data and accounts. Additionally, some banks attempt to conceal existing cybercrimes to preserve client trust.

The conclusions of the study conducted by the authors are agreed with; however, the study lacks a classification of cyber threats and does not address the impact of digitalization on the financial sector's economic security.

Some authors (Teslyuk S., Matviychuk N., Levchuk A., 2024) and (Kopylyuk O., Zhyhar N., Petrynyak A., 2024) suggest evaluating the indicators of financial security in banking activities under the influence of digitalization by analyzing their innovative practices. The authors highlight leading banks that are implementing various types of innovative technologies, identify the main threats to the functioning of financial institutions, and propose a range of measures aimed at enhancing the integration of new technologies in banks while ensuring their financial security.

The authors' approach is agreed with; however, it is considered appropriate to emphasize the risks and threats that impact the management of information security within a banking institution, as well as the need to consider the effect of the sustainable functioning of the financial sector on the economic security of the country.

The authors (Balkan B., 2021; Doran N., Bădîrcea R., Manta A., 2022) suggest that open banking, which allows data sharing via Application Programming Interfaces (APIs), has enabled Fintech companies to develop innovative financial services. They also describe how banks may need to adjust their products, business processes, services, and organizational structures to stay aligned with the ongoing digital transformation.

Their position that banks have adapted to mobile technology and that significant development is the establishment of digital banks providing direct digital financial services is agreed with. However, the study does not explore how cyberattacks affect online banking.

AIMS AND OBJECTIVES

This study focuses on financial institutions, which are crucial to the functioning and stability of a nation's economic system. These institutions facilitate essential processes, including money circulation, lending, investing, saving, and the execution of daily transactions for both individuals and businesses. As such, the effective operation of the financial sector is essential for fostering economic activity, ensuring social stability, and maintaining public trust in governmental institutions. Cyberattacks on financial institutions pose significant risks, with the potential for wide-ranging adverse consequences. Such attacks can result in account blockages, disruptions of transaction operations, and breaches of confidential information. Consequently, these incidents may undermine client trust and harm the reputation of businesses. Small and medium-sized enterprises are particularly at risk, as they may incur financial losses from the temporary unavailability of financial services, which in turn can negatively influence the overall economic environment. This issue becomes increasingly pertinent during periods of martial law, when the frequency of coordinated attacks on critical infrastructure tends to rise. Notably, Ukraine has experienced numerous large-scale cyber incidents that have led to temporary disruptions in banking services and restricted access to payment systems, resulting in financial setbacks for the population.

This study aims to examine how digitalization affects the economic security of financial institutions amid growing cyber threats by identifying key risk factors, evaluating vulnerabilities within institutions, and proposing a strategic framework to strengthen cybersecurity and economic stability in a digital world. This has led to the formulation of the following research tasks:

1. To identify the various cyber threats affecting the operations of financial institutions.
2. To examine the management system for the economic and information security of financial institutions.
3. To evaluate the impact of digitalization on the financial sector and identify digital tools that can help banking institutions proactively mitigate cyber threats.
4. To propose a multifactorial predictive model for assessing the level of information and economic security of a financial institution.

METHODS

The theoretical study employs various methods to analyze digitalization's impact on financial institutions' economic security amid increasing cyber threats. The primary research methods include the transition from the abstract to the concrete, the

axiomatic method, analysis, synthesis, logical-semantic and system-analytical approaches, as well as scientific abstraction and formalization.

Specifically, the logical-semantic method was applied to clarify the conceptual and categorical framework, enhancing the understanding of key terms and concepts related to financial institutions' digital transformation and information security. System analysis was used to examine the regulatory framework and relevant scientific literature concerning the digital optimization of financial security.

The bottom-up methodology, moving from abstract to concrete, facilitated the formulation of theoretical definitions and the structuring of concepts, helping to identify key categories and draw conclusions from the research. Formalization was employed to systematize the principles, functions, tasks, and priorities involved in implementing digital technologies within the economic security framework of financial institutions.

The specific methodology for the empirical part of the study can be outlined in the following steps:

1. Analysis of the number and types of cyber threats affecting the operations of financial institutions.
2. Identification and proposal of measures to counter the most critical vulnerabilities inherent in financial institutions.
3. Development of a risk assessment model based on existing threats and the security levels of digital systems within financial institutions.

It is important to note that due to limited access to official and reliable data, empirically verifying the theoretical conclusions is challenging. However, the study's theoretical foundation remains crucial for the further development of practical recommendations aimed at enhancing cybersecurity within financial institutions in the context of digitalization.

RESULTS

Of course, it is necessary to note the positive developments in the level of the banking system's digitalization during the war. Thus, the National Bank of Ukraine (NBU) is actively implementing a digital transformation strategy to increase the banking system's security based on close cooperation with the Ministry of Digital Transformation. The interaction of these structures is aimed at making financial services more accessible through online services even during crises, ensuring the uninterrupted functioning of financial institutions and constant access of consumers to services during the war, thanks to online payment systems and digital identification documents through the application "Diya" (NBU).

It should be noted that in Ukraine the Cabinet of Ministers of Ukraine issued Resolution No. 1295 on December 23, 2020, titled "Some Issues of Ensuring the Functioning of the System for Identifying Vulnerabilities and Responding to Cyber Incidents and Cyberattacks" and designated the State Cyber Defence Centre under the State Service for Special Communications and Information Protection (SCPC) as responsible for overseeing the functioning of the system to identify vulnerabilities and respond to cyber incidents and cyberattacks. Additionally, several services are operational to address cybersecurity concerns:

1. Governmental Computer Emergency Response Team (CERT-UA) operating under the State Special Communications Administration, CERT-UA plays a critical role in responding to cyber incidents.
2. National SBU Platform MISP-UA (Malware Information Sharing Platform - Ukrainian Advantage) facilitates the exchange of information on cybersecurity threats, supporting collaboration among various stakeholders.
3. The Cyber Defence Centre (CSIRT-NBU) is tasked with collecting and analyzing cyber incidents reported by banks and non-banking entities, ensuring swift and coordinated responses to mitigate the effects of cyberattacks. These institutions and frameworks are essential to maintaining the cybersecurity of financial institutions, which in turn safeguards the overall economic stability of Ukraine.
4. State-owned banks, such as Oschadbank and PrivatBank, are actively developing their digital platforms, switching to cloud technologies and modernizing IT infrastructure, which helps financial institutions quickly respond to new threats and ensure uninterrupted services.

It is worth noting that, according to the International E-Government Development Index (EGDI) ranking, which is compiled annually by the UN, Ukraine has recently shown stable positive trends in this index. As of the 2022 results, Ukraine was categorized among countries with a high level of e-government development, with metrics exceeding the world average. In particular, the country has significantly improved its standing due to the implementation of innovative state digital platforms, such as "Diya, " which simplifies access to services for citizens and businesses. In 2024, Ukraine achieved

DOI: 10.55643/fcaptp.4.63.2025.4790

another breakthrough in the EGDI ranking, placing fifth in the world for the development of digital public services. This ranking surpasses the average European indicator, reflecting the active growth of electronic infrastructure, improvement of digital services, and strengthening of cybersecurity. Key factors contributing to this growth include the integration of new electronic services, an increase in the number of users on digital platforms, and the proactive government policy supporting digitalization across all levels of government (Figure 1).

The above shows that digitalization is not only an important tool for ensuring the stable functioning of financial institutions under the influence of various challenges and threats, but also acts as a critical factor in ensuring the country's economic security during the war.

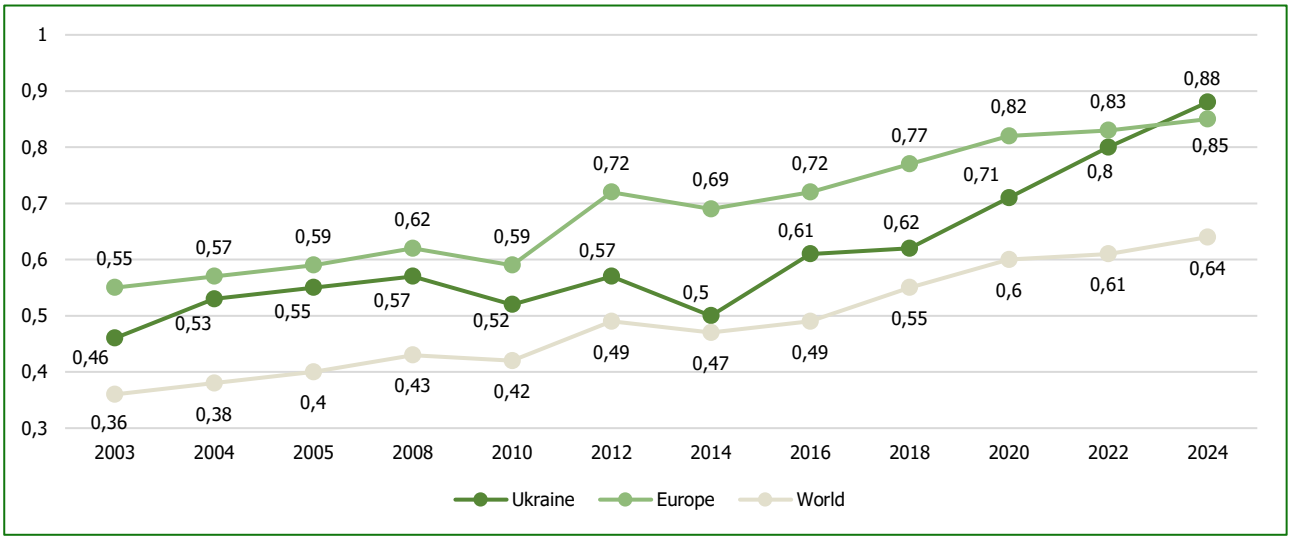

Figure 1. Analysis of the dynamics of the digital level of e-government and citizen engagement through e-services in Ukraine and globally. *(Source: prepared based on the results of a UN study)*

To confirm the hypothesis regarding the rapid digitalization of the financial sector within the national economy, the study presents the dynamics of transactions in the Electronic Payment System (EPS) of the National Bank of Ukraine and performs a trend analysis (Figure 2).

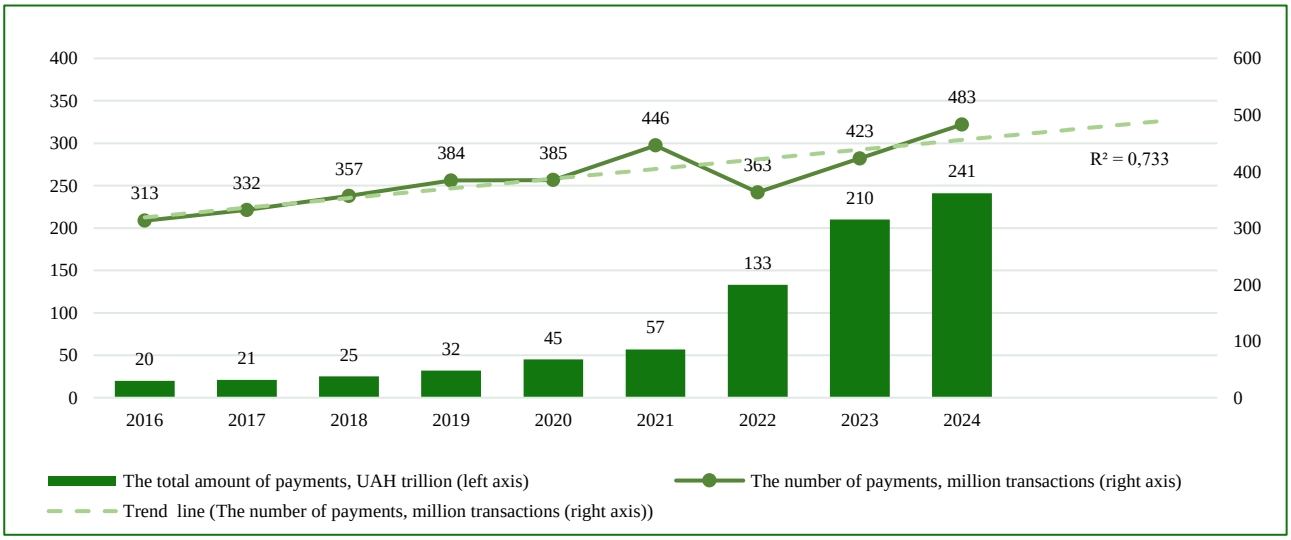

Figure 2. Trend analysis of indicators of the electronic payment system (EPS) of the National Bank of Ukraine. *(Source: prepared based on NBU data)*

The dynamics of the volume and number of payments in the SEP from 2016 to 2024 show a consistent upward trend, reflecting the ongoing digitalization of the financial sector. Since 2016, the total amount of electronic payments in Ukraine has risen from UAH 20 trillion to UAH 241 trillion by 2024. This increase indicates a significant expansion in the volume of payment transactions, driven by the integration of new technologies and a surge in the number of digital transactions.

The rate of change in quantitative indicators of the electronic payment system in Ukraine, which can serve as a key indicator of the digitalization of the financial sector, is accelerating according to a polynomial function (formula 1), taking into account the global trend of accelerated growth in the level of digitalization:

$$y = 0{,}0032x^2 + 17{,}084x + 301{,}81 \quad (1)$$

The R^2 value of 0.733 indicates that the model effectively captures the current trend and supports reasonably reliable short-term forecasts within that trend, as most of the variation in the data can be explained. As illustrated in Figure 2, the number of electronic payments is expected to continue increasing in 2025 and 2026. This growth can be attributed to the successful digitalization of financial processes, the effective implementation of innovations in payment infrastructure, and the rise of cashless transactions. This presents new challenges for ensuring the economic security of financial institutions, as they must maintain a high level of cybersecurity while processing large volumes of data and financial transactions. Vulnerabilities arising from inadequate cybersecurity measures or technological failures could pose significant threats to the economic security of these institutions.

The evolution of payment systems demands that financial institutions invest not only in technological infrastructure but also in ongoing improvements to cybersecurity measures. This ensures safe and effective operations amidst the digitalization of the economy, especially considering the significant rise in cyber incidents in 2022 following the onset of Russia's full-scale war against Ukraine (Figure 3).

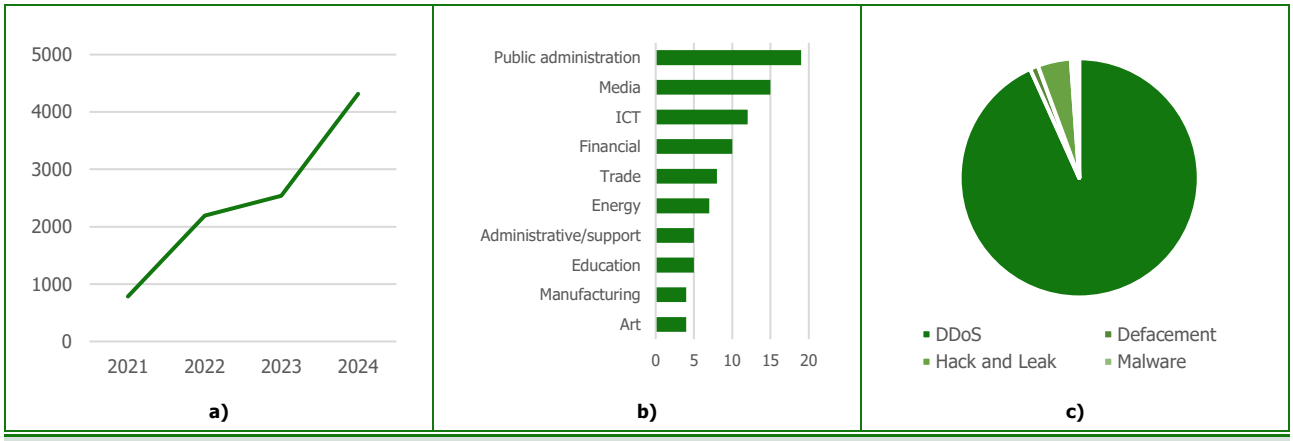

Figure 3. Cyber incident rates in the financial sector of Ukraine. Note: a) Registered cyber incidents; b) Top 10 Sectors Targeted; c) Types of attacks have been documented against the financial sector. *(Source: prepared based on data from the State Service for Special Communications and Information Protection of Ukraine and the Cyber Peace Institute)*

These trends highlight the importance of financial institutions adapting to the new realities of digital transformation, where increased transaction volumes are accompanied by a rise in cyber threats, which can significantly impact their economic security (Onyshchenko et al., 2023).

In the process of digitalizing financial institutions in the country, it is essential to focus on risks such as fraud and cyber threats. Enhancing the cybersecurity of the critical infrastructure within the banking system is of utmost importance. According to CERT-UA, various sectors have been targeted by cyberattacks: the energy sector experienced 92 attacks, the telecom 81, the educational institutions 38, the transport 32, the financial sector 30, and the IT sector 25. Typically, hacker attacks originate from domains registered in countries like China, Taiwan, South Korea, India, Mexico, and Brazil. The number of attacks on the financial sector continues to rise each year. Failures and disruptions in banking services usually have two main causes:

1. External: attacks targeting the infrastructure of a financial institution.
2. Internal: technical failures within the bank itself, without external interference.

Cybercriminals employ a variety of methods to gain unauthorized access to government, public, and corporate networks and systems, steal user credentials, obtain confidential information, and block transactions. In recent years, the following types of cyberattacks have become increasingly common:

1. Phishing attacks.
2. Malicious software (MS) attacks.

DOI: 10.55643/fcaptp.4.63.2025.4790

3. Exploitation of vulnerabilities.
4. DDoS attacks (Figure 4).

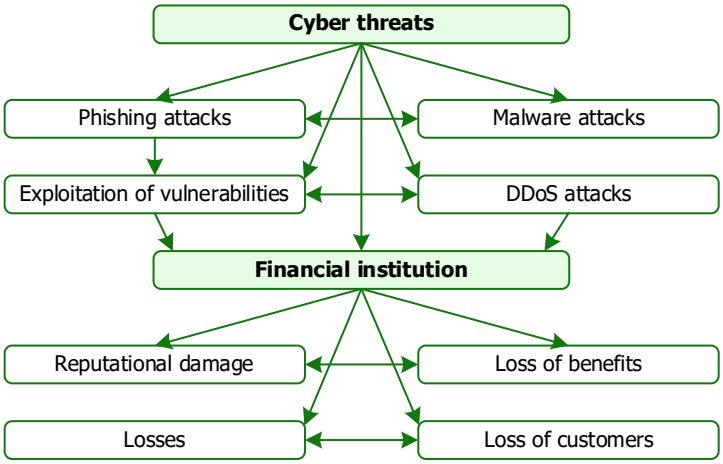

Figure 4. Types of cyberattacks carried out on financial institutions. *(Source: prepared based on Onyshchenko et al., 2023)*

Phishing attacks are the most prevalent form of cybercrime. As of 2023, approximately 3.4 billion phishing emails are sent daily from compromised email accounts, and around 200,000 phishing websites are created every day. Phishing attempts are often disguised as emails from corporate, business, financial entities, or even Microsoft. Since 2021, LinkedIn has emerged as the primary platform for phishing attacks, accounting for 52% of detected incidents, followed by Facebook with 20% and Twitter with 9%.

It is important to note that 43% of employees do not pay adequate attention to cybersecurity measures during their work, particularly new employees and those whose roles involve frequent email communication and the processing of large volumes of information. Analyzing recent cyberattacks, it can be concluded that financial institutions continue to be the most attractive targets for phishing attacks. Phishing is not only affecting bank clients, who are at risk of having their account data disclosed, but also employees of financial institutions. These employees are often targeted with deceptive content posing as communications from Ukrainian authorities or special services. Frequently, attachments in such emails contain malicious software designed to capture passwords and other sensitive data stored on bank servers. Cybercriminals persist in attacking financial institutions with various malicious programs and viruses, which can cause significant damage to the banks' infrastructure and result in disruptions or complete failures of their online services.

In 2023, CSIRT-NBU identified and initiated the blocking of approximately 41,233 phishing resources (compared to 5,710 in 2022) related to financial fraud. These phishing sites were designed to mimic government portals such as the Cabinet of Ministers of Ukraine, Diya, eDopomoga, EPilga, EVyplata, humanitarian aid portals, Ukrposhta, OLX, and Nova Poshta, and used the identities and logos of Ukrainian banks and payment services. To distribute phishing messages, attackers actively exploited networks and messaging platforms (Facebook, Telegram, Instagram, Viber), utilizing channels, bots, and groups. According to the analysis of trending fraudulent campaigns in 2023, the phishing domain filtering system (Protective DNS) recorded nearly 18.5 million clicks on phishing links and successfully redirected about two million requests from Ukrainian citizens to secure landing pages to prevent further exposure to these fraudulent resources.

Malware attacks are prevalent at all levels and target various institutions. In 2023, approximately 300,000 new malware samples were detected globally. Attackers typically target systems 95% of the time via email, along with websites and EXE files. In 2023, CSIRT-NBU detected and analyzed around 14,925 malware samples (up from 11,280 in 2022) and promptly informed Ukrainian banks about detected cybersecurity incidents, as well as recorded attempts at cyberattacks. Additionally, around 116 reports on cyber incidents and cyber threat indicators were submitted to the "Malware Information Sharing Platform & Threat Sharing" (MISP-NBU), a platform actively used by banks for information exchange on current cyber threats.

The presence of a wide variety of applications installed on computers serves as a key factor for attackers to exploit vulnerabilities in these applications. These weaknesses provide opportunities for cybercriminals to gain unauthorized access to an organization's computer systems and assets, leading to significant losses and potential long-term negative consequences. According to the CISA vulnerability catalog, the most dangerous vulnerabilities for financial institutions can be identified, and strategies to counter their negative effects can be proposed (Table 1).

Table 1. The most dangerous vulnerabilities for financial institutions and ways to counteract negative impacts. *(Source: prepared based on CyberPeace Institute (2022-2023), Cyble (2023), Cloudflare (2023), Microsoft (2022), SecurityWeek (2023), Securonix (2023), SocRadar (2023), Zyxel (2023))*

Vulnerability	Essence and content	Impact on the activities of a financial institution	Countermeasure recommendations
F5 BIG-IP	CVE-2023-46747 is a critical vulnerability that poses a serious threat because it allows attackers to execute remote code (RCE) without authentication, gaining full administrative access to the system via the Traffic Management User Interface (TMUI).	▪ Attackers can access sensitive data or manipulate system files. ▪ Attackers can download malware that will affect the operation of critical systems of a financial institution. ▪ The attack can cause network disruptions or denial of service (DoS).	It is recommended to always install relevant security updates to reduce risks.
Log4shell	CVE-2021-44228, also known as Log4Shell, is a critical vulnerability that allows attackers to execute remote code (RCE) on a server through Log4j by simply sending malicious logging data. The impact of Log4Shell on financial institutions is especially severe due to the potential for significant loss of customer trust and substantial financial losses from possible attacks. The vulnerability opens the door for cybercriminals to exploit affected systems, leading to data breaches, service disruptions, and long-term damage to the reputation of financial institutions.	▪ Attackers could exploit this vulnerability to gain access to financial system servers, potentially leading to the theft of sensitive data such as bank accounts or personal customer information. ▪ Cybercriminals could inject ransomware or other malicious software into the system, which could block access to critical infrastructure, paralyzing financial transactions and causing substantial financial losses. ▪ The vulnerability could also be exploited to modify or forge transactions in systems where Log4j is responsible for logging financial activities, allowing attackers to alter transaction records and commit fraud.	Immediately update your version of Log4j to the latest patches released by Apache that address this vulnerability. Monitor traffic and implement intrusion detection systems (IDS) to detect anomalous activity related to Log4Shell. Train staff on security to avoid situations where attackers can infiltrate the system through phishing or other social engineering attacks.
Libwebp	CVE-2023-4863 is a critical vulnerability that allows attackers to use maliciously crafted WebP files to execute remote code (RCE), which can be used to compromise systems, including through browsers or other applications that support WebP.	▪ An attacker can gain access to critical systems of a financial institution using infected image files, which can lead to the leakage or modification of confidential information. ▪ The vulnerability can be used to compromise customer systems, for example, through browsers or mobile applications that support WebP, which is especially dangerous if the bank uses applications that allow downloading or viewing images. ▪ Vulnerable systems can be subjected to DoS attacks, which can lead to disruptions in the operation of important services and financial transactions.	Financial institutions are advised to immediately update all systems that use the libwebp library to the latest version (1.3.2 and above) to reduce the risks of attack.
Zyxel RCE Vulnerability	CVE-2024-7261 is a critical vulnerability and can be exploited even without authentication, via a specially crafted cookie request sent to the vulnerable device.	▪ Exploiting this flaw can lead to unauthorized access to internal networks, data breaches, or the installation of malware, such as ransomware or botnets, which can disrupt operations or expose customer information. Attacks exploiting this vulnerability can compromise the confidentiality, integrity, and availability of financial services, leading to regulatory fines, reputational damage, and financial losses.	To protect themselves, users should regularly check for updates and apply recommended patches from Zyxel.
ProxyNotShell	CVE-2022-41040 and CVE-2022-41082 are critical vulnerabilities that allow attackers to perform remote code execution (RCE) via Exchange servers. One of the main issues with ProxyNotShell is the ability to exploit these vulnerabilities to inject malicious code via a webshell (a small server script that allows one to take control of the system) after gaining access to an Exchange user account.	▪ Many financial institutions use Exchange to manage email, and attackers could infiltrate the network and gain access to user accounts, potentially stealing sensitive information and distributing malware. ▪ Successful attacks could cripple an institution's email infrastructure, making it difficult for employees to work and disrupting critical communications. ▪ If a financial institution interacts with partners who use vulnerable Exchange servers, there is a risk that attackers could gain access to the network through these partner systems.	It is recommended to update systems and apply all necessary patches.
Atlassian Confluence RCE Flaw	CVE-2023-22527 is a critical vulnerability because it allows remote code execution (RCE) through improper data handling in OGNL (Object-Graph Navigation Language) template queries.	▪ Can give attackers access to corporate systems and confidential information, which is critical for financial institutions, as it can lead to the leakage of personal customer data or corporate secrets. ▪ Remote code execution can be used to install malware that can paralyze financial systems or use the server for unauthorized activities, such as cryptojacking - illegal mining of cryptocurrencies.	It is recommended to immediately update Confluence to the latest version or install patches for vulnerable versions. It is also important to conduct regular security audits and implement proper network segmentation to minimize potential exposure.
Microsoft Office Bug	CVE-2022-30190 is a critical vulnerability as it allows attackers to execute remote code by opening infected documents. Specifically, the attack uses the Microsoft Support Diagnostic Tool (MSDT), which is invoked via a malicious Office document, such as Word or Excel, allowing PowerShell commands to be executed without the need for macros or additional user intervention.	▪ Attackers can gain access to confidential information by downloading malware via open documents, potentially leaking sensitive information. ▪ Can target employees of financial institutions. This makes the organization vulnerable to hacking, especially if employees carelessly open suspicious documents.	Immediately install all the latest updates from Microsoft that address this vulnerability. Educate employees to be cautious with suspicious emails and attachments. Disable MSDT or implement additional security measures, such as restricting the use of PowerShell in the corporate environment.

Most attacks are carried out by hacktivists and criminal groups, including pro-russian hackers. In June 2023, the group NoName057(16) openly threatened attacks on Ukrainian banks, which led to several significant incidents. These attacks are aimed at undermining trust in financial institutions and causing disruption in the economy.

DOI: 10.55643/fcaptp.4.63.2025.4790

DDoS attacks not only disrupt services but can also serve as a cover for other malicious activities, such as data theft or cyber espionage. Ukrainian financial institutions are continually strengthening their cyber defence strategies to counter these growing threats, but the volume of attacks continues to escalate. This trend is corroborated by reports from leading cybersecurity firms like Akamai and FS-ISAC, which highlighted that the financial services sector was the most targeted in 2023.

The forecast for 2025 regarding cyber threats to financial institutions in Ukraine predicts a significant rise in cyberattacks across various fronts:

- the number of cyberattacks is expected to rise by 15%, with attacks targeting the theft of confidential data increasing by 18%;
- new vulnerabilities are anticipated, accompanied by the emergence of criminal groups that will leverage ransomware to attack financial institutions;
- the use of artificial intelligence (AI) will make phishing attacks more sophisticated, personalized, and difficult to detect. Email, social media platforms, and SaaS services will be the primary channels for these attacks;
- given the unstable geopolitical situation, an increase in DDoS attacks is expected, potentially leading to the shutdown of key financial and other institutions;
- cloud resources, artificial intelligence, and cryptocurrencies will become increasingly attractive targets for cybercriminals;
- both cybercriminals and financial organizations will use AI to develop more advanced methods of attack and enhance cybersecurity measures;
- financial institutions must focus not only on securing their systems but also on addressing vulnerabilities within their supply chains and third-party networks.

Virtual space will continue to be a battleground for ongoing threats, making the security and resilience of systems a top priority. To mitigate these risks, relevant state bodies have been established to ensure information security for financial institutions, given their critical role in the economic security of the country. All state bodies continually monitor cyber incidents and assess their impact on various sectors of the economy. While the model used for evaluating such impacts is comprehensive and general, it does not differentiate by specific types of economic activities. Nevertheless, it is essential to emphasize that a robust mechanism for countering cyber threats must be developed at every level, involving cooperation among all relevant stakeholders. This is crucial to ensure economic security not only within financial institutions but also across government entities, public organizations, and the citizens of the country.

In this context, an algorithm can be proposed for the strategic management of the digitalization process within financial institutions. This algorithm is designed to enhance the economic security of these institutions while addressing the needs of all stakeholders involved in the process (Figure 5).

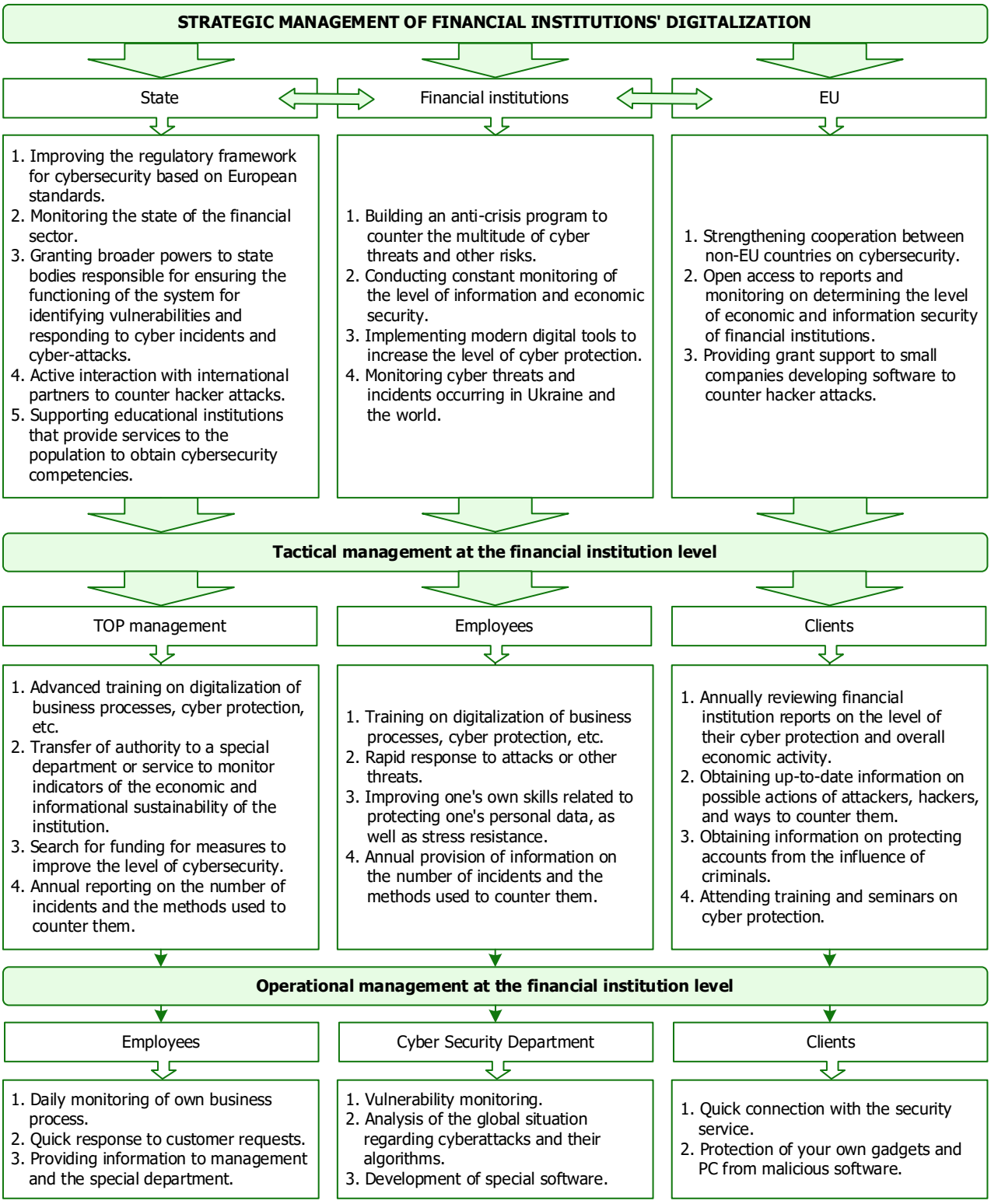

Figure 5. An algorithm for strategic management of financial institutions' digitalization to increase the level of information and economic security.

Proposed algorithm for strategic management of financial institutions' digitalization to increase the level of its security and unite economic and informational vectors of the institution's functioning. It should be clear that these two areas should be considered together since ensuring information security is not possible without the use of economic and financial incentives, which is why the authors proposed a comprehensive approach to understanding the relationship between economic and information security of financial institutions. All management decisions and actions should be directed towards these

DOI: 10.55643/fcaptp.4.63.2025.4790

two areas of security since the combination of various indicators of the financial system's stability will give a more complete picture of the state and prospects for the development of a financial institution.

The proposed algorithm can serve as a strategic tool for top management to refine existing business strategies, as well as tactical and operational plans. To effectively digitalize business processes, it is essential to first identify the most frequent types of cyberattacks, as well as the primary targets of these attacks.

In practice, the emergence of cyber threats and negative outcomes is often influenced by subjective factors. For example, insufficient employee qualifications or their neglect of cybersecurity protocols can lead to significant losses at the institutional level. Similarly, clients who inadvertently respond to cybercriminals or provide access to sensitive information (such as account or card details) can also contribute to financial losses and other adverse situations.

Unfortunately, due to martial law in Ukraine, there is no open access to the indicators of the financial institutions' activities related to their level of cyber protection. However, it is worth noting that the activities of the financial sector are constantly monitored by the National Bank of Ukraine and various state institutions and produced (Kornyliuk R., 2018) a bank stability rating, which is conducted quarterly based on rating indicators from one to ten. The key indicators are:

- stress resistance (dependence on deposits of individuals, quality of funding, profitability, liquidity, capital adequacy, scale of the bank's activities);
- depositor loyalty (bank's share in the retail deposit market, absolute growth of the retail deposit portfolio per quarter, relative growth of the retail deposit portfolio per quarter, experience in the market, payment reputation of the bank);
- analysts' assessment;
- place in the ranking of deposits of individuals.

At the moment, the following banks have the highest stability rating (TOP-10 banks): Ukr-Sibbank, Credit Agricole Bank, Raiffeisen Bank, Kredobank, OTP Bank, Privatbank, The First Ukrainian International Bank, Procredit Bank, Oschadbank, and Universal Bank (Figure 6).

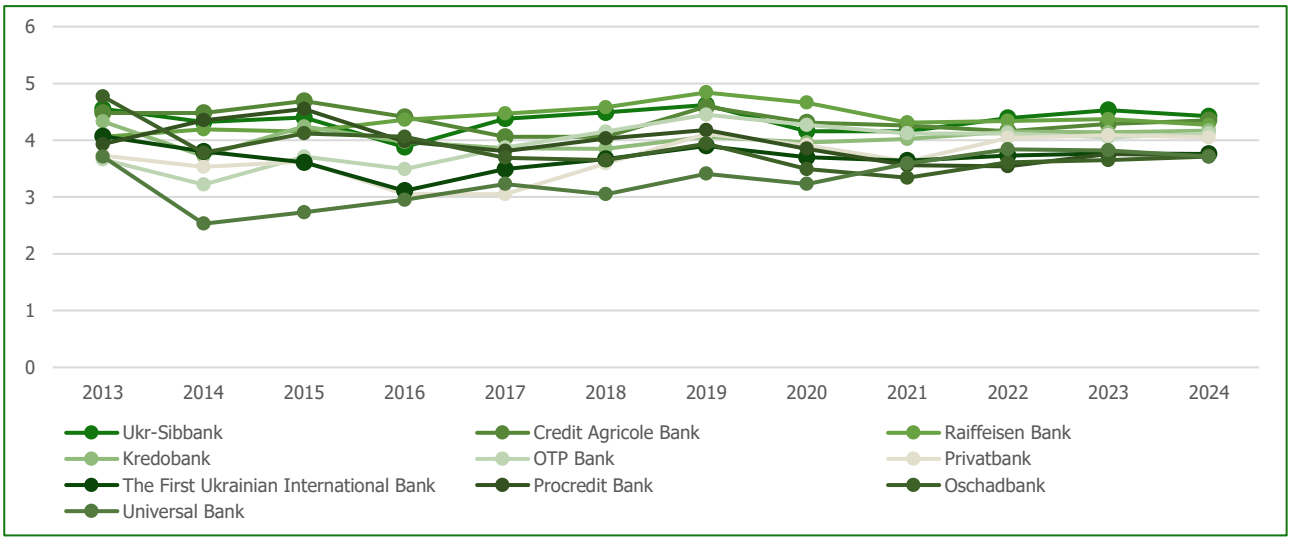

Figure 6. Dynamics of the Ukrainian bank's stability rating for 2013-2024. *(Source: prepared based on Kornyliuk, 2018; NBU, 2024)*

The proposed approach to determining the stability of banks helps to determine the level of its security, analyze the dynamics of activity, and expectations from customers. However, it is designed only for banking institutions and does not take into account the cyber protection component. The prospects for further research and improvement of existing methodologies are the development of an approach to assessing the stability, information, and economic security of all financial institutions, i.e., not only banks but also credit unions, pawnshops, leasing, and insurance companies.

To address this, the development of a multifactor predictive model aimed at identifying the key indicators that most significantly affect the economic security of a financial institution in the context of digitalization (Table 2). The model would incorporate both internal factors (those controllable by the institution itself) and external factors (such as external risks and threats). By employing statistical and machine learning techniques, the model can analyze these data points and provide predictions regarding the level of information and economic security, helping to mitigate risks proactively.

A predictive model may include the following steps:

1. Data collection and processing (collect historical data on the number of incidents, attacks, and other parameters, use logging and data from security monitoring systems).
2. Forecasting model selection – regression methods, such as linear regression or logistic regression, can be used to build the model.
3. Risk and probability assessment involve setting weightings for each factor to calculate the integrated risk. The model may use probabilistic methods, such as Bayesian networks, to predict the probability of specific threats.
4. Model validation and testing – it is recommended to perform cross-validation and evaluate the accuracy of predictions based on past data. The model should be constantly updated with new data to reflect current threats (Komelina O., Kharchenko Y., 2023).

Table 2. Key factors for building a predictive model of the financial institution's level of economic security in the context of digitalization. *(Source: prepared based on CyberPeace Institute (2022-2023), Cyble (2023), Cloudflare (2023), Microsoft (2022), SecurityWeek (2023), Securonix (2023), SocRadar (2023), Zyxel (2023))*

Parameters	Indicators
Technical parameters	Number and types of vulnerabilities in systems (both internal and external). Level of security tools implementation (firewalls, intrusion detection systems, antivirus programs, encryption systems). Number and complexity of security patches and updates. Availability of a disaster recovery plan.
Behavioural factors	Employee cybersecurity training and behaviour (frequency of phishing tests, response to threats). Number of internal security incidents (e.g., data leaks or configuration errors).
External threats	Number of external attacks on the institution, including DDoS, phishing, and ransomware attacks. Geopolitical situation. Threat vector analysis (for example, through Threat Intelligence systems that indicate future possible attacks).
Compliance and regulatory framework	Institution's compliance with regulatory requirements and security standards (e.g., ISO 27001, GDPR, PCI DSS). Security audits and the number of findings that were remediated.
Cyber resilience and incident preparedness	Incident response time (Mean Time to Detect – MTTD, Mean Time to Respond – MTTR). Availability of backup systems and mechanisms for recovery after attacks.

The authors propose the following initial indicators of the model:

1. Security index (for example, a scale from 0 to 100).
2. Forecasted number of incidents for the next period (year, quarter).
3. Probability of successful attack by certain threat vectors (DDoS, phishing, etc.).
4. Estimation of financial losses in case of data leakage or stoppage of operations due to attacks.

Such a model will allow financial institutions to assess risks in advance and take appropriate measures to improve the protection of their systems.

A multifactor model for predicting the level of a financial institution's information security can be written as an equation. Let Y be the predicted level of security (security index), and X_1, X_2, X_3, ..., X_n are variables representing various factors that affect this level (vulnerabilities, number of attacks, personnel training, etc.).

The equation can be in the form of a linear regression:

$$Y = \beta_0 + \beta_1*X_1 + \beta_2*X_2 + \beta_3*X_3 +...+ \beta_n*X_n + \varepsilon \quad (2)$$

where Y is the level of information security of the institution (for example, a scale from 0 to 100); X_1 is the number of vulnerabilities detected in security systems; X_2 is the frequency of phishing attacks; X_3 is the number of DDoS attacks; X_4 is the response time to security incidents (MTTD, MTTR); X_5 is the level of cyber resilience (for example, the presence of a recovery plan, backup systems); X_n is other factors: compliance with standards (ISO 27001, GDPR, etc.), the level of staff training, the use of the latest technologies (for example, artificial intelligence), etc.; β_0 is a constant (the basic level of security in the absence of the influence of factors); β_1, β_2, β_3,..., β_n are weighting factors for each factor, which determine how much each factor affects the level of security; ε is random noise or error, which takes into account unpredictable factors.

DOI: 10.55643/fcaptp.4.63.2025.4790

Example of an extended equation:

$$Y = 50 + 0.8*X_1 - 0.5*X_2 + 1.2*X_3 + 0.7*X_4 - 0.3*X_5 + \varepsilon \quad (3)$$

Here, the β coefficients show how much each factor affects the overall security index. For example, if the number of DDoS attacks (X_3) increases, the overall security level decreases (the coefficient can be negative).

DISCUSSION

The findings of this study underscore the increasing complexity and significant impact of cyber threats on the operations of financial institutions, particularly with regard to their informational and economic security. This type of security is essential for the sustainable growth of a nation and has a direct bearing on its overall economic stability. Our results validate the general trends identified in prior research, including the heightened frequency and sophistication of cyberattacks targeting the financial sector (e.g., Harkavenko, Grinko, 2021), and reinforce earlier conclusions regarding the financial losses associated with ransomware incidents.

However, this study advances the discourse in several significant ways. First, while previous works primarily focused on either financial metrics or general security measures, our approach integrates both informational and economic dimensions into a single predictive framework. This dual focus allows for a more comprehensive risk assessment, which has not been sufficiently addressed in earlier models. Moreover, unlike prior studies, which often relied on retrospective analysis of incidents, our proposed predictive model incorporates machine learning and multifactor analysis, enabling forward-looking diagnostics of institutional resilience.

Furthermore, the strategic management algorithm proposed in this study differs from earlier theoretical frameworks by being tailored to the conditions of hybrid warfare and digital transformation under martial law—a context largely absent in the existing literature. While some scholars (e.g., Aldasoro et al., 2022; ENISA Threat Landscape Report, 2023) acknowledge geopolitical risks, few have developed operational tools applicable in countries facing active military threats.

These distinctions suggest that the current research contributes both methodologically and contextually to the field. By bridging theoretical insights with actionable tools, this study not only complements existing knowledge but also offers practical solutions tailored to high-risk environments. It invites further empirical testing and validation in diverse institutional settings to ensure broader applicability and scalability.

Despite its contributions, the study has certain limitations. The data was primarily drawn from publicly reported cyber incidents, which may underrepresent the true scope of the problem due to underreporting by institutions. Additionally, while the proposed predictive model and management algorithm are promising, their real-world implementation has yet to be fully tested across institutions with varied digital maturity and threat exposure. Future research should aim to validate these tools under dynamic conditions and explore cross-sectoral comparisons to refine the frameworks further.

CONCLUSIONS

The study revealed that financial institutions are exposed to an evolving array of cyber threats, including ransomware, phishing, data exfiltration, and the misuse of open-source software components. In the context of hybrid warfare—particularly amid the ongoing military conflict in Ukraine—politically motivated hacktivist attacks have emerged as an additional destabilizing factor. These threats jeopardize not only financial assets but also consumer trust, posing systemic risks to financial stability. The complexity of executing such cyberattacks indicates that threat actors often possess a deep understanding of internal systems and operational protocols. Cybercriminals exploit vulnerabilities to gain unauthorized access to sensitive information. For example, a single data breach can expose thousands of customer profiles—according to IBM, the average cost of a data breach in the financial sector reached USD 5.9 million in 2023, surpassing the cross-industry average of USD 4.45 million. In Ukraine, the number of cyber incidents targeting the financial sector increased by 48% between 2021 and 2023, according to the State Service of Special Communications and Information Protection of Ukraine (SSSCIP). The more databases attackers penetrate, the more granular and profitable their stolen profiles become. The research also demonstrated that current management systems in financial institutions frequently lack integration between economic and information security domains. Addressing this gap requires coordinated governance involving both internal mechanisms and regulatory oversight. The establishment of centralized response structures such as sectoral Computer Emergency Response Teams (CERTs) is critical. These entities facilitate real-time threat sharing, strategic risk assessment,

and coordinated incident response. For example, the European Union's enforcement of the General Data Protection Regulation (GDPR) has led to over €1.6 billion in cumulative fines since 2018, underscoring the importance of compliance and robust data protection frameworks.

Digitalization, while introducing new vulnerabilities, also empowers financial institutions with innovative tools to counter cyber threats. The study highlighted the effectiveness of proactive cybersecurity measures such as automated threat detection, behavioural analytics, secure software development life cycles (SDLC), and dependency monitoring systems. These tools significantly enhance institutions' ability to detect, prevent, and respond to incidents in real time. According to IBM's 2023 Cost of a Data Breach Report, organizations that fully deploy AI-driven security tools and automation shorten breach lifecycles by an average of 108 days and reduce costs by up to USD 1.76 million per incident compared to those without automation. Behavioural analytics solutions have been shown to detect up to 90% of insider threats that would otherwise go unnoticed using traditional rule-based systems. The implementation of secure SDLC frameworks also leads to a 30–40% reduction in exploitable software vulnerabilities, according to the Open Web Application Security Project (OWASP). Moreover, dependency monitoring tools like Software Composition Analysis (SCA) can reduce open-source component risk exposure by up to 60%, improving overall software integrity. These findings underscore that digitalization, when strategically managed, can serve as both a vector of innovation and a shield against evolving cyber threats. By integrating these tools into their cybersecurity infrastructure, financial institutions can not only improve security but also reduce long-term operational and reputational risks.

The proposed multifactorial predictive model integrates technical, organizational, and regulatory factors to assess the information and economic security levels of financial institutions. This model enables dynamic vulnerability assessment and supports strategic decision-making by quantifying risks across multiple dimensions. It acts as a practical tool for early warning and prioritization of cybersecurity investments in an increasingly dynamic digital context. Financial organizations must strengthen their vulnerability management processes and prioritize safeguarding their network perimeters. It's crucial to focus on the growing risk of malware that masquerades as legitimate open-source components. Developers should closely monitor their code dependencies and thoroughly inspect third-party components for potential backdoors and vulnerabilities.

Further research is essential in the areas of hybrid warfare and ongoing military conflicts. A comprehensive investigation into the role of hacktivism in destabilizing financial systems and eroding public trust is vital. Additionally, developing predictive models to simulate the consequences of cyberattacks, along with exploring human factors that influence institutional cybersecurity, represents a critical avenue for sustained scholarly inquiry.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). Operational and cyber risks in the financial sector. SUERF – The European Money and Finance Forum. https://www.suerf.org/wp-content/uploads/2023/11/f_dda594513217fac90bbe56e5248d576c_18421_suerf.pdf
2. Balkan, B. (2021). Impacts of digitalization on banks and banking. In S. Bozkuş Kahyaoğlu (Ed.), The Impact of Artificial Intelligence on Governance, Economics and Finance, I, 49–65. https://doi.org/10.1007/978-981-33-6811-8_3
3. Barchenko, N., Lubchak, V., & Lavryk, T. (2022). Model of indicators for assessing the national level of digitalization and cybersecurity of countries around the world. Cybersecurity: education, science, technology, 18, 73–85. https://doi.org/10.28925/2663-4023.2022.18.7385
4. Blynda, Y., & Kirkach, O. (2024). The impact of digital technologies on the efficiency of public administration: The

DOI: 10.55643/fcaptp.4.63.2025.4790

experience of developed countries. Successes and Achievements in Science, 4(4).

5. Bochko, O. Yu., & Pihotska, O. M. (2023). The impact of digitalization on financial monitoring of entrepreneurial activity. Academic Visions, 23. https://www.academy-vision.org/index.php/av/article/view/816
6. Boldyrieva, L., Chaikina, A., & Ganiyev, K. (2022). Management in the construction sector using smart technologies: European experience. Lecture Notes in Civil Engineering, 181, 615–623. http://dx.doi.org/10.1007/978-3-030-85043-2_58
7. Cabinet of Ministers of Ukraine. (2020). Resolution of December 23, 2020 No. 1295 "Some issues of ensuring the functioning of the system for identifying vulnerabilities and responding to cyber incidents and cyber attacks." Cabinet of Ministers of Ukraine. https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF
8. Cloudflare. (2023). Uncovering the hidden WebP vulnerability CVE-2023-4863. Cloudflare Blog. https://blog.cloudflare.com/uncovering-the-hidden-webp-vulnerability-cve-2023-4863/
9. CyberPeace Institute. (n.d.). Cyber conflicts. CyberPeace Institute. Retrieved March 30, 2025, from https://cyberconflicts.cyberpeaceinstitute.org/
10. Cyble. (2023). Exploitation of Atlassian Confluence RCE vulnerability CVE-2023-22527. Cyble Blog. https://cyble.com/blog/exploitation-of-atlassian-confluence-rce-vulnerability-cve-2023-22527/
11. Doran, N. M., Bădîrcea, R. M., & Manta, A. G. (2022). Digitization and financial performance of banking sectors facing COVID-19 challenges in Central and Eastern European countries. *Electronics, 11*(21), 3483. https://doi.org/10.3390/electronics11213483
12. Efremova, K. V. (2023). New requirements for calculating the level of economic security of Ukraine under the influence of digitalization. In Economic security: International and national level: Collection of scientific works based on the materials of the II scientific and practical conference, April 21, 2023 (pp. 25–30). Kharkiv: Research Institute of the National Academy of Sciences of Ukraine.
13. Finitestate. (2023). Active vulnerability alert: The WebP library vulnerability CVE-2023-4863 - What you need to know. Finitestate Blog. https://finitestate.io/blog/active-vulnerability-alert-the-webp-library-vulnerability-cve-2023-4863-what-you-need-to-know
14. Garkavenko, V., & Grinko, I. (2021). The impact of digitalization on the transformation of the global financial market. Economy and Society, 33. https://doi.org/10.32782/2524-0072/2021-33-74
15. Karimov, N. G., Khamidova, F. A., Saydullaev, S. S., & Parpieva, R. A. (2022). Digital transformation of the economy as a new challenge to economic security. In Proceedings of the 5th International Conference on Future Networks and Distributed Systems (ICFNDS '21) (pp. 348–355). ACM. https://doi.org/10.1145/3508072.3508129
16. Koibichuk, V., & Kurovska, Y. (2022). The impact of integral indicators of digitalization of socio-economic transformations on the level of digital development of the country. Bulletin of Economy, 1, 83–96. https://doi.org/10.35774/visnyk2022.01.083
17. Komelina, O., & Kharchenko, Y. (2023). The formation of the bank optimal loan portfolio in the conditions of increasing business environment risks. In V. Onyshchenko, G. Mammadova, S. Sivitska, & A. Gasimov (Eds.), Proceedings of the 4th International Conference on Building Innovations (pp. 299). Springer. https://doi.org/10.1007/978-3-031-17385-1_59
18. Kopylyuk, O., Zhyhar, N., & Petrynyak, A. (2024). Threats to the financial security of Ukrainian banking institutions under the conditions of digitalization. *Economic Journal of Lesya Ukrainka Volyn National University, 2*(38), 61–68. https://doi.org/10.29038/2786-4618-2024-02-61-68
19. Kornyliuk, R., & Kornyliuk, A. (2018). Ukrainian banks' business models under systemic risk. In ICTERI (pp. 124–138). https://ceur-ws.org/Vol-2105/10000124.pdf
20. Kornylyuk, R. (2023). Main trends in the banking market during the 12 months of the war. Economic Truth. https://www.epravda.com.ua/columns/2023/03/13/697976/
21. Korol, M., & Parlag, S. (2020). The impact of digitalization on banking in Ukraine. Uzhhorod National University Repository. https://dspace.uzhnu.edu.ua/jspui/handle/lib/35064
22. Krasnobayev, V., Yanko, A., Hlushko, A., Kruk, O., Kruk, O., Gakh, V., Onyshchenko, S., Maslii, O., & Hrashchenko, I. (2023). Economic and cyber security. Medychna Knyha. https://doi.org/10.15587/978-617-7319-98-5
23. Krasnobayev, V., Yanko, A., Martynenko, A., & Kovalchuk, D. (2023, September 21–23). Method for computing exponentiation modulo the positive and negative integers. In Proceedings of XI International Scientific and Practical Conference "Information Control Systems & Technologies (ICST-2023)", 3513, 374–383). https://ceur-ws.org/Vol-3513/paper31.pdf
24. Krupianyk, A. (2023). Digital economy of Ukraine: Key development factors. VoxUkraine. https://voxukraine.org/en/digital-economy-of-ukraine-key-development-factors
25. Kudinov, O. (2022). The influence of information technologies on the socio-economic development of territorial communities. *Economics and Region, 1*(84), 82–88. http://dx.doi.org/10.32782/EiR.2022.1(84).2549
26. Maslii, O., Buriak, A., Chaikina, A., & Cherviak, A. (2025). Improving conceptual approaches to ensuring state economic security under conditions of digitalization. *Eastern-European Journal of Enterprise Technologies, 1*(13(133)), 35-45. https://doi.org/10.15587/1729-4061.2024.319256
27. Mehed, A. M., & Varnalii, Z. S. (2021). Financial security of enterprises in the digital economy. *Socio-Economic Relations in the Digital Society, 3*(42), 55–61. https://doi.org/10.18371/2221-755x3(42)2021253524

28. Microsoft. (2022). Analyzing attacks using the Exchange vulnerabilities CVE-2022-41040 and CVE-2022-41082. Microsoft Blog. https://www.microsoft.com/en-us/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/

29. Ministry of Finance. (2024, July 1). Bank ratings. https://minfin.com.ua/ua/banks/rating/?date=2024-07-01

30. National Bank of Ukraine. (n.d.). NBU ta Mintsyfry spilno pratsiuiut nad tsyfrovizatsiieiu bankivskoi systemy Ukrainy. https://bank.gov.ua/en/news/all/nbu-ta-mintsifri-spilno-pratsyuyut-nad-tsifrovizatsiyeyu-bankivskoyi-sistemi-ukrayini

31. National Coordination Center for Cybersecurity of Ukraine. (n.d.). Critical infrastructure protection. National Coordination Center for Cybersecurity of Ukraine. https://cip.gov.ua/ua

32. Onyshchenko, S. V., & Maslii, O. A. (2017). Organizational and economic mechanism of prevention of threats to budget security of Ukrainian economy. *Scientific Bulletin of Polissia, 1*(9), 176-184. https://www.webofscience.com/wos/woscc/full-record/WOS:000409454100024

33. Onyshchenko, S., Maslii, O., & Hlushko, A. (2025). Digital and economic security of the state under global threats. In Lecture Notes in Networks and Systems (Vol. 1338, pp. 580–602). Springer. https://doi.org/10.1007/978-3-031-89296-7_29

34. Onyshchenko, S., Skryl, V., Hlushko, A., & Maslii, O. (2023). Inclusive development index. In Lecture Notes in Civil Engineering. *Springer, 299,* 779–790. https://doi.org/10.1007/978-3-031-17385-1_66

35. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., & Cherviak, A. (2023). Cybersecurity and improvement of the information security system. *Journal of the Balkan Tribological Association, 29*(5), 818–835. https://www.scopus.com/record/display.uri?eid=2-s2.0-85181654278&origin=recordpage

36. Onyshchenko, V., Onyshchenko, S., Maslii, O., & Maksymenko, A. (2023). Systematization of threats to financial security of individual, society, business, and the state in terms of the pandemic. In Lecture Notes in Civil Engineering, 299, 749–760). https://doi.org/10.1007/978-3-031-17385-1_63

37. Onyshchenko, V., Yehorycheva, S., Maslii, O., & Yurkiv, N. (2022). Impact of innovation and digital technologies on the financial security of the state. *In Lecture Notes in Civil Engineering, 181,* 749–759. https://doi.org/10.1007/978-3-030-85043-2_69

38. SecurityWeek. (2023). Attackers exploiting critical F5 BIG-IP vulnerability. SecurityWeek. https://www.securityweek.com/attackers-exploiting-critical-f5-big-ip-vulnerability/

39. Securonix. (2023). ProxyNotShell revisited. Securonix Blog. https://www.securonix.com/blog/proxynotshell-revisited/

40. Shkolnyk, I., Frolov, S., Orlov, V., Datsenko, V., & Kozmenko, Y. (2022). The impact of financial digitalization on ensuring the economic security of a country at war: New measurement vectors. *Investment Management and Financial Innovations, 19*(3), 119-138. https://doi.org/10.21511/imfi.19(3).2022.11

41. SocRadar. (2023). Atlassian's Confluence Data Center and Server affected by critical RCE vulnerability CVE-2023-22527. SocRadar. https://socradar.io/atlassians-confluence-data-center-and-server-affected-by-critical-rce-vulnerability-cve-2023-22527-patch-now/

42. Svistun, L., Glushko, A., & Shtepenko, K. (2018). Organizational aspects of development projects implementation at the real estate market in Ukraine. *International Journal of Engineering & Technology, 7*(3.2), 447-452. https://doi.org/10.14419/ijet.v7i3.2.14569

43. Teslyuk, S., Matviychuk, N., & Levchuk, A. (2024). Financial security of banking institutions in the context of digitalization. Economy and Society, 60. https://doi.org/10.32782/2524-0072/2024-60-117

44. United Nations. (n.d.). Ukraine: Country information. United Nations E-Government Development Database. https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine

45. Kulyk, V. et al. (2020). Assessing overall level of enterprise's environmental security: Possibilities of applying modern economic and mathematical methods. International Multidisciplinary Scientific GeoConference: SGEM, 20 (5.2), 1–9. http://dx.doi.org/10.5593/sgem2020/5.2/s21.011

46. Yanko, A., Krasnobayev, V., Smirnov, O., & Kuznetsova, T. (2019, November 29–30). Methods of nulling numbers in the system of residual classes. In International Workshop on Conflict Management in Global Information Networks (CMiGIN 2019), Lviv, Ukraine. CEUR-WS. http://ceur-ws.org/Vol-2588/paper9.pdf

47. Yarovenko, H., Kuzior, A., Norek, T., & Lopatka, A. (2024). The future of artificial intelligence: Fear, hope or indifference? *Human Technology, 20*(3), 611–639. https://doi.org/10.14254/1795-6889.2024.20-3.10

48. Zedgenizova, I., Ignatyeva, I., Zarubaeva, E., & Teplova, D. (2021). IT opportunities: Increasing the level of financial security in digital economy. *Journal of Advanced Pharmacy Education and Research, 11*(3), 157–161. https://doi.org/10.51847/Cwojg5cIf1

49. Zhyvylo, Y., Onyshchenko, S., Cherviak, A., & Bilko, S. (2023). Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. *Eastern-European Journal of Enterprise Technologies, 5*(13(125)), 65–76. https://doi.org/10.15587/1729-4061.2023.288175

50. Zyxel. (2023). Zyxel security advisory for post-authentication RCE in firewalls. Zyxel. https://support.zyxel.eu/hc/en-us/articles/9974726608786-Zyxel-security-advisory-for-post-authentication-RCE-in-firewalls

DOI: 10.55643/fcaptp.4.63.2025.4790

Кудінова А., Маслій О., Смоквина В., Циганенко К.

ВПЛИВ ЦИФРОВІЗАЦІЇ НА ЕКОНОМІЧНУ БЕЗПЕКУ ФІНАНСОВИХ УСТАНОВ В УМОВАХ ЗРОСТАННЯ КІБЕРЗАГРОЗ

Основна мета дослідження – виявлення різноманітних кіберзагроз, які впливають на діяльність фінансових установ, зокрема на їхню інформаційну та економічну безпеку, адже вона має вирішальне значення для сталого розвитку країни та безпосередньо впливає на її економічну безпеку. Фінансовий сектор у глобальному масштабі зазнає найбільших збитків від кіберінцидентів: у середньому фінансові організації по всьому світу втрачають близько 5,9 мільйона доларів США на один інцидент, що перевищує середній показник по всіх галузях, який становить 4,45 мільйона доларів США. Збитки фінансових установ охоплюють не лише викуп за нерозголошення викрадених даних і витрати на відновлення інфраструктури після атак програм-вимагачів, а й прямі фінансові втрати в окремих випадках. У дослідженні визначено найпоширеніші типи кібератак, проаналізовано їхній вплив на функціонування фінансових установ, а також запропоновано шляхи реагування та запобігання таким інцидентам. Уперше запропоновано алгоритм стратегічного управління цифровізацією фінансових установ, який спрямований на зміцнення їхньої економічної та інформаційної безпеки. Алгоритм може бути впроваджений на всіх рівнях управління та в усі бізнес-процеси для мінімізації впливу суб'єктивних факторів ризику. Крім того, розроблено та обґрунтовано багатофакторну прогностичну модель, що є подальшим розвитком існуючих підходів до оцінювання інформаційної та економічної безпеки фінансових установ. Модель ураховує й внутрішні (контрольовані самою установою), і зовнішні (пов'язані із зовнішнім середовищем) чинники, застосовуючи статистичні методи та технології машинного навчання для аналізу даних і прогнозування рівня безпеки. З огляду на розвиток цифровізації в Україні, що триває, фінансові установи мають адаптуватися до нових викликів і впроваджувати інноваційні рішення для забезпечення свого сталого функціонування, зокрема в умовах воєнного стану.

Ключові слова: економічна безпека, кіберзагрози, інформаційна безпека, менеджмент, фінансові установи, бізнес-стратегія, цифровізація, цифрові технології

JEL Класифікація: G21, G28, O33, L86, K24, D81