DOI: 10.55643/fcaptp.2.61.2025.4672

Halyna Kryshtal
D.Sc. in Economics, Professor of the Department of Finance, Banking and Insurance, Interregional Academy of Personnel Management, Kyiv, Ukraine;
e-mail: gkryshtal@ukr.net
ORCID: 0000-0003-3420-6253
(Corresponding author)

Mariia Samofalova
PhD in Economics, Associate Professor of the Department of Management and Administration, Open International University of Human Development "Ukraine", Kyiv, Ukraine;
ORCID: 0009-0009-8060-7956

Liudmyla Sakhno
Candidate of Economy Sciences, Department of Finance, Accounting and Taxation, Dmytro Motornyi Tavria State Agrotechnological University, Zaporizhia, Ukraine;
ORCID: 0000-0003-0339-3404

Vita Fedyna
Candidate of Economy Sciences, Associate Professor of the Department of Finance, Banking and Insurance, National Academy of Statistics, Accounting and Auditing, Kyiv, Ukraine;
ORCID: 0000-0002-3916-5932

Tetiana Mokiienko
Candidate of Economy Sciences, Associate Professor of the Department of Accounting and Taxation, Poltava State Agrarian University, Poltava, Ukraine;
ORCID: 0000-0003-1344-4981

Maryna Yermolaieva
Candidate of Economy Sciences, Associate Professor of the Department of Accounting and Taxation, Poltava State Agrarian University, Poltava, Ukraine;
ORCID: 0000-0003-0469-0435

Received: 08/12/2024
Accepted: 13/03/2025
Published: 30/04/2025

CYBER RISKS IN THE FINANCIAL AND BANKING SYSTEM: ANALYSIS OF DIRECT AND SYSTEMIC LOSSES

ABSTRACT

The article focuses on the impact of cyber risks on the banking sector and the financial system, particularly in relation to the country's economic stability. The key factors contributing to the emergence of cyber threats are identified, and methods for their mitigation at the level of individual financial institutions are examined. In the course of the study, the authors considered a model based on the analysis of the direct and systemic impact of cyberattacks, taking into account the macroeconomic distribution and the application of the Leontief input-output table. This approach made it possible to create an objective picture of economic losses across all sectors of the economy, rather than solely at the enterprise level. The authors propose an approach to assessing losses through the depreciation of intangible assets and operational risks, which is crucial for accurately determining the consequences for the financial system, the banking sector, and the competitiveness of individual banks. Revenue reduction due to declining profitability and lost profits is also highlighted as critical factors that must be considered in calculations. The study emphasizes the development of international cybersecurity standards and provides recommendations for active risk management, particularly through risk avoidance, mitigation, and transfer, which are essential for the practical application of the research findings in both business and public administration. The authors demonstrate that further research in the field of cybersecurity, including the analysis of the impact of cyber risks on macroeconomic stability, forecasting the consequences of cyberattacks for GDP and financial stability, and improving cooperation mechanisms between the public and private sectors, is highly relevant. The study has practical value for the development of cybersecurity protection strategies and can be useful for policymakers, regulators, and business leaders seeking to ensure the cybersecurity of economic infrastructure.

Keywords: digitalization, cyber risks, financial system, banking system, competitiveness

JEL Classification: E50

INTRODUCTION

The modern development of the economy is characterized by the active implementation of digital technologies, the development of advanced materials, the analysis of large volumes of data, and the creation of new management systems. These changes shape new production and economic relationships, which, in turn, transform business practices and the principles of interaction between economic entities. Simultaneously, technological innovations such as Big Data, artificial intelligence, blockchain, and cloud computing significantly optimize decision-making processes, ensure access to extensive information, and create conditions for improving the efficiency of companies.

However, alongside the numerous advantages of digitalization, new threats emerge, particularly risks associated with cybersecurity, which can significantly impact economic entities. The issue of cybersecurity is especially pressing in the financial sector. Companies and organizations handling monetary transactions become prime targets for cybercriminals due to the concentration of large financial resources and sensitive customer data. The vulnerability of the financial sector is driven by the high level of interconnectivity among systems and the substantial volume of information flows. A cyberattack

targeting one financial institution can quickly spread to others through the network of interconnected financial operations, creating systemic risks for the broader economy.

A particular threat arises from outdated technological platforms, which, while still in use, often lack adequate protection. Such systems fail to meet modern cybersecurity standards, making them attractive targets for attacks. The consequences of cyberattacks can be critical: direct financial losses affect the organization's operations, while indirect losses, such as reputational damage and loss of customer trust, can lead to long-term negative effects on the business. Recovery from a cyber incident also requires significant financial and time resources, complicating business operations and potentially slowing down growth.

Addressing cyber risks and establishing appropriate defence mechanisms is of strategic importance to ensuring the resilience and reliability of the financial system. Scientific research aimed at analyzing the determinants of cyber risk management development can significantly contribute to forming effective approaches to protection against cyber threats. Modern digitalization trends require financial institutions to adapt to new realities, including identifying vulnerabilities, assessing potential threats, developing proactive protection measures, and establishing response mechanisms for potential incidents. This becomes a key factor in ensuring the sustainable development and competitiveness of not only individual institutions but also the financial system as a whole.

LITERATURE REVIEW

From an investor's perspective, cyber risks are a component of systematic risk, which is challenging to control or avoid, even through diversification. Systematic risk, also known as non-diversifiable risk, encompasses threats that affect the entire market or specific sectors. Investopedia defines it as the risk of volatility that is difficult to predict and impossible to eliminate solely by distributing assets across various investments. This risk is inherent in general market trends, driven by economic changes, global events, or technological advancements. The only approach investors can use to mitigate the impact of systematic risks is through hedging or employing instruments to protect against sudden market fluctuations.

Frederic Mishkin (Mishkin Frederic, 2007) describes systematic risk as the probability of unforeseen events that significantly impact the financial market. Such events can drastically alter market dynamics, disrupt the normal functioning of financial institutions, and complicate access to capital for investors. As a result, markets lose their ability to efficiently allocate funds to the most attractive investment opportunities. This type of risk may arise in response to political crises, economic recessions, major technological accidents, or cyber threats that destabilize financial systems.

Researchers (Cebula, 2010; Bouveret, 2018) define cyber risk as a form of operational risk related to technological and informational assets, that pose a threat to data security. Potential threats include breaches of confidentiality, integrity, and availability of information or networks, which can have severe consequences for organizations. Confidentiality refers to restricting third-party access to private or internal information, integrity ensures protection against unauthorized interference or alteration, and availability guarantees the usability of information within the daily operational processes of a financial organization.

In the context of information security management, risk is assessed as a combination of the potential consequences and the likelihood of their occurrence. The latter depends on the level of threat, system vulnerabilities, and the expected outcomes of possible compromises (Bouveret, 2018). This concept can be expressed through the formula:

$$\text{Risk} = f(\text{Threat}, \text{Vulnerability}, \text{Consequences}) \quad (1)$$

Modern financial organizations are highly sensitive to cyber risks due to numerous factors. As highlighted by Kopp E. (Kopp, 2017), cyber threats in the financial industry are significant due to cybercrime, hacktivist activity, and various manifestations of cyber espionage. Numerous vulnerabilities in the modern financial system stem from the dependence of financial institutions on integrated networks, such as payment systems, electronic communications, and international fund transfer systems (SWIFT). The consequences of cyberattacks include both direct financial losses and potential damages resulting from breaches of confidentiality and data availability, which can lead to severe reputational risks and diminished trust in financial institutions.

Protecting against cyber risks is a complex and multifaceted process, as financial losses and other consequences of compromise can not only affect an individual organization but also trigger a domino effect due to the high interconnectivity of the financial industry.

DOI: 10.55643/fcaptp.2.61.2025.4672

Previously, cybersecurity strategies in the financial sector primarily focused on protecting personal data and investor information from unauthorized access, alteration, or loss, which threatened data confidentiality, integrity, and availability. Today, while safeguarding investor data remains a priority, significant attention must also be directed toward securing the information networks and communication channels themselves. These networks support the operations of banks, investment funds, exchanges, clearing, and payment systems, and their compromise can create chaos, undermining the stability of financial markets and operations. Accordingly, cybersecurity specialists, such as representatives from the New York Department of Financial Services, warn that cyberattacks on financial infrastructure pose an existential threat to the industry by disrupting the normal functioning of financial markets and risking widespread systemic failures.

The U.S. Financial Industry Regulatory Authority (FINRA) has developed the concept of a "digital threat risk management triangle," which includes three categories of risks: endogenous, exogenous, and systemic. Endogenous risks are associated with internal factors, such as potential misuse or errors by employees, which can unintentionally or deliberately compromise data confidentiality or integrity. Exogenous risks originate outside the organization and may arise from interactions with counterparties or third-party information systems. The third component of the triangle is systemic risks, which have a global nature and impact the entire financial market. FINRA emphasizes that special attention should be paid to managing endogenous and exogenous threats, as they can have immediate and substantial effects on operational security.

Modern cyber threats also include attacks exploiting vulnerabilities in information networks critical to financial operations. As financial organizations become increasingly integrated, disruptions in the systems of one counterparty can quickly spread to others, causing significant financial losses and destabilizing markets. In this context, cybersecurity is not only about preserving data confidentiality but also a critical element in maintaining the integrity of financial infrastructure.

On the other hand, Eisenbach T. (Eisenbach, 2019) argues that cyber risk in the banking sector has fundamentally different characteristics from traditional operational risk, highlighting the specific consequences that may arise from cyber incidents. Operational risk, which includes losses due to internal failures or external factors, often triggers a "run on deposits" as trust in financial institutions declines, resulting in liquidity risk. However, cyber risk extends beyond these consequences. Disruptions to data integrity, confidentiality, and access to banking information systems can lead to much deeper and more multifaceted outcomes, including not only a loss of client trust but also the potential for critical failures in the functioning of the entire financial infrastructure.

Unlike operational risks, cyber risks threaten the very foundations of a bank's information infrastructure. According to Eisenbach, such incidents can trigger a "domino effect," where a single attack sets off a series of adverse events that impact not just an individual bank but have the potential to destabilize the financial market as a whole. For instance, if attackers gain access to confidential information, it could cause panic among the bank's clients and partners. Additionally, cyber incidents often result in the suspension of critical operations or the disruption of business processes, which may have long-term repercussions.

Moreover, cyber risk is complex, involving vulnerabilities linked to modern information technologies that evolve rapidly and require constant monitoring and updates to protective protocols. At the same time, the consequences of cyber incidents can be less predictable and harder to quantify than those of operational risks, complicating the planning of risk management measures. As Eisenbach underscores, it is crucial not only to prevent such threats but also to develop effective recovery strategies to minimize losses from potential attacks and build a transparent and resilient data protection system (Eisenbach T., 2019).

AIMS AND OBJECTIVES

The purpose of this study is to examine cyber risks in the financial and banking system, assess their impact on direct and systemic losses, and develop recommendations to minimize these risks, ensuring the stability and security of financial and banking institutions.

Objectives of the Study:

1. Analyze the key types of cyber risks faced by financial and banking institutions, such as cyberattacks, data breaches, fraudulent activities, and other threats to information systems.
2. Build an objective picture of economic losses based on a new calculation model.
3. Develop recommendations for financial and banking institutions to enhance cybersecurity through the implementation of modern technologies, staff training, and risk monitoring.

METHODS

To achieve the stated goals, the study employs a comprehensive methodological approach, incorporating several methods and analytical techniques to ensure the accuracy and depth of the obtained results:

1. **Economic and mathematical modelling of direct and systemic losses** – a method that allows for the assessment of the impact of cyber risks on the financial performance of institutions. It involves forecasting both direct losses (costs of mitigating attack consequences, fines, and compensations) and systemic consequences (loss of customer trust, reduction in asset market value). The application of this approach helps identify optimal measures to mitigate the impact of cyber risks.
2. **System analysis** – considers the financial and banking system as an interconnected structure vulnerable to cyber risks. This approach makes it possible to assess the likelihood of cascading effects that could lead to systemic losses across the entire sector and identify key areas for improving system resilience.

The application of these methods provides a comprehensive understanding of cyber risks in the financial and banking system, contributing to the development of effective mechanisms to protect against and minimize both direct and systemic losses in this area.

RESULTS

In recent years, cyber incidents have not only become more frequent but also significantly more costly, with some cases resulting in losses amounting to hundreds of millions of dollars. Cyber threats in the financial and banking sector can cause substantial financial losses for individual institutions and the economy as a whole, potentially undermining its stability.

Research in this area demonstrates the critical importance of addressing cyber risks. However, comparing results is often challenging due to differences in methodologies, assumptions, and data sources. Researchers employ various models to assess both direct losses (e.g., direct financial costs, system recovery expenses, and damage mitigation) and systemic costs (e.g., reputational damage, loss of trust in financial institutions, and heightened regulatory requirements). Many studies lack transparency in their evaluation criteria, applied mathematical models, and datasets, significantly limiting the ability to accurately compare findings.

Direct and systemic risks are interrelated concepts, yet they are not equivalent, as they differ in nature, scope of impact, and mechanisms of realization.

Direct Risks – These are risks that directly affect the operations of an individual financial or banking institution. They have clearly defined consequences, such as financial losses from a specific incident, costs associated with mitigating the effects of an attack, fines, legal dispute expenses, or customer compensation.

For example, a cyberattack on a bank leads to the leakage of customers' personal data and the costs associated with its protection.

Systemic Risks – These are risks that affect the entire financial sector or the economy as a whole and can lead to cascading effects, disrupting the stability of multiple institutions simultaneously. Such risks arise from the interconnectedness between financial institutions, markets, and economic system participants.

For example, a mass cyberattack on key banks in a country results in a crisis of trust, liquidity, and disruptions in financial flows.

In Table 1, we present the correlation between the concepts of "direct risks" and "systemic risks".

Table 1. Correlation between the Concepts of "Direct Risks" and "Systemic Risks." *(Source: constructed by the author based on Issues Examination Guidance to Banks Outlining New Targeted Cyber Security Preparedness Assessments, 2012)*

Criteria	Direct Risks	Systemic Risks
Scope of Impact	Localized, on a single institution	Global, across the entire system
Cause-and-Effect Relationship	Direct losses (financial, reputational)	Interconnected impact on other institutions
Mechanism of Occurrence	Specific attack or threat	Chain reaction, spread
Example of Consequences	Data recovery costs	Market panic, institution bankruptcies

DOI: 10.55643/fcaptp.2.61.2025.4672

Thus, we can conclude that systemic risks are not a direct equivalent of indirect risks, although there are some similarities between them. Indirect risks are the consequences that emerge in the long-term following the realization of direct risks. (For example, after a successful cyberattack, a bank may face a loss of customer trust or a decline in market value, which are indirect losses). In other words, indirect risks are secondary consequences of direct risks, which can be either localized or systemic. Systemic risks, on the other hand, extend beyond a single entity and affect the interconnected network of financial institutions, creating a domino effect. Systemic risks are large-scale and can be triggered by both direct and indirect risks.

For effective risk management, it is necessary to consider the interrelationship between direct, indirect, and systemic risks, developing comprehensive cybersecurity mechanisms.

In light of these challenges, this study proposes the development and description of a model to assess losses from cyberattacks in the context of Ukraine's economy, with a particular focus on the financial and banking sectors. This model aims to analyze the economic consequences of cyber risks not only at the level of individual institutions but also in terms of their impact on sectoral output and national GDP. The model will calculate both direct and systemic losses, assessing the economic impact through the financial institutions' direct expenses and potential market-wide consequences, such as reduced investor confidence, fluctuations in the market value of banking assets, and potential macroeconomic implications.

The model also includes sectoral components to account for the specific characteristics of each major economic sector, evaluating the potential impact of cyber risks on each sector's contribution to GDP. With a focus on the financial and banking sectors, the model will establish the relationship between direct losses from cyber incidents (e.g., infrastructure recovery costs, insurance payouts, and reduced bank profits) and their systemic consequences, which may affect related sectors of the economy. By incorporating macroeconomic factors, the model can forecast the impact of cyber incidents on economic growth, inflation, and employment levels.

The structure of the proposed model is based on the work of Dreyer, P. (Dreyer, 2018) and analysts from the RAND Corporation titled *"Estimating the Global Cost of Cyber Risk: Methodology and Examples."* This study aimed to create a universal methodology for assessing both current and projected costs of cyber risks at global, national, and sectoral levels. The methodology acknowledges the high degree of uncertainty associated with both the frequency and cost of cyber incidents. To account for this uncertainty, the model employs various types of probability distributions, including uniform, triangular, trapezoidal, generalized beta, and Delphi distributions. The Delphi distribution, derived from expert surveys, allows for adapting estimates to the specifics of the data and available expert information, thereby reducing forecasting errors.

To develop the model, the first step is to define several key structural sets that will be used to describe economic processes in the context of cyber risks. These sets are descriptive by nature and lack measurement units; however, their role in the modelling process is critical for understanding the structural organization of losses. These sets include:

1. Countries ($c \in C$) — a set of countries for which the analysis is conducted. Each country may have unique characteristics influencing the level and nature of cyber incidents, such as economic development, technological infrastructure, and political stability.
2. Industry Sectors ($i \in I$) — a set of economic sectors most vulnerable to cyber threats. These may include financial, energy, telecommunications, healthcare, and other critical industries. The selection of sectors determines how cyber risks affect production processes and the overall economic well-being of a country.
3. Economic Losses ($e \in E$) — a set of categories of economic losses resulting from cyber incidents. These losses may include direct financial damages, system recovery costs, reputational damage, litigation and compensation expenses, as well as broader economic impacts that are harder to measure, such as a decline in trust in the financial system.
4. Threats ($p \in P$) — a set of various cyber threats, such as cyberattacks, data breaches, viruses, fraud, and other threats affecting system security. The diversity of threats influences how they translate into economic losses, causing direct or systemic damages across different sectors.

These sets are mutually exclusive and collectively exhaustive, meaning each element belongs to only one of the specified classes. Together, they form a clear framework for analyzing the consequences of cyber risks at both the sectoral and national levels.

Within this model, the costs associated with cyber risks are divided into two primary categories:

1. Direct Losses (dci) — costs directly incurred by each economic sector (i) in each country (c) due to a cyber incident. These include costs for recovery from an attack, compensation for affected parties, fines, legal fees, and operational disruptions in enterprises directly impacted by the cyberattack.
2. Systemic Losses (sci) — macroeconomic consequences for other sectors arising from a cyber incident in one economic sector. Systemic losses reflect the impact on other industries through economic disruptions caused by the affected sector.

To evaluate costs, the model employs probabilistic distributions, allowing for the inclusion of uncertainty in input data. This approach enables more accurate and substantiated forecasts, as the model accounts for variability and complexity in the scenarios faced by countries and sectors. Each parameter of the model can be defined either through point estimates or using different probabilistic distributions, depending on the available data and specific conditions for a particular country or sector.

Thus, this model facilitates a detailed analysis of costs arising from cyber risks at both sectoral and national levels. It helps identify the most vulnerable areas and propose measures to enhance resilience against cyber threats.

In developing this model, the first step involves determining $\boldsymbol{wci}$, which represents the contribution share of sector i to the economy of the country c, i.e., its weight in the country's gross domestic product (GDP). This metric allows for the assessment of how much of the overall economic activity is accounted for by a particular sector. Therefore, $\boldsymbol{wci}$ is a critical indicator for understanding which sectors play a significant role in the economy and what potential economic consequences may arise from cyber threats impacting these sectors.

A simple multiplication of wci by $GDPc$ yields the added value (contribution to GDP) of sector i within the economy of the country c. This metric provides an understanding of the economic size of a sector in the economy and indicates the importance of that sector for economic growth or stability. If a specific sector is disrupted due to cyberattacks, it may lead to significant changes in economic indicators, including a slowdown in economic growth or even a recession in the event of substantial damage.

The next step in the model is defining $\boldsymbol{Oci}$, which represents the output volume of sector i in country c. This value is critical for estimating potential losses as it reflects the production volume generated by the sector and how cyber incidents might reduce these figures due to operational disruptions, production halts, or losses of goods and services caused by failures in technological infrastructure or financial systems.

The following step involves determining $\boldsymbol{Ycie}$, which denotes the share of sector i's output in country c that is at risk due to financial exposure of type (e). This parameter helps assess which portion of production capacities or economic resources in each sector may be directly exposed to risk from cyberattacks. Considering different types of financial exposures allows for calculating how assets within the sector might be damaged or destroyed, regardless of their direct connection to cyber threats.

The final parameter, $\boldsymbol{Xciep}$, determines the financial exposure at risk in the country (c) due to threat (p). This reflects the portion of assets that may be destroyed or stolen as a result of specific cyber threats targeting individual sectors or financial flows within the country. This metric is essential for evaluating the economic impact of a particular cyberattack, especially in terms of disruptions to financial or physical assets resulting from criminal activities or attacks on information systems.

Thus, $\boldsymbol{Ycie}$ and $\boldsymbol{Xciep}$ calculate the fractional impact of each cyber threat on economic indicators, such as production and value added by each sector. These parameters allow for assessing the likelihood and scale of economic losses caused by cyber incidents and aid in designing strategies to mitigate risks. Calculating these indicators is a crucial step in determining the extent to which each sector might be affected by cyber threats and identifying potential methods to minimize such losses through improved cybersecurity, preventive measures, and effective cyber risk management.

To estimate economic losses from cyber threats at the sectoral level, the model can calculate direct output losses for each sector i in the country c by integrating the impact of various types of threats and exposures. This provides deeper insights into how cyberattacks might affect each specific sector of the economy. The calculation of these losses is based on summing up the range of risks associated with different types of exposures (e) and threats (p). For each threat and exposure type, the model determines how their impact ($\boldsymbol{Ycie}$ and $\boldsymbol{Xciep}$) correlates with the sector's output volume, enabling precise estimation of direct economic losses due to cyber threats.

The formula for determining the direct output losses for each sector is as follows:

$$dcio = Oci \sum e \in E \sum p \in p \; YcieXciep \; \forall i \in I, \; c \in \mathrm{C} \qquad (2)$$

DOI: 10.55643/fcaptp.2.61.2025.4672

Where: Oci is the output volume of sector i in country c, which is one of the key parameters for determining the scale of economic losses, $Ycie$ is the share of gross product $wci * Gc$, illustrating the amount of money at risk from each type of exposure (e), $Xciep$ is the share of exposure at risk in country c and sector i that could be successfully destroyed, stolen, or otherwise lost due to a specific cyber threat (p).

This approach allows for a comprehensive assessment of potential economic losses from cyber incidents, determining both the direct losses within each sector and how these losses may impact the overall economic picture in the country.

By altering production volumes in a specific sector, we can observe how this affects the overall sectoral GDP loss. Specifically, the formula for calculating variable losses is as follows:

$$dcig = wciGc \sum \sum YciepXciep = wciGc\ Oci\ e\in E\ p\in p\ dcio\ \forall i \in I, c \in C \quad (3)$$

In this case, $\boldsymbol{dcig}$ represents the economic losses resulting from reduced production, as well as their impact on the country's overall gross product. An increase in risks and partial destruction of assets within a sector causes these losses, which can be calculated using the parameters mentioned earlier.

Next, to estimate the total economic loss, it is necessary to aggregate losses across all sectors, providing an overall view of economic losses due to cyber threats at the national level:

$$dco = \sum dcio \quad (4)$$

Furthermore, to calculate the total GDP losses for the country, the following aggregated indicators are applied:

$$dcg = \sum i\in I\ dcig \quad (5)$$

Thus, aggregating losses by sectors and analyzing total economic losses allows not only the estimation of potential financial losses but also the identification of weak spots in the economy that require enhanced cybersecurity measures. This approach enables strategic planning and the implementation of actions aimed at reducing risks and minimizing losses in the event of cyber incidents.

Given the high complexity of measuring cyber risks and the uncertainty associated with evaluating potential cyberattack scenarios, it is crucial to understand how different models and assumptions can influence calculations of economic losses, particularly when determining the share of sectoral GDP $\boldsymbol{wci * Gc}$ for a specific country c. This is critical because estimates of economic losses caused by cyberattacks can vary significantly depending on the assumptions and models used to forecast these risks.

The primary advantage of our model over many previous approaches to assessing cyber losses is that it allows for the calculation of not only the direct economic losses of individual sectors but also their systemic impact on the entire national economy. A key feature of our model is that it considers not only the direct losses suffered by specific institutions impacted by cyberattacks but also the broader macroeconomic effect.

A distinguishing feature of our model is that the input data for it is a Leontief "input-output" table (an example of a classical Leontief "input-output" table is shown in Table 2). This allows for sector-level analysis, which is more convenient and realistic for economic modelling than analyzing individual market players. Using a sectoral approach, we can effectively evaluate the systemic impact of a cyberattack, considering not only direct but also indirect effects on the economy.

Table 2. Classical Leontief "Input-Output" Table. *(Source: constructed by the author based on Issues Examination Guidance to Banks Outlining New Targeted Cyber Security Preparedness Assessments, 2012)*

Sectors / Expenditures	Sector A	Sector B	Sector C	Final Demand	Gross Output
Sector A	30	10	20	40	100
Sector B	15	25	5	55	100
Sector C	20	15	10	55	100
Expenditures	65	50	35	-	150

According to Table 2, all three sectors are interconnected through internal and external costs, ensuring an effective allocation of resources. The gross output is balanced in relation to costs and final demand, indicating the stability of the economic system within the framework of the given model.

There are two main approaches for implementing a theoretical model of this type, each with its own features and limitations. The first is the use of an input-output table, and the second is the application of a calibrated Computable General Equilibrium (CGE) model. Each of these approaches has its advantages and disadvantages. In the input-output table, we can clearly identify how changes in one sector of the economy are transmitted to others. However, this model has limitations because it does not account for substitution effects. That is, changes in one sector are treated as linear, and the possibility of flexible adaptations, such as firms adjusting their expenditures or resource usage in response to price changes, is not considered.

The choice between these two approaches depends on the available data and the goals of the study. In our case, we will use the input-output method for calculations because it allows us to focus on studying the direct economic losses caused by cyber-attacks, and it is more accessible for implementation when the precision of modelling substitution effects is less critical. However, in future research, we also plan to apply the calibrated CGE model to assess long-term adaptation effects and gain a better understanding of economic dynamics under cybersecurity threats.

In our model for calculating systemic cyber-risk, particularly for assessing systematic output losses ($scio$) based on the analysis of the impact of cyber threats on various sectors of the economy, we focus not only on the financial and banking sector but also on the broader impact of these threats on the economy as a whole. The key tool for such calculations is the use of the input-output model, which enables the study of interrelationships between changes in one sector and their impact on other sectors. This allows us to form a clear understanding of how cyber-attacks or cyber-risks can cause systemic losses in economic production.

To calculate the systemic output losses from cyber-threats, we use the following formula:

$$scio = \sum j \in I\ zcijdcio\ \forall i \in I,\ c \in C \quad (6)$$

where $zcij$ represents the elements of the inverse matrix (In − Ac)−1, which describes the dependence between sectors in the economy.

This matrix allows us to calculate how changes in one sector (for example, in the financial sector) are transmitted to other sectors through their interconnections within the economy. Each element of this matrix represents a multiplier that defines how changes in the output of one sector alter the overall production level in another sector.

The input-output model is based on the principle of linear changes in costs and production. When a cyber threat causes losses in a specific sector, these changes are transmitted through a chain of intersectoral relationships. Thus, systemic losses in a particular sector (for instance, in the financial and banking sector) will also impact other sectors, creating spillover effects that lead to overall losses in production.

To account for these changes in GDP structure, we introduce the following equation:

$$scig = scio\ (wciGc/Oci)\ \forall i \in I,\ c \in C \quad (7)$$

where $scig$ is the systematic loss within a specific sector; wci, Gc, and Oci are coefficients that adjust the impact of each sector on the overall production volume.

This allows for a more accurate estimate of how cyber-risks affect various aspects of the economy, considering not only direct losses but also spillover effects that may have far-reaching consequences for all economic links.

By aggregating these sectoral losses, we can obtain the total systemic output losses and GDP losses for the entire country:

$$sco = \sum scio;\ i \in I\ scg = \sum i \in I\ scig\ c \in C \quad (8)$$

This enables us to obtain the total losses for the economy, which include both direct and systemic output losses caused by cyber-threats.

In this model, it is particularly important to identify how direct economic losses due to cyber-attacks transform into broader systemic effects that encompass the entire economy. That is, even if a specific sector experiences direct damage from

DOI: 10.55643/fcaptp.2.61.2025.4672

cyber-attacks, it may have a domino effect, leading to losses in other sectors of the economy. This mechanism of systemic losses allows not only the measurement of the consequences of cyber-attacks for individual sectors but also the evaluation of how these threats may undermine the overall stability of the economy, affecting the country's GDP as a whole.

As the first step in building an objective picture of economic losses across all sectors of the economy based on the proposed model, we suggest examining the consolidated calculations of the model parameters Ycie for Ukraine's financial sector and other industries (calculated using the formulas provided above and presented in Table 3).

Table 3. Assessment of model parameters Ycie for Ukraine's financial sector and other industries of the economy. *(Source: constructed by the author based on Issues Examination Guidance to Banks Outlining New Targeted Cyber Security Preparedness Assessments, 2012)*

Sector	Ycie Parameters	Capital Assets U()	Intangible Assets U()	Profit/Loss U()
All Sectors Together	R=0.964, R^2=0.931, F(3,69)=309.26	-	0.193 ± 0.057	0.279 ± 0.053
Asset Management	U(0.89, 0.92)	U(0, 0.04)	U(0.03, 0.06)	-
Banking Sector	U(0.35, 0.47)	U(0, 0.4)	U(0.15, 0.27)	U(0, 0.08)
Business and Professional Services	U(0.69, 0.93)	U(0.07, 0.30)	U(0, 0.11)	U(0.02, 0.05)
Consumer Goods	U(0.93, 0.97)	U(0, 0.6)	U(0.04, 0.09)	U(0.06, 0.09)
Defense and Aerospace	U(0.91, 0.93)	U(0, 0.03)	U(0.02, 0.05)	U(0.01, 0.03)
Healthcare and Insurance	U(0.89, 0.91)	U(0, 0.05)	U(0.02, 0.06)	U(0.04, 0.06)
Media	U(0.90, 0.95)	U(0, 0.03)	U(0.03, 0.06)	U(0.03, 0.07)
Oil, Gas, and Chemicals	U(0.65, 0.76)	U(0.10, 0.20)	U(0.09, 0.27)	U(0.05, 0.12)
Public Sector	U(0.79, 1)	U(0, 0.08)	U(0, 0.32)	U(0.06, 0.15)
Technology and Electronics	U(0.90, 0.99)	U(0, 0.09)	U(0, 0.09)	U(0.08, 0.12)
Telecommunications	U(0.85, 0.95)	U(0.09, 0.25)	U(0, 0.03)	U(0.02, 0.05)
Transportation	U(0.89, 1.23)	0	U(0, 0.29)	U(0.10, 0.18)
Utilities	U(0, 1.39)	U(0, 1.39)	U(0, 1.21)	U(0.15, 0.35)
Wholesale and Retail Trade	U(0.90, 0.94)	U(0, 0.04)	U(0.03, 0.06)	U(0.04, 0.07)
Other	U(0.93, 0.96)	U(0, 0.02)	U(0.04, 0.06)	U(0.02, 0.05)

The table presents the statistical characteristics of the study, including the coefficients of determination (R = 0.964, R^2 = 0.931), which indicate the high quality of the constructed model. The value of F(3,69) = 309.26 confirms the significance of the selected factors in explaining the dependent variable.

The logarithmic transformation of dependent and independent variables in the model allows for the interpretation of coefficients as elasticities, i.e., as the percentage change in sectoral profitability (output) in response to a percentage change in the corresponding factors. For example, under the model's assumptions, a 1% decrease in the value of intangible assets results in a 0.2% reduction in the financial sector's profitability. Similarly, a 1% reduction in total assets exposed to operational risks leads to a 0.4% decrease in profitability, while the loss of profit results in a 0.2% decline in performance.

Since the primary goal of the model is to determine direct systemic and aggregate losses in Ukraine's financial sector, the estimation of the Ycie parameter was performed only for the banking sector. Empirical data was used for this, and the coefficients for other sectors were adapted based on Dreyer's calculations.

Thus, logarithmic indicators provide a deeper understanding of the impact of individual factors on economic stability, allowing for an accurate assessment of risks and identifying key areas for minimizing losses.

After analyzing the nature of cyber threats impacting financial exposures, we proceed to the mathematical model for determining the Xciep parameter. This parameter represents the share of exposure in a specific country (ccc), sector (iii), and asset type (eee), which can be lost, stolen, or damaged due to the implementation of a specific cyber threat (ppp). In other words, this indicator allows for the assessment of which portion of financial assets or resources is at risk in the event of a cyber incident.

Table 4 presents estimates of the share of the economic product at risk due to cyber threats in the form of triangular probabilistic distributions. This approach allows for accounting for uncertainty and variability in forecasts, which is essential for modelling complex risks in the digital age.

Table 4. Estimates of the share of the economic product at risk due to cyber threats in the form of triangular probabilistic distributions. *(Source: constructed by the author based on Issues Examination Guidance to Banks Outlining New Targeted Cyber Security Preparedness Assessments, 2012)*

Model Threats	Interaction with Financial Exposures (T, Probabilistic Distributions)	Relevance to Financial and Banking System Threats
Data Exfiltration of Company Information	Capital Assets: T(0, 0.0043, 0.021) Intellectual Property: T(0, 0.00012, 0.00096) Net Income: T(0, 0.0015, 0.0032)	Leakage of confidential bank information, violation of information security policies, reputational risk
Data Exfiltration of Client Information	Capital Assets: T(0, 0.0043, 0.021) Intellectual Property: T(0, 0.00012, 0.00096) Net Income: T(0, 0.0015, 0.0032)	Loss of personal client data, increased costs to restore trust and compensate losses
Data Degradation, Destruction, and Damage	Capital Assets: T(0, 0.0083, 0.041) Intellectual Property: T(0, 0.00025, 0.0021) Net Income: T(0, 0.0031, 0.0079)	Disruption of banking systems' availability, destruction of transactional data, operational slowdown
Business Interruption	Capital Assets: T(0, 0.0083, 0.041) Intellectual Property: T(0, 0.00025, 0.0021) Net Income: T(0, 0.0031, 0.0079)	Complete failure of banking systems, shutdown of online banking, risks of bankruptcy and financial crisis

Thus, the analysis results indicate the need for financial institutions to focus on preventing cyber threats and minimizing potential losses by enhancing cybersecurity levels.

As a result of the conducted analysis, it was determined that direct losses for the financial and banking sector amount to USD 14.05 million, while systemic losses reach USD 38.03 million. This indicates a high concentration of risks due to the presence of systemically important financial institutions that perform critical functions in the national economy. The risks associated with cyber threats are not limited to direct losses; they also have a significant systemic impact on the economy. For example, the leakage of personal and identification information can have a deep and lasting effect on the trust in financial institutions, which, in turn, leads to additional losses throughout the country's financial system. This increases the level of interconnections and correlations between different types of risks, highlighting the need to develop comprehensive strategies for their mitigation.

Particular attention should be paid to how cyber threats can create so-called "domino effects" in the economy. For instance, a reduction in production capacities in the defence sector or technology companies may lead to a decrease in demand for products from other sectors, such as transport or consumer goods, which in turn reduces the overall economic output. This requires considering cyber risks not only as localized threats but as global factors that influence the stability and growth of the entire economy.

Cyber risk management can be carried out using several key methods, including risk avoidance, mitigation, and transfer. Each of these approaches has its own specifics and application possibilities depending on the nature of the threats and the scale of potential business consequences.

1. **Risk Mitigation:**
   - Risk mitigation involves implementing technical and organizational measures aimed at minimizing the likelihood of cyber threats and mitigating their impact if they occur. One of the most effective measures is the installation of reliable information protection systems such as firewalls, intrusion detection and prevention systems (IDS/IPS), data encryption, and regular software updates to safeguard against new vulnerabilities.
   - Reducing cyber risks also includes ensuring reliable access to information systems for authorized users only and implementing multi-factor authentication, which significantly reduces the likelihood of unauthorized access. Additionally, it is important to develop internal security policies and continuously train employees, as the human factor is often a weak link in ensuring cybersecurity.
2. **Risk Transfer:**
   - Risk transfer involves using external tools and services to reduce the financial burden of cyber threats. One of the most common mechanisms is cyber risk insurance, which allows a company to transfer part of its financial liability for potential losses from cyber incidents to insurance companies. This way, businesses can protect themselves from severe financial consequences while preserving their resources for recovery after incidents.

DOI: 10.55643/fcaptp.2.61.2025.4672

- Another option for risk transfer is the use of secure third-party services, such as cloud services and cybersecurity solutions provided by external companies with high expertise in data and system protection. In this case, the company delegates part of its cybersecurity environment to other organizations specializing in such matters, thereby reducing risks for itself.

3. Risk Avoidance:

- Risk avoidance is the most radical approach to managing cyber threats. In the case of a significant likelihood of serious incidents, a company may choose to redesign its business processes or discontinue high-risk technologies and platforms. For example, some enterprises may decide to limit the use of certain software products or switch to more secure technologies if there is a high probability they could be used for attacks. Discontinuing the use of certain online services or integrating with new platforms may also help avoid potential threats.
- However, such risk avoidance should be part of a strategic plan, as radical changes can affect the efficiency and flexibility of the business. In this context, it is essential to carefully analyze whether the security benefits outweigh the possible losses from changes in business processes.

4. Cyber Risk Management Tools and Mechanisms:

- National Bank of Ukraine and other supervisory bodies, can significantly reduce systemic cyber risk by implementing stringent data protection requirements and securing the information infrastructure of critical sectors of the economy. They can develop and implement regulatory acts that are mandatory for all businesses operating in the financial and technology sectors.
- An essential part of this process is the creation of national cybersecurity standards that consider international practices and trends. International standards such as ISO/IEC 27001 for information security management, as well as GDPR standards, set clear requirements for personal data protection and can be adapted to ensure protection not only from external attacks but also to prevent internal threats.
- Thus, cyber risk management is a multifaceted and complex process that requires the use of various methods, including prevention, mitigation, transfer, and even avoidance of risks. This allows not only reducing the likelihood of cyber incidents but also minimizing their consequences, ensuring business resilience and protecting its reputation.

Regulation of the financial sector is a critical component of ensuring economic stability, as it creates conditions for growth, maintaining trust, and reducing potential risks arising from instability in financial markets. One of the primary tasks of such regulation is to minimize the negative impacts on the economy, particularly costs associated with financial crises, defaults, and other unforeseen situations that may destabilize the market. However, to ensure that regulation remains effective in modern conditions, it must be adapted to new challenges, including technological changes and risk factors that are increasingly becoming more significant, such as cyber risks.

The G7 group of countries has taken an important step toward creating global standards for managing cyber risks by proposing a set of high-level principles that should serve as the foundation for developing and implementing cybersecurity strategies in the financial sector. This approach involves creating a standardized and coordinated cybersecurity management model that would be universally applicable to all types of institutions, regardless of whether they belong to the public or private sector. The key goal of this set of principles is to ensure not only the internal security of organizations but also to increase cooperation between public institutions, financial organizations, and international regulators to create an effective system for countering cyber threats.

Specifically, the "building blocks" concept for cybersecurity, as proposed, includes not only practical steps for implementing a strategy to protect against cyber threats but also defines the structure and organizational elements that should form the foundation of this strategy. This allows each organization that adopts these standards to develop its own cybersecurity policy, taking into account both international and national requirements, as well as the specific challenges of their particular industry.

In our opinion, the following elements should be highlighted as part of a comprehensive cybersecurity management model for financial and banking institutions:

1. **Cybersecurity Strategy and Framework**. As the development of a comprehensive cybersecurity strategy is a necessary condition for effectively combating cyber threats, it should take into account the specifics of cyber risks and interactions with other sectors and international organizations involved in oversight and regulation in this area.

2. **Governance**. Defining clear roles and responsibilities among staff responsible for implementing the cybersecurity strategy ensures not only the effectiveness of its implementation but also establishes an accountability system, which is crucial for quick responses to incidents and managing crisis situations.
3. **Risk and Control Assessment**. This allows organizations to clearly understand which elements of their operations are most vulnerable to cyber threats, and based on this, create measures to mitigate these risks, as well as detect and neutralize potential threats at early stages.
4. **Monitoring**. Continuous monitoring of the organization's cybersecurity status provides the ability to respond promptly to new threats and incidents that arise in the network. Regular checks and testing help identify weaknesses in existing protection systems and take necessary measures.
5. **Incident Response**. Timely detection of cyber incidents is crucial, but so is the effective response to them, including containing the spread of the threat, informing stakeholders, and coordinating actions to mitigate the consequences of the incident.
6. **Post-Incident Recovery**. After any cyberattack, the organization must have a recovery plan in place to restore its operations. This includes not only technical recovery but also analyzing potential vulnerabilities, addressing them, and ensuring resilience to similar incidents in the future.
7. **Information Sharing**. Effective information exchange about cyber threats between financial institutions, government agencies, and other stakeholders contributes to improving protection at the global level. Rapid data exchange on new threats and vulnerabilities allows organizations to promptly adapt their protection strategies.

All of these elements create a comprehensive cybersecurity management model, which is crucial in the rapidly changing technological landscape constantly influenced by new cyber threats. However, to achieve effectiveness, these standards must be adapted to the specific conditions of different countries and organizations, which requires ongoing international cooperation and exchange of experience. As a result, the proposed model not only protects financial institutions from cyberattacks but also creates a foundation for global security, which is an important factor for the stability of the global economy.

DISCUSSION

Cyber risks in the financial and banking system represent one of the greatest threats in today's digital world. We agree with the perspective of Eisenbach T. (Eisenbach, 2019) that it is crucial not only to prevent cyber threats but also to develop effective recovery strategies that minimize losses and ensure system resilience.

Modern cyber threats are increasingly complex and can lead not only to direct financial losses but also to significant systemic risks that may impact the stability of the economy as a whole. Key aspects of managing cyber risks should not only include technical measures but also the development of clear regulatory mechanisms, as well as effective interaction between government bodies, businesses, and international partners. Considering these factors will help establish a solid foundation for the development of financial institutions resilient to cyber threats, which will ensure trust from clients and strengthen the economy in the context of globalization.

Therefore, based on the conducted research, we proposed an innovative model for assessing economic losses from cyber risks (including cyberattacks) for Ukraine's economy. Unlike existing approaches, this model is specifically designed for the financial and banking sector.

CONCLUSIONS

The paper proposes an innovative model for assessing economic losses from cyber risks (specifically cyberattacks) for the economy of Ukraine, with a focus on the financial and banking sector. This model is based on the analysis of losses through different types of cyber risks, divided into direct and systematic, considering macroeconomic distribution, where the analysis is conducted at the sector level rather than for individual enterprises or market players. This approach allows for the assessment of the impact of cyber incidents on the economy as a whole, particularly on key sectors that are strategically important for the financial system and the banking sector.

One of the main aspects of the model is the use of a Leontief "input-output" table, which helps determine how changes in one sector of the economy affect other sectors through mutual economic connections. This table allows for calculating the

DOI: 10.55643/fcaptp.2.61.2025.4672

multiplier effect of losses from cyberattacks, considering not only direct losses but also secondary effects that can affect the entire economic chain from production to consumption.

For accurate calculation of cyber losses arising from cyberattacks, the model includes several key factors reflecting the financial exposures of different sectors of the economy. One important element is the assessment of the impact on intangible assets of enterprises. Specifically, if the value of intangible assets decreases by 1%, it will lead to a 0.2% reduction in profitability. Intangible assets such as software, intellectual property, brands, and company reputation are crucial components of capital, and their loss can have significant long-term consequences for the financial stability of companies in the sector.

Another key aspect is the evaluation of the impact on total assets subject to operational risk. A 1% decrease in these assets may result in a 0.4% decline, reflecting serious economic consequences for the financial and banking sector, where the main assets are loans, deposits, investments, and infrastructure that support operational activities. Cyberattacks can disrupt this infrastructure, affecting the ability of financial institutions to perform their core functions.

Additionally, an important factor for assessing financial losses is the foregone profit. If enterprises are unable to carry out operations or reduce their productivity due to cyber incidents, this leads to losses in the form of unearned profits. In the case of the financial and banking sector, a decrease in revenue from providing financial services or securities operations can have a significant impact on the overall financial results and even cause liquidity shortages in the system.

Overall, the econometric model proposed by the authors is a powerful tool for comprehensive analysis of the economic consequences of cyber threats at the macroeconomic level, especially for the financial and banking sector, which is one of the most vulnerable industries to cyberattacks. This allows not only for assessing direct losses but also for forecasting long-term effects on the country's economy, including through a loss of confidence in the financial system, capital outflows, or deterioration of the investment climate. Considering such parameters enables governments and enterprises to better prepare for potential cyber threats and develop effective protection strategies.

Active risk management is crucial for the effective implementation of cybersecurity measures in any organization, as it helps not only reduce potential threats but also maintain stability and competitiveness. Cyber risks can arise at any moment, and to successfully minimize them, a comprehensive approach is necessary, incorporating both technological and organizational measures. It is important not only to react to existing cyber threats but also to actively prevent them. Recommendations at the level of individual business units focus on several key strategies: avoidance, reduction, and risk transfer.

1. **Avoiding Cyber Risks** involves radical changes in business processes. This may include modernizing the company's infrastructure, abandoning outdated technologies, implementing the latest information protection protocols, and changing policies for accessing critical data. Changing business processes can include transitioning to more secure operational models, implementing the principle of least privilege, and network segmentation to reduce the likelihood of cybercriminals gaining access.
2. **Reducing Cyber Risks** involves using technologies and approaches that decrease the probability and scale of cyber incidents. This includes cybersecurity training for staff, conducting stress tests, assessing IT system vulnerabilities, and developing and maintaining incident response plans. Continuous improvement of employees' knowledge and skills, and training them to respond to potential threats, are key elements in maintaining the organization's resilience to cyberattacks.
3. **Transferring Risk** involves using financial instruments such as insurance. Purchasing cyber insurance allows organizations to transfer some of the financial losses to insurance companies in the event of a cyber incident. This helps organizations reduce their potential financial losses and focus on recovery after an incident.

An important aspect is the development of international cybersecurity standards, which helps establish common rules and procedures for ensuring security not only for individual enterprises but also for the entire sector. For example, setting requirements for whitelists of applications, using standardized protection system configurations, restricting administrator rights, and using cloud infrastructures help systematize the approach to cybersecurity and simplify the implementation of protective mechanisms. These measures ensure higher reliability and resilience to potential cyber threats, reducing the likelihood of critical disruptions in organizations' operations.

Moreover, to reduce systemic cyber risk and improve cybersecurity at the national economic level, financial sector regulators must play an active role in forming clear norms and standards. One of the first steps is developing a common terminology and definitions that allow for standardizing approaches to cyber risk management across all sectors of the economy and ensuring accuracy in the interaction between different authorities and the private sector. Such definitions will help

avoid misunderstandings in policy formulation and create the basis for more effective cooperation among all cybersecurity participants.

To ensure transparency and effective monitoring of cyber risks, regulators should set requirements for financial institutions to provide regular reports on internal cyber risk data. This should include both periodic reporting and real-time notifications of new incidents. An important aspect is protecting the confidentiality of company information. Therefore, data should be anonymized or aggregated to a level that provides an overall picture without violating business secrets.

Thus, creating a cyber-secure economic infrastructure requires a comprehensive approach that includes not only technical protection measures but also institutional changes, effective cooperation between different authorities and the private sector, and the development and implementation of unified standards for cyber risk management.

Our future research will focus on: further studying the impact of cyber risks on the financial and banking sector, particularly identifying vulnerable infrastructure elements and assessing potential losses from cyber incidents; developing models for forecasting cyberattacks and their consequences for macroeconomic stability, analyzing their impact on GDP and financial stability; evaluating the effectiveness of national cybersecurity strategies and regulations, improving mechanisms for co-operation between government, private, and international partners; analyzing the implementation of international cyber-security standards for the financial sector and adapting them to the needs of Ukrainian institutions; developing recom-mendations for financial institutions on creating cyber risk management strategies, including building cybersecurity sys-tems, training personnel, and selecting insurance products for risk transfer; studying the impact of cyber insurance on reducing the financial consequences of cyber incidents for institutions and their clients.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors received no funding for this research.

REFERENCES

1. Akimov, O., Karpa, M., Parkhomenko-Kutsevil, O., Kupriichuk, V., & Omarov, A. (2021). Entrepreneurship education of the formation of the e-commerce managers professional qualities. *International Journal of Entrepreneurship, 25*(7), 1-8. https://ep3.nuwm.edu.ua/20936/1/Akimov%2C%20Oleksandr.%2C%20Karpa%2C%20Marta.%20Parkhomenko-Kutsevil%2C%20Oksana.%20Kupriichuk%2C%20Vasily.%20Omarov%2C%20Azad.%20%282021%29.%20Entrepreneurship%20Education%20of%20the%20Formation%20of%20the%20E-Commerce%20Managers%20Professional%20Qualities%20%D0%B7%D0%B0%D1%85.pdf
2. Akhtar, S., Sheorey, P. A., Bhattacharya, S., & Ajith Kumar, V. V. (2021). Cyber Security Solutions for Businesses in Financial Services. *International Journal of Business Intelligence Research*, *12*(1), 82–97. https://doi.org/10.4018/ijbir.20210101.oa5
3. Aldasoro, I. et al. (2020). Cyber risk in the financial sector. *SUERF. The European Money and Finance Forum, 206.* https://www.suerf.org/publications/suerf-policy-notes-and-briefs/cyber-risk-in-the-financial-sector/
4. Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.3203026
5. Bowe, M., Kolokolova, O., & Michalski, M. J. (2016). Systemic Risk, Interbank Market Contagion, and the Lender of Last Resort Function. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2760879
6. Brando, D., Kotidis, A., Kovner, A., Lee, M., & Schreft, S. L. (2022). Implications of Cyber Risk for Financial Stability. *FEDS Notes*, *2022*(3077). https://doi.org/10.17016/2380-7172.3077
7. Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). *A Taxonomy of Operational Cyber Security Risks Version 2*. Defense Technical Information Center. https://doi.org/10.21236/ada609863
8. Cooley, T. F., Philippon, T., Acharya, V. V., Pedersen, L. H., Philippon, T., & Richardson, M. (2012). Regulating Systemic

DOI: 10.55643/fcaptp.2.61.2025.4672

Risk. *Restoring Financial Stability* (p. 277–303). John Wiley & Sons, Inc. https://doi.org/10.1002/9781118258163.ch13

9. Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J., & Winkelman, Z. (2018). *Estimating the Global Cost of Cyber Risk: Methodology and Examples*. RAND Corporation. https://doi.org/10.7249/rr2299
10. Eisenbach, T. M., Kovner, A., & Lee, M. J. (2021). Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics*. https://doi.org/10.1016/j.jfineco.2021.10.007
11. Elliott, J., Wilson, C., Khiaonarong, T., Jenkinson, N., Adelmann, F., Morozova, A., Gaidosch, T., Schwarz, N., & Ergen, I. (2020). Cyber Risk and Financial Stability: It's a Small World After All. *Staff Discussion Notes*, *2020*(007). https://doi.org/10.5089/9781513512297.006
12. Frederic, S. M. (2007, September 28). Systemic risk and the international lender of last resort. *Tenth Annual International Banking Conference.* Chicago: Federal Reserve Bank of Chicago. https://www.bis.org/review/r071003f.pdf
13. Freixas, X., Parigi, B. M., & Rochet, J.-C. (2002). Systemic Risk, Interbank Relations, and Liquidity Provision by the Central Bank. *Financial Crises, Contagion, and the Lender of Last Resort* (p. 407–434). Oxford University: PressOxford. https://doi.org/10.1093/oso/9780199247202.003.0019
14. Issues Examination Guidance to Banks Outlining New Targeted Cyber Security Preparedness Assessments (2012, December 10). An official website of New York State. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1412101
15. Kryshtanovych, M., Akimova, L., Akimov, O., Kubiniy, N., & Marhitich, V. (2021). Modeling the process of forming the safety potential of engineering enterprises. *International Journal of Safety and Security Engineering, 11*(3), 223-230. https://doi.org/10.18280/ijsse.110302
16. Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability. *IMF Working Papers*, *17*(185). https://doi.org/10.5089/9781484313787.001
17. Lelyk, L., Olikhovskyi, V., Mahas, N., & Olikhovska, M. (2022). An integrated analysis of enterprise economy security. *Decision Science Letters, 11*(3), 299-310. https://doi.org/10.5267/j.dsl.2022.2.003
18. Martinez-Jaramillo, S., Molina-Borboa, J. L., & Bravo-Benitez, B. (2018). The role of Financial Market Infrastructures in Financial Stability. *Risk and Contingency Management* (p. 256–276). IGI Global. https://doi.org/10.4018/978-1-5225-3932-2.ch014
19. Mia, M. M., Rizwan, S., Zayed, N. M., Nitsenko, V., Miroshnyk, O., Kryshtal, H., & Ostapenko, R. (2022). The impact of green entrepreneurship on social change and factors influencing AMO theory. *Systems, 10*(5). https://doi.org/10.3390/systems10050132
20. Mishkin, F. S. (2000). Systemic risk, moral hazard and the international lender of last resort. *Private Capital Flows in the Age of Globalization* (p. 185–197). Edward Elgar Publishing. https://doi.org/10.4337/9781035335473.00018
21. Nikonenko, U., Shtets, T., Kalinin, A., Dorosh, I., & Sokolik, L. (2022). Assessing the policy of attracting investments in the main sectors of the economy in the context of introducing aspects of industry 4.0. *International Journal of Sustainable Development and Planning, 17*(2), 497-505. https://doi.org/10.18280/ijsdp.170214
22. Novak, A., Pravdyvets, O., Chornyi, O., Sumbaieva, L., Akimova, L., & Akimov, O. (2022). Financial and economic security in the field of financial markets at the stage of European integration. *International Journal of Professional Business Review, 7*(5), 1-20. https://doi.org/10.26668/businessreview/2022.v7i5.e835
23. Sumets, A., Kniaz, S., Heorhiadi, N., Skrynkovskyy, R., & Matsuk, V. (2022). Methodological toolkit for assessing the level of stability of agricultural enterprices. *Agricultural and Resource Economics, 8*(1), 235-255. https://doi.org/10.51599/are.2022.08.01.12
24. Sung Keun, O. (2017). Analysis of the Cyber Security of Financial Transactions for Financial Stability. *Korean Journal of Banking and Financial Law*, *10*(1), 3–35. https://doi.org/10.35274/kbfla.2017.10.1.001

Кришталь Г., Самофалова М., Сахно Л., Федина В., Мокієнко Т., Єрмолаєва М.

КІБЕРРИЗИКИ У ФІНАНСОВІЙ ТА БАНКІВСЬКІЙ СИСТЕМІ: АНАЛІЗ ПРЯМИХ І СИСТЕМАТИЧНИХ ВТРАТ

Стаття присвячена дослідженню впливу кіберризиків на банківський сектор і фінансову систему, зокрема на економічну стабільність країни. Визначено ключові фактори, що сприяють виникненню кіберзагроз, а також розглянуто методи їх мінімізації на рівні окремих фінансових установ. У процесі дослідження автори розглянули модель, що базується на аналізі прямого та систематичного впливу кібератак, з урахуванням макроекономічного розподілу й застосування леонтієвської таблиці типу «витрати-випуск», що дозволило створити об'єктивну картину економічних втрат на рівні всіх секторів економіки, а не лише на рівні окремих підприємств. Автори запропонували підхід до оцінки втрат через зниження вартості нематеріальних активів і операційних ризиків, що є важливим для точного визначення наслідків для фінансової системи, банківського сектора та конкурентоспроможності кожного окремого банку. Зниження доходів через зменшення доходності та недоотриманий прибуток — це також критичні фактори, які важливо враховувати при розрахунках. Закцентовано увагу на розвитку міжнародних стандартів для кібербезпеки, а також надано рекомендації щодо активного менеджменту ризиків, зокрема через уникнення, зменшення та

перенесення ризиків, що є важливим для практичного застосування результатів дослідження в бізнесі та державному управлінні. Автори довели, що перспективи для подальших досліджень у галузі кібербезпеки, включаючи аналіз впливу кіберризиків на макроекономічну стабільність, прогнозування наслідків кібератак для ВВП та фінансової стабільності, а також удосконалення механізмів взаємодії між державними й приватними структурами, є надзвичайно актуальними. Дослідження має практичну цінність для розробки стратегій захисту від кіберзагроз і може бути корисним для політиків, регулятора і бізнес-лідерів, що прагнуть забезпечити кібербезпеку економічної інфраструктури.

Ключові слова: цифровізація, кіберризики, фінансова система, банківська система, конкурентоспроможність

JEL Класифікація: E50

DOI: 10.55643/fcaptp.2.61.2025.4672