



ISBN: 978-83-963452-7-1

TACKLING ILLICIT FINANCIAL FLOWS AND CYBERATTACKS FOR ENHANCING NATIONAL SECURITY

**OLHA KUZMENKO
HANNA YAROVENKO
VICTORIA BOZHENKO**

CENTRE OF SOCIOLOGICAL RESEARCH

2021

Tackling Illicit Financial Flows and Cyberattacks for Enhancing National Security

Reviewers:

Prof. Dr. Ludmila Malyarets

PhD. Bholá Khan

Dr. Anton Boyko

This publication has been approved by the Editorial Board of the Centre of Sociological Research Publishing House to be issued as a scientific monograph.

Olha KUZMENKO
Hanna YAROVENKO
Victoria BOZHENKO

**Tackling Illicit Financial Flows and
Cyberattacks for Enhancing National
Security**

Centre of Sociological Research
Szczecin, 2021

Bibliographic information of The National Library of Poland

The National Library of Poland / Biblioteka Narodowa lists this publication in the Polish national bibliography; detailed bibliographic data are on the internet available at <<https://www.bn.org.pl>>.

ISBN: 978-83-963452-7-1

First edition, 2021

Publishing House: Centre of Sociological Research

<http://www.csr-pub.eu>

Szczecin, Poland 2021

All rights reserved.

The work including all its parts is protected by copyright. Any use away from the narrow limits of copyright law is inadmissible and punishable without the consent of the publisher. This applies in particular to reproductions, translations, microfilming and the storage and processing in electronic systems

To read the free, open access version of this book online, scan this QR code with your mobile device:



CONTENTS

INTRODUCTION	7
1. CYBERSECURITY IN FINANCIAL SERVICES AND ILLICIT FINANCIAL FLOWS: TRENDS AND PATTERNS	10
1.1. Transformation of the financial services sector in the context of digitalization	10
1.2. Trends and patterns in cybercrime research: bibliometric analysis	18
1.3. Modern global trends in the financial cybercrime in the financial sector	29
1.4. Assessing the cyber vulnerability of financial service consumers.....	54
1.5. Criteria for informal financial transactions mediated by financial institutions.....	68
2. CONCEPT OF CONVERGENCE OF FINANCIAL MONITORING AND CYBERSECURITY SYSTEMS	79
2.1. Fundamentals of convergence processes of financial monitoring and cybersecurity systems.....	79
2.2. Assessing the convergence level of the cyber security system and counteraction of money laundering.....	100
2.3. DEA-analysis of the effect of financial monitoring and cybersecurity systems integration	113
2.4. Key algorithms of financial monitoring and cybersecurity systems of financial institutions.....	136
CONCLUSIONS.....	166
REFERENCES.....	168
APPENDIX A	184

INTRODUCTION

The rapid introduction of innovative information technologies at different levels of the financial system, on the one hand, contributes to an increase in the country's competitiveness in the world arena, as well as its investment attractiveness. On the other hand, it causes an increase in the scale of cross-border economic crime, an increase and spread of various cybercrime schemes, an increase in the number of illegally obtained income, accompanied by the improvement of money laundering mechanisms. Given the increasing geopolitical competition in cyberspace and the growing landscape of cyber threats, especially in the context of the Covid-19 pandemic, the issue of protecting information from cyberattacks, both at the level of a financial institution and the state, is an urgent task for today and future five years.

Nowadays, international requirements for the anti-money laundering system are growing, which involves constant monitoring to detect suspicious transactions. But there is a growing number of transactions aimed at money laundering and terrorist financing involving hackers and other cybercriminals, which requires increased requirements for financial cybersecurity. Against this background, there is also an increase in information flows, rapid changes in the environment, and improved software and hardware tools, leading to a slowdown in financial institutions to effectively combat cyber and financial crime.

Therefore, the current realities of the growth of cyber fraud and criminal proceeds legalization also require the introduction of more effective measures, which is possible at the legal, methodological, informational, program-technological and organizational levels of the financial sector management. Ensuring these processes is possible only through the

convergence of two systems - cybersecurity and financial monitoring.

Based on the relevance of cybersecurity of financial services and illegal financial flows, the object of the study is the system of economic relations between economic entities and financial market regulators, which arise in the integrated application of financial monitoring and combating cybercrime. The research subject is the methodological basis of the formation of complex preventive intellectual mechanisms of regulation of financial market subjects to ensure their cybersecurity.

The purpose of this monograph is to identify trends and patterns of financial services in the context of cybersecurity and develop a concept of convergence of financial monitoring and cybersecurity systems. It is necessary to solve such tasks to achieve the goal:

- study of the processes of transformation of the financial services sector in the context of their digitalization;
- identification of trends and patterns of cybercrime research through bibliometric analysis;
- analysis of current global trends in the spread of cybercrime in the financial sector;
- assessing the level of cyber vulnerability of consumers of financial services;
- construction of a phase portrait of a cyber-fraud victim;
- substantiation at the theoretical level convergence processes of financial monitoring and cybersecurity systems;
- assessment of the potential convergence of the cybersecurity system and counteraction to financial fraud, taking into account the levels of economic development of different countries;
- conducting DEA-analysis of the effect of financial monitoring and cybersecurity systems integration;
- development of algorithms for cybersecurity and financial monitoring convergence in financial institutions.

The monograph was performed within the framework of the research themes «Data Mining for Countering Cyber Fraud and Money Laundering in the Context of Digitalization of the Financial Sector of the Ukrainian Economy» (0121U100467), «National security through the convergence of financial monitoring and cybersecurity systems: intelligent modeling of financial market regulation mechanisms» (0121U109559) which are financed by the State budget of Ukraine.

1. CYBERSECURITY IN FINANCIAL SERVICES AND ILLICIT FINANCIAL FLOWS: TRENDS AND PATTERNS

1.1. Transformation of the financial services sector in the context of digitalization

The intensive development of digital technologies has transformed the financial services market, posing new challenges and threats to the further functioning of traditional financial institutions. It has been established that due to the rapid development of innovative technologies, financial companies could lose up to a third of their income (Payments Industry Intelligence, 2019). In these conditions, financial institutions are increasingly beginning to cooperate with fintech companies and are investing intensively in modernizing their infrastructure, optimizing business processes, improving the quality of financial services, and increasing their level of information security.

The development of financial technologies is one of the main topics for discussion at international economic forums and conferences. This issue is widely covered in the works of foreign scientists. According to Albeshr and Nobanee (2020), blockchain can completely change banking services. It has a high level of security, increased transparency of transactions, a decentralized system, and can conduct transactions more efficiently.

Risman et al. (2021) evaluated the impact of potential threats and risks caused by the rapid growth of IT on the stability of the financial system. The regression analysis showed that if the level of systemic risk in the country increased, the positive effect of digital technologies on financial stability decreased. Frame et al. (2014) are convinced that financial innovation transforms the

financial sector in three dimensions: new products and/or services, new production processes, and new business models.

Particular attention should be paid to the work of a group of scientists (Lyeonov et al., 2019), which proposed an integral indicator for assessing the level of technologization of financial services based on the aggregation of indicators that characterize the level of digitalization of society, financial inclusion of the population, and the use of a digital channel for providing financial services. Based on the results of calculating this integral indicator, it was found that the level of technologization of financial services in Ukraine is growing steadily every year but significantly lagged behind European countries (in 2017, Ukraine – 17.7%, Norway – 57.3%, Latvia – 40.4%).

Based on the results of the Frontier analysis, it was found that an increase in banks' investment in the development of their digital infrastructure encourages growth in the volume of financial transactions through digital channels (Wiridiyanti, 2018; Carbó-Valverd et al., 2020).

The development of digital technologies and the accumulation of a significant amount of data have allowed fintech lending technologies to become a potentially promising solution for reducing the cost of loans and increasing financial inclusion. The paper (Bazarbash, 2019) uses machine-learning methods to assess the client's solvency: models based on decision trees with various construction algorithms, vector models, and neural networks. In addition, another study (Huang et al., 2020) assessed the level of a borrower's creditworthiness based, firstly, on big data and machine learning models, and secondly, on the financial data provided by a client using classical banking techniques. An empirical study has shown that the fintech approach allowed building a more accurate forecast of the risk of non-payment of funds on loans during periods of economic stability and during the crisis period. Thus, innovative solutions for analyzing the solvency of legal entities and

individuals allow improving the bank's risk management system and creating conditions for its stable functioning.

Along with financial institutions and fintech companies, new players are gradually entering the banking services market – BigTech companies (large IT companies), initially developing their payment systems and expanding the range of innovative and technological financial services.

Methods of qualitative (SWOT and PEST matrices) and quantitative (correlation coefficients, regression model) analysis were used to study the impact of the interaction between fintech companies and banks (Martínez-Sánchez et al., 2020). The study results showed that, using the example of the Lithuanian banking system, technologization and informatization contribute to an increase in the efficiency of its activities and require strengthening cooperation between financial institutions and IT companies to meet the needs of customers. The authors of this study note that to analyze the relationship between banking and financial technologies, it is better to choose qualitative analysis methods.

Companies that develop flexible financial technologies can improve the efficiency of financial companies and help national regulators improve approaches in the field of prudential regulation and supervision, monitoring of fraudulent transactions, monetary policy, etc. Nowadays, the central banks of many countries of the world make the transition from inspections with the participation of the regulator's employees to automated training of neural networks based on algorithms.

PwC (2017) experts view financial technologies (FinTech) as a dynamically developing segment at the intersection of financial services and technology sectors, in which financial institutions, technology startups, and new financial market participants apply innovative approaches to products and services.

The leading advanced technologies include artificial intelligence, blockchain, Big Data, cloud technologies, the Internet of Things, automation of robotic processes, biometric technologies, virtual reality technologies, etc.

Big Data should imply a set of structured and unstructured data directly or indirectly related to the object under study. The data can be used at any stage of the financial institution's life cycle: determining the target audience and cost of a financial service, assessing the borrower's creditworthiness, developing a policy for promoting and selling a financial service to the market, identifying fraudulent transactions, etc. Thus, extensive data analysis allows attracting new customers and retaining them, meeting their expectations as much as possible, and predicting their behavior. It has been established that by 2030 the banking services market will save more than \$1 trillion through the introduction of artificial intelligence and machine learning technologies, which is about 22% of the costs of banking institutions (Marsh & McLennan companies, 2019). Examples of the use of artificial intelligence in the banking sector are:

- introduction of chatbots that provide automated on-demand assistance (for example, answering frequently asked questions), perform bank account maintenance, etc.;
- a customer relationship management system (CRM) that automates interaction with consumers of financial institutions and meets their needs;
- a system for assessing the risk of using financial institutions to make fraudulent transactions. According to a study conducted by the Association of Certified Fraud Examiners, in 2019, 13% of companies already use artificial intelligence to fight financial crime.

Financial institutions increasingly use this database technology to create, securely transfer and store information due to the advantages of distributed ledger technology (blockchain).

It is worth noting that this technology is not controlled or administered centrally. Blockchain creates smart contracts or agreements that automatically execute an agreed transaction if certain conditions are met. This allows storing any digital information and allows the party to access or modify the data only following a set of predefined rules. In addition, the blockchain increases the speed of transaction processing.

Cloud technologies provide cost-effective and relatively easily scalable on-demand data processing, which minimizes the operating costs of financial institutions, creates a complementary information security system and increases the flexibility of management measures to meet the challenges of the external environment.

Automation is an essential component of digital transformation for financial companies. The financial services sector is based on transactions that generate large amounts of data, and therefore their automatic processing allows increasing the efficiency and profitability of your activities.

Biometric technologies include recognizing physiological or behavioral characteristics that can be used to authenticate a person by identifying characteristics unique to individuals. Among the methods currently used for verification are fingerprint scanning, voice authentication, face recognition, iris scanning, and gait recognition

The impact of digitalization on the development of major financial technologies is presented in Table 1.1.

The COVID-19 pandemic has also made its adjustments to the functioning of national financial systems worldwide, including the provision of digital financial services and the organization of the FinTech market. The introduction of numerous quarantine restrictions and social distancing has made it necessary to use digital channels to provide financial services and other services in the field of e-commerce.

Table 1.1. – The impact of digitalization on the development of major financial technologies

	Main financial services				Internal business processes	
	Payments and transfers	Financing	Capital management services	Insurance	Communication with clients	Security and protection
Influence of digital technologies	BC	BC, BD, CT	BC, BD, AI, VR	BC, BD, AI, BT	BC, BD, AI, VR	BC, BD, BT
Types of financial technologies	Online payment services, online transfer services, P2P payments, cryptocurrency, mobile and web wallets	P2P consumer lending, P2P business lending, crowdfunding, scoring model improvement	robo-surveying, financial planning applications, platforms for social trading, algorithmic exchange trading	digital insurance, platforms for reinsurance, improvement of underwriting, P2P insurance	chatbots, personal messages - reminders	data encryption, improvement of authentication and authorization procedures
BC – blockchain; BD – big data; CT – cloud technologies; AI – artificial intelligence, BT- biometric technologies; VR - virtual reality technologies.						

Source: compiled based on Rubanov (2019), Semenog & Tsyruk (2018), Marsh&McLennan companies (2019), European Commission (2020)

World Bank specialists conducted a thorough study of the impact of the COVID-19 pandemic on changes in the regulatory environment of FinTech companies in different countries. This study was based on data from a survey of representatives from 118 national regulatory authorities in the world's financial

sector. The study found an increase in the use of FinTech products in the world during the pandemic. In particular, 65% of respondents in developed countries reported an increase in digital payments and money transfers, while in developing countries – only 50 % (fig. 1.1). It is worth noting that the intensity of increasing services in digital insurance and investment is higher in emerging economies.

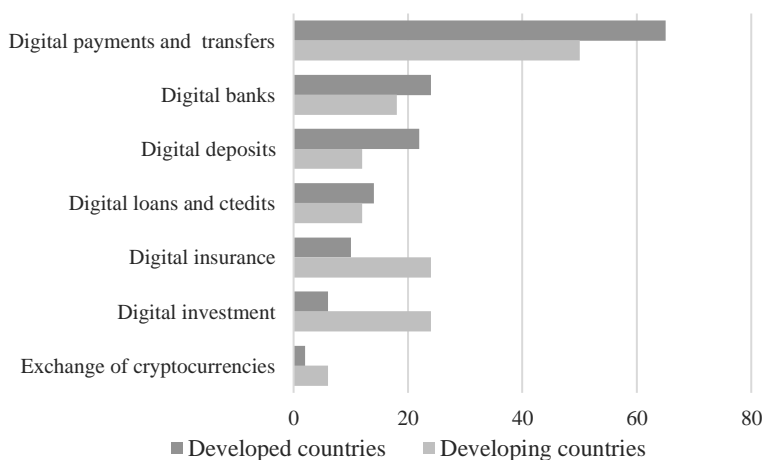


Figure 1.1. The share of respondents who reported an increase in the use of FinTech products during the pandemic

Source: compiled based on World Bank Group and the University of Cambridge (2020).

Despite the increased demand for FinTech services, the volume of investment in developing financial technologies in the world in 2020 decreased by 37.3% and amounted to \$105.3 billion (KMP, 2020). The sharp drop in financing for innovative financial technologies was due to a decrease in activity in the field of mergers and acquisitions. In contrast, venture financing remained at the level of the previous year.

One of the critical threats to digitalization is an increase in the frequency and scale of cyber fraud, which has negative

consequences for the stable functioning of financial service providers and their consumers, namely: loss of information, lack of access to it, unauthorized interference in the operation of corporate information systems, dissemination of personal financial information about customers, etc. In addition, the consequence of fraudulent actions of cybercriminals is reputational losses of financial institutions and a decrease in public confidence in the security and reliability of financial transactions both with the participation of a particular financial institution and the financial system as a whole. In particular, during the pandemic, the number of cybersecurity breaches among FinTech companies increased by an average of 17% (World Bank Group and the University of Cambridge (2020)).

Thus, the growth in the number of users of mobile devices, the spread of Internet penetration, the rapid increase in the volume of e-commerce, and the global pandemic have led to the rise in demand for digital financial products. Under these conditions, the active participation of the state in the development of digital technologies in the financial market is one of the main factors in the development of the digital economy. For the effective and safe development and functioning of the digital financial space, it is necessary to implement coordinated activities at the level of all participants, which will, on the one hand, maintain the stability of the financial system and protect consumer rights, and, on the other, contribute to the development and implementation of digital innovations.

1.2. Trends and patterns in cybercrime research: bibliometric analysis

In recent years, the proactive development of information technologies has forced the financial services market players to change their activities fundamentally, automate business processes as much as possible, and transfer the sale of services and products to the virtual plane. More and more cash payments are made in non-cash form using mobile or Internet banking from anywhere and at any time. This leads to the active development of e-commerce and other virtual services. It is necessary to highlight the formation of electronic money, which further expands the ability of business entities to implement financial transactions in cyberspace.

At the same time, the development of e-commerce has intensified a new type of fraud – cybercrimes, which are associated with the theft of information on bank accounts and bank cards, password cracking, ATM fraud, etc. These types of crimes lead to significant losses of specific financial institutions or clients and the state's economic security as a whole since criminals direct the illegally obtained financial resources to other more significant offenses.

The above situation determines the need to create an adequate cyber protection and information security system to protect the population, business entities, and the state from significant financial, material, and reputational losses. The specified problem certainly deserves the attention of domestic and foreign scientists, which should be implemented in numerous scientific articles and analytical reports of a theoretical, methodological, and practical nature. However, the development of this topic and its further formalization in scientific works should be conceptual, international, and high-quality, which may be indicated by the publication of the results obtained in journals indexed by the international databases Scopus and Web of

Science. However, it is fair to note that articles dealing with analyzing the relationship between cybercrime, the financial sector, and economic security are of particular practical value. This is because the consequences of cybercrimes are synergistically spreading to clients of financial institutions, directly to financial intermediaries, and the state in the framework of the accumulation of future threats and the shortfall in current budget allocations.

The globalization of financial markets and the internationalization of economic relations have narrowed the gaps between the time of the spread of the latest developments in different countries. Thus, the introduction of financial innovations in the central division of a global company almost immediately extends to its structural divisions. These phenomena intensify the development of both positive and negative processes in the financial sectors of national economies. In parallel with real financial processes, scientific work and practical scientific and methodological developments should also develop in this topic. However, scientific research, like international financial products, must be global. The development of modern economic science is impossible within the isolated territory of a particular country. Thus, the bibliometric analysis was based on the international database of scientific publications – Scopus. In our case, the Scopus database allows identifying various vectors of cybercrime research in the context of digitalization of the financial sector of the state economy.

Turning directly to the results of bibliometric analysis of significant scientific publications for 2012-2019, a map of the relationship of the concept of “cybercrime” with other scientific categories was formed. VOSviewer was the tool for implementing this stage. This allowed distinguishing seven groups, which in the figure are summarized using turquoise, purple, red, gray, blue, pink, and brown (fig 1.2). It should be

There are intersections between the identified groups, namely: the effectiveness of organizing the digital criminalistics process increases the level of crime detection and the volume of the evidence base, and the effective system for countering information crimes is an effective preventive tool for these types of crimes. Artificial intelligence and large databases analysis is an incentive for the effective fight against cybercrime, as it helps law enforcement agencies find criminals on the Internet, and for criminals, as it helps to analyze the security system of various internal systems of institutions and organizations. The Internet is the home of cybercriminals, e-commerce is the domain of cybercrimes, and digital storage is the basis for their implementation.

Based on the size of the rectangle describing the level of influence of the phenomenon in the study of aspects of cybercrime, it testified that the fundamental categories in the study of cybercrime in the context of digitalization of the financial sector of the state economy deal with such categories as “digital forensics”, “digital storage of data”, etc. This is evidenced by the data shown in Figure 1.3

Expanding the evolutionary-temporal perspective of the ongoing research, we analyze the contextual-temporal block of bibliometric analysis (fig 1.3). The main substantive determinants of cybercrime research in the context of financial digitalization. The color saturation in Figure 1.3 varies from rich blue (early publications) to yellow (modern publications).

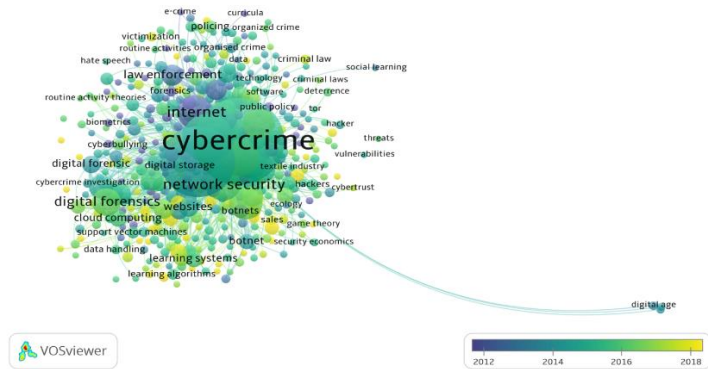


Figure 1.3. Visualization map of the contextual-temporal dimension of cybercrime research for 2012-2019 in Scopus-indexed journals

Thus, according to the results of the contextual-temporal analysis on cybercrime, three stages of change in the research vectors were established, in particular: in 2012-2013, scientists determined the legal framework for identifying cybercrimes on the Internet, since at the initial stages it was necessary to understand what exactly to interpret as cybercrimes. At the turn of 2014-2017, researchers' interest was focused on digital data storage and cloud technologies, as the latest technologies that allowed cybercriminals to expand the capabilities of their activities significantly. In 2018–2019, systems for learning and algorithmization began to occupy the central place as the most modern methods of optimizing any processes related to the activity of the population.

A logical continuation of the temporal bibliometric analysis of cybercrime research is its spatial component (fig. 1.4). Based on the data shown in Figure 1.4, it is feasible to identify seven major global research centers for this problem. Undoubtedly, the country leading the study of cybercrime in the context of the digitalization of the financial sector is the United States, an

equally important state is the United Kingdom. This group also included Austria, Italy, Norway, and Ukraine. Other much smaller groups of countries are Australia and China, India and Taiwan, Canada, Spain and Portugal, Indonesia, South Africa, Chile, and Switzerland.

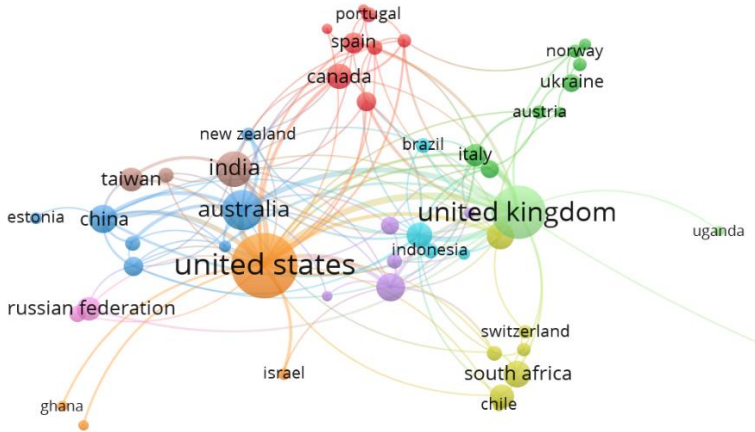


Figure 1.4. Territorial branching of the scientific bibliography of the “cybercrime” concept in recent years using the VOSViewerv.1.6.10 software

One of the final stages of bibliometric analysis is the study of the industry affiliation of the analyzed publications. Thus, based on Figure 1.5, we note that the vast majority of scientific publications on cybercrime are found in computer science (30%) and in the field of social sciences (37.88 %), almost the same number of empirical research is implemented in the field of economics, econometrics, and finance (29.79 %). At the same time, a significant proportion of publications on relevant topics relate to business, management, and accounting (24%). A significant amount of research devoted to cybercrime is observed in engineering (15%). The economic area that is interesting to us accumulates only 10% of all scientific research

dealing with cybercrime research. The share of scientific research devoted to cybercrime in all other industries does not exceed 6%. In turn, it should be noted that the category under study is complex and multifaceted, which determines the interdisciplinary nature of its research. This hypothesis is confirmed by Figure 1.5, which shows the intersection of the concepts of cybercrime and the financial sector.

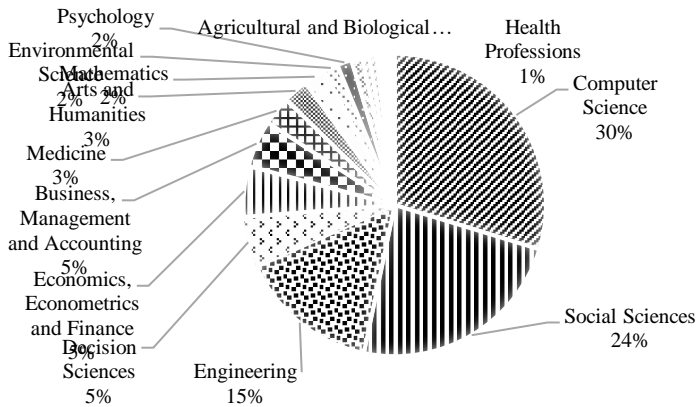


Figure 1.5. Structural industry affiliation of scientific publications on “cybercrime” in the Scopus database for 2012-2019.

Based on the data in Figure 1.6, we note that the main relationship between cybercrime and the financial sector occurs through the implementation of the following chains: through money laundering through cyberspace (blue cluster); through crimes in the field of e-commerce through hacking of information technologies that are used there (red cluster); through cyberattacks on personal computers and computer networks of individuals and legal entities (green cluster).

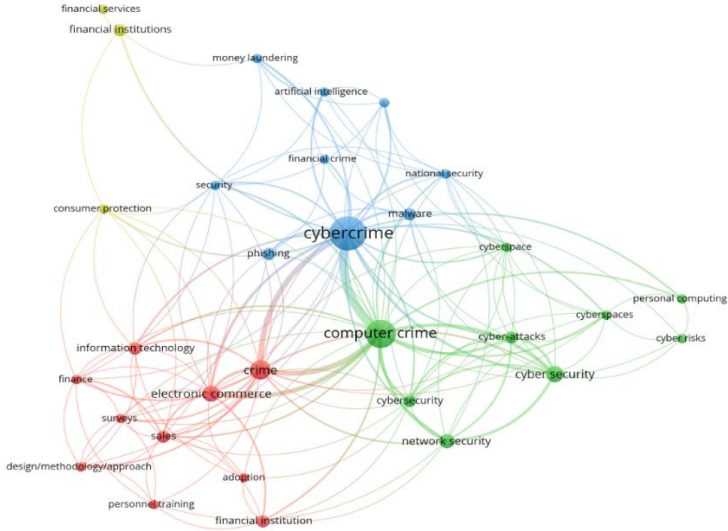


Figure 1.6. Scientific bibliography of the intersection of the concepts of “cybercrime” and “financial sector” for 2012-2019

To counter cyber threats, it is advisable to consider methods and ways of identification, and issues of the effectiveness of the information system. Considering the results of the bibliometric analysis of scientific publications for 2010-2020, a map of the relationship between the concept of “efficiency of cyber fraud” and other scientific categories was formed. VOSviewer was the tool for implementing this map. This allowed selecting seven clusters, which in Figure 1.7 are displayed as red, blue, green, blue, purple, yellow, and orange. It is worth noting that the larger size of the rectangle corresponds to a higher frequency of mentioning the category indicated in it as a key concept concerning the category “efficiency of cyber fraud”.

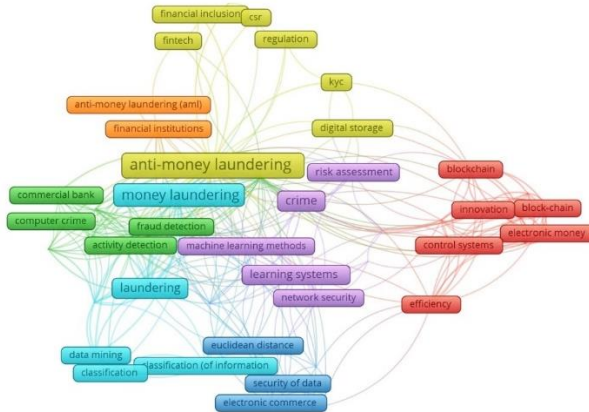


Figure 1.7. Scientific bibliography of the concept of “efficiency of cyber fraud” using the VOSviewer 1.6.15 software for the period from 2010 to 2020

Analyzing the results of the content-contextual block of bibliometric analysis, we note that the main body of scientific research is focused on identifying the relationship between the effectiveness of cyber fraud and combating money laundering (yellow cluster), crime and risk assessment (purple cluster), proceeds of crime (blue cluster), blockchain and governance (red cluster), computer crime (green cluster), financial institutions (orange cluster), and data security (blue cluster).

Thus, the fundamental categories in the study of the efficiency of cyber fraud are such categories as “countering money laundering”, “funds obtained by criminal means”, “crime”, etc. This is also proved by the data shown in Figure 1.8.

Based on the data in Figure 1.8, we note that the main relationship between the effectiveness of cyber fraud and the effectiveness of countering money laundering occurs through the implementation of the following chains: through the implementation of countering money laundering in the financial sector (yellow cluster); through cybercrime in the field of e-

commerce (red cluster); through cyberattacks on personal computers of individuals and legal entities (green cluster).

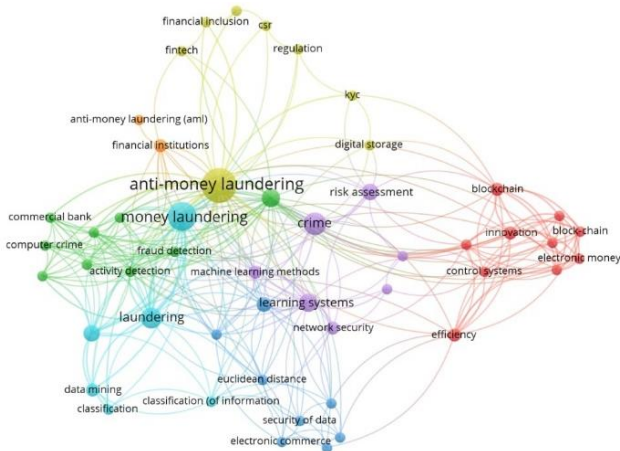


Figure 1.8. Scientific bibliography of the intersection of the concepts of “efficiency of cyber fraud” and “efficiency of anti-money laundering” for 2010-2020.

Expanding the research, we will analyze the contextual-time block of bibliometric analysis (Figure 1.9). The color saturation in Figure 1.9 varies from dark purple (early publications) to yellow (modern publications).

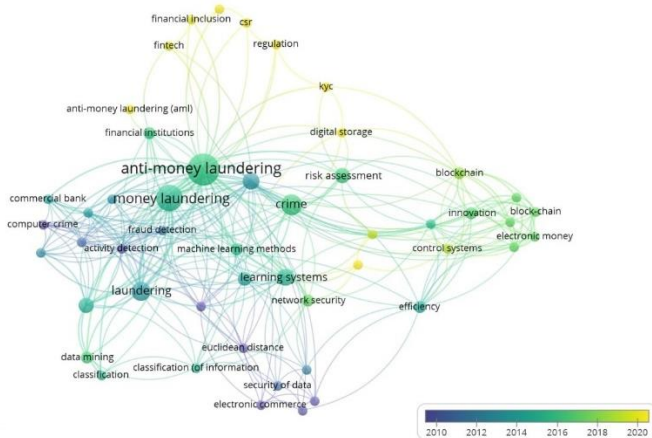


Figure 1.9. Visualization map of the contextual-temporal dimension of cyber fraud efficiency for 2010-2020 in Scopus-indexed journals

Thus, based on the results of a contextual-time analysis on cyber fraud efficiency, three stages of changing the research vectors were established. In particular, in 2010-2013, scientists tried to clearly understand and define how to interpret the concept of “cyber fraud” and its types. During 2014-2018, researchers were concerned with the issues of countering cyber fraud, assessing the risks of its occurrence, and establishing control over financial institutions in the framework of combating money laundering. In 2019-2020, with the development of electronic funds and blockchain, the focus began to be on financial technologies and countering cyber fraud in modern realities.

Summing up, we note that the study made it possible to more thoroughly formalize, within the context of contextual, evolutionary, and spatial analysis, the theoretical aspects of the spread of cybercrime in the context of the digitalization of the financial sector within the contextual, evolutionary, and spatial analysis of the state economy. It is established that the process

of studying the category of “cybercrime” is relatively young and concentrated in highly developed countries, such as the United States and the United Kingdom. In the economic sector, insufficient attention is paid to cybercrime. However, in recent years, due to the development of e-commerce and the digitalization of financial processes, this problem is becoming more urgent and causes significant damage to the economy.

1.3. Modern global trends in the financial cybercrime in the financial sector

The financial sector serves the economic relations of many participants: public and private institutions and organizations, their employees and clients, other financial intermediaries, etc. All these participants’ personal information, business data, and financial information are sent to financial institutions. However, given modern technological capabilities, some individuals and/or groups seek to use such resources for illegal purposes. There is a threat that confidential information can be broken and get to criminals through cybercrimes. Given the rapid use of digital products in a pandemic, the problem of cybercrime is becoming more acute. It is one of the main threats to the national reputation, security, and economy.

Dynamic digitalization of the economy makes banking and non-banking financial institutions more vulnerable to cybercrime. Financial institutions accumulate a significant amount of information from their customer. In case of the information security breach, confidential data may be used for illegal activities or sold on dark web sites, which may lead to the loss of business reputation of both financial institutions and their customers.

In 2020, the damage from cybercrimes in the United States was estimated at \$ 4.2 million, which is double that of 2018 (\$ 2.7 million). At the same time, in recent years, financial services

have been and remain the main target for cybercriminals (table 1.2).

Based on data on attacks and incidents of information security breaches from managed X-Force networks and publicly disclosed cybercrimes, IBM specialists established that the most vulnerable in 2020 were the spheres of finance, production, and energy.

Table 1.2. – Rating of vulnerability of activity to cybercrime in the period from 2018 to 2020

	2018	2019	2020	Changes, 2020/2018
Financial services	1	1	1	-
Industry	5	8	2	-3
Энергетика	10	9	3	-7
Retail	4	2	4	-
Professional services	3	5	5	+2
Administrative services	7	6	6	-1
Health care	8	10	7	-1
Media	6	4	8	+2
Transport	2	3	9	+7
Education	9	7	10	+1

Source: compiled based on IBM (2021)

In 2019, 39% of EU citizens who used the Internet faced security issues in the virtual space. The value of this indicator varies considerably in different member states: more than 50% in the UK and 10% in Lithuania (European Commission, 2020).

The most common forms of cyberattacks in the financial sector are ransomware, supply chain attacks, cryptojacking, and destructive attack (F-Secure, 2019).

One of the most common methods for stealing money directly from company accounts is the BEC scam (Business Email Compromise). The principle of the BEC scam is as follows: a cybercriminal misleads a company employee who has access to confidential information with the requirement to transfer funds to an account that allegedly belongs to the client or counterparty of the company, but the funds are redirected to the account of a

criminal organization. In 2020, losses from BEC scams and EAC scams (Email account Compromise), which are analogs to BEC scams for individuals, in the United States were estimated at \$1.8 billion (or 36% of the total amount of losses from cybercrime), while in 2019 – \$1.7 billion (or 48.57% of the total amount) (Federal Bureau of Investigation, 2020).

In the vast majority of cases, cyberattacks in the financial sector are carried out with the participation of such entities as (Nish et al., 2020):

- hackers and hacktivists motivated by curiosity, attention, revenge, violation of social justice norms, etc. Hackers usually use existing tools, basic scripts, or web resources;
- criminals and scammers whose aim is to obtain financial resources. This group of scammers can develop their own software tools for committing cybercrime;
- the state and its spies who carry out illegal activities for the purpose of defense, establishing geopolitical interests, influencing public opinion at the national and international levels, etc.

Table 1.3 shows the largest cybercrime groups that attack financial institutions globally.

Currently, most cryptocurrencies are used for money laundering after cybercrime. In 2018, 4 billion pounds were legalized in Europe with the help of cryptocurrencies. Cryptocurrency is inherently low-regulated and not controlled by a central authority, so financial transactions cannot be closely monitored.

Table 1.3 – The largest cybercrime groups that carry out attacks on financial institutions in the world

Name	Cyberattack difficulty level	Victims	Features of cyberattacks
Money Taker (Russian Federation)	the group uses its cyberattack tools, malicious software that will work even after a reboot, and customizes publicly available tools for its own needs.	banks, companies that provide services and/or technologies to financial institutions	more than 20 successful attacks on banks, financial institutions and law firms in the United States, Great Britain, and Russia.
Carbanak (Russian Federation)	the group uses malicious software that provides a wide range of features: authorization, reading bank card data, and personal information.	Banks, financial companies, e-commerce/retail companies	more than 300 successful attacks on banks, financial institutions, and retailers, including the Oracle system
Lazarus Group (North Korea)	the group has powerful capabilities, namely technologies for evading corporate cyber defense systems, three-level attacking servers, and encrypted communications.	Banks, financial companies, and government agencies	attack on Sony Pictures, program developer, attack on SWIFT (\$1 million), Central Bank of Bangladesh (\$81 million), etc.

Source: compiled based on Insights (2018)

According to the forecast of the analytical and consulting company Juniper Research, which specializes in researching trends in the development of the digital technology market, the losses of business companies from cyberattacks will exceed \$5 billion in 2024 (Securitymagazine, 2019). Strengthening cybersecurity measures for financial socio-economic entities of

the European Union is detailed in the strategic plan 2020-2024 of the Directorate-General for Informatics (DIGIT), which plays a coordinating role in the development of information technology and information and communication technology systems (European Commission). The main goal is to create a secure and modern digital environment that can provide reliable, cost-effective and secure infrastructure and services, keeping pace with new ways of working and collaborating that align with the expectations of employees, citizens, businesses and stakeholders.

The European Financial Stability Facility focuses on the need to approve new standards and oversight initiatives on cybersecurity in financial services. The three main areas of cyber defense that need to be addressed first are cyber risk identification, cyber risk management, and cyber resilience.

In 2020, the EU announced the launch of the EU Cybersecurity Strategy as a key component of shaping Europe's digital future and a plan to rebuild Europe, promote global and open cyberspace by strengthening cooperation. The European Commission has invested more than 63.5 million euros in four pilot projects (CONCORDIA, ECHO, SPARTA, CyberSec4Europe), which serve as the basis for creating a European network of cybersecurity expertise centers aimed at improving the system for countering cybercrime in various spheres of public life.

Security agencies are increasingly focusing on the ability of financial socio-economic entities (banks, financial institutions, firms, organizations, enterprises) to assess their propensity to cyber risk objectively. For example, the challenges banks face in terms of coherence in their internal control system are of great importance, especially given the growing focus on internal cyber control between different departments. The breach reporting rules, in line with the General Data Protection Regulation, add incentive for banks to strengthen their ability to quickly detect

cyberattacks and data breaches. Timely and clear management information about violations can speed up the search for a solution to the problem and get ahead of the cyber threat in advance (Deloitte, 2018).

In most jurisdictions, there is strong regulatory pressure to avoid turning a cyber threat into an “IT problem” and to take a holistic approach to minimizing and responding to cyber risks. However, the issue of ultimate responsibility remains unresolved. Some financial institutions take an approach involving appointing a non-executive director of cybersecurity responsible for security (Deloitte, 2018).

Resistance to cyber risks is due to the search for modern and powerful tools for testing potential cyber threats by individual financial institutions. For example, as part of an industry-wide initiative in the UK, the SIMEX 16 program was introduced, simulating the shutdown of British payments with gross settlement in real-time. After all, the UK, where payment for household services (47.6%) and financial services (27.3%) is made using mobile banking, is a very attractive platform for cyberattacks. However, despite the high costs of ensuring cybersecurity and taking a high position in terms of readiness for cyberattacks, the Bank of England, when simulating a major cyberattack on the British financial system, was not ready to resist it. Thus, the test revealed some alarming results: the largest number of financial institutions are not ready for a large-scale online attack based on identity information (identity-based attacks). Even small attacks have led to serious security breaches and a drop in core business processes.

The European Central Bank has made significant progress in shaping its understanding and ability to intervene in cyber security. Since the inception of the Enterprise Content Management (ECM) system in 2014, authorities have applied IT risk oversight best practices by engaging with national supervisors and senior IT risk professionals at banks. In recent

years, the European Central Bank has accumulated information to determine the main patterns of cyberattacks, both at the level of an individual financial institution and the system level. This information was used to develop tools to combat cyber fraud. Outside of banking supervision, the ECB is pursuing initiatives better to understand the cyber vulnerabilities inherent in the financial system and has developed a cyber strategy based on three pillars: financial institution cyber preparedness, sector resilience, and the involvement of strategic industry regulators.

In 2011, Germany adopted the German Cyber Security Strategy, according to which the Federal Government applied measures based on already established structures to the appropriate threat levels for the following strategic goals: 1) creation of an IT security system; 2) protection of infrastructure requires greater reliability of IT systems of citizens, as well as small and medium enterprises; 3) strengthening of IT security in public administration; 4) optimizing the operational cooperation of all government agencies and improving the coordination of protection measures against IT cases, the National Cyber Defense Center was established; 5) the creation of the National Cybersecurity Council, whose activities are aimed at identifying and eliminating the constructive causes of crises – an essential preventive tool in cybersecurity; 6) effective fight against crime in cyberspace – strengthening the capabilities of law enforcement agencies, the Federal Security Service in the field of IT and the economy in the context of overcoming cybercrime; 7) effective cooperation in cybersecurity in Europe and the world. Security in global cyberspace is achieved only through a set of agreed means and methods at the national and international levels; 8) the use of reliable information technology. All these measures confirm Germany's high level of preparation for the issue of cybersecurity and the quality of efforts to combat the latest technologies of cyber threats.

It is impossible not to consider the risk of the COVID-19 pandemic affecting digital security in today's conditions. Cybercriminals use the epidemic to make their attacks more successful. Since February 2020, there has been an increase in phishing attacks using COVID-19 content, including emails with the subject of the coronavirus in the subject field; letters purportedly sent from the names of leaders or institutions such as the World Health Organization; links or web applications that mimic legitimate initiatives. For example, Italian financial institutions recorded a 75% increase in phishing attacks in March 2020 (up from 25% in March 2019). One COVID-19 phishing campaign reached more than 10% of all organizations in the country, leading recipients to open a harmful attachment via email. In Germany, from March 2019 to March 2020, phishing attacks increased from 21% to 25% (OECD, 2020)

In 2020, the EU announced the launch of the EU Cybersecurity Strategy as a critical component of Shaping Europe's Digital Future and Recovery Plan for Europe, contributing to the development of global and open cyberspace through enhanced cooperation, and has allocated a total of 64 million euros to fund projects aimed at the best protection against cyberattacks.

Thus, modern financial institutions that offer banking products based on digital and mobile services face increasing pressure from malware, phishing, and fraudulent activities. The global COVID-19 pandemic has accelerated the transition to an online format for many business processes, financial services, and operations using digital services. At the same time, there is a significant increase in cyberattacks on government agencies, private companies, and individuals.

Cybersecurity is at the top of the European Commission's list of priorities: trust and security are central to the Digital Single Market Strategy while combating cybercrime is one of the three pillars of the European security program.

The scientific and practical world community is taking various measures to combat possible cyberattacks to detect, neutralize, minimize, and prevent cyber risks. The effectiveness of the use of mechanisms for countering cyber fraud directly depends, first, on identifying patterns in the implementation of cyberattacks from the experience of countries worldwide.

Today, when specific patterns are identified, specialists are processing large databases, which requires the development of specific models capable of processing significant information resources. One of the most effective solutions to this issue is using association rules and their adaptation to the study of the issues under consideration.

Association rules are a powerful technology for identifying relationships between related events or elements. They are described as: $X \rightarrow Y, X \cap Y \rightarrow \emptyset$. Moreover, any association rule can be represented by two main characteristics (Savchuk et al., 2020):

- support $supp(X \rightarrow Y)$ of association rule $X \rightarrow Y$ acts as a value equal to the ratio of the number of records $X \cup Y$ in database D to the total number of records in the database;
- confidence $conf(X \rightarrow Y)$ to the association rule $X \rightarrow Y$ acts as a value equal to the ratio of its support $supp(X \rightarrow Y)$ to the support $supp(X \rightarrow Y)$ of the set X.

Association rules that arise when analyzing multidimensional data are classified into the following types:

- interdimensional association rules, i.e., rules between attributes of different dimensions (Formula 1.1) (Horban et al., 2021):

$$(A_I^x \in D_I) \wedge \dots \wedge (A_J^y \in D_J) \rightarrow A_K^z \in D_K, \quad (1.1)$$

where I, J, K are certain size indices included in the association rule, and I, J, K = 1 ...n; where n – the number of dimensions, $D_I - I^{th}$ – a dimension, x, y, z – certain attributes of the dimension, and x, y, z = 1 ... m_i ; m_i – number of attributes I^{th} – measurements; A_I^x – specific attribute I^{th} – dimension.

–intra-dimensional association rules, i.e., rules of association within a single dimension (Formula 1.2) (Horban et al., 2021)**Ошибка! Источник ссылки не найден.:**

$$(A_I^x \in D_I) \wedge \dots \wedge (A_I^y \in D_I) \rightarrow (A_I^z \in D_I) \wedge \dots \wedge (A_I^v \in D_I), (1.2)$$

where $I = 1 \dots n$; where n – the number of dimensions, x, y, z, v – certain dimension attributes, and $x, y, z, v = 1 \dots m_i$; m_i – total number of attributes I^{th} – dimension.

–hybrid association rules, i.e., possible dependencies between dimensions, and certain operands can represent attributes of the same dimension (Formula 1.3) (Horban et al., 2021):

$$(A_I^x \in D_I) \wedge \dots \wedge (A_J^y \in D_J) \rightarrow (A_J^v \in D_J) \wedge \dots \wedge (A_K^z \in D_K), (1.3)$$

The formation of association rules is used for the following: identification and study of vulnerabilities in the processes under consideration, which will allow in the future in the early stages to minimize or even avoid additional material costs; enabling the management to determine the optimal amount of required resources and their effective allocation; automatic identification, correction, problem-solving and improvement of the processes under consideration.

We consider the obtained patterns of cyberattacks in EU countries based on the use of association rules through the following sequence of stages:

Stage 1. Formation of the input data structure for cyberattacks based on the logical generalization method. At this stage, data on the characteristics of cyberattacks during 2005-2020 is being collected and systematized (Table 1.4).

Table 1.4 – Fragment of the input data structure for cyberattacks

Name	Date	Victim country	Initiator country	Type of cybercrime	Sphere of industry
Attack on the Austrian Ministry of Foreign Affairs	2020	Austria	Russia	espionage	public
Attack on the Polish University of Military Studies	2020	Poland	Russia	deface	public
Attack on the Polish University of Military Studies	2020	Poland	Russia	deface	military
Attack on Central European aerospace and defense companies	2020	EU	North Korea	espionage	private
Attack on RedDelta	2018	Italy	China	espionage	public
...
Attack on Avast	2019	Czech Republic	China	espionage	private
Attack on think tanks in the US and Europe	2019	EU	Russia	espionage	private
Attack on the Czech Ministry of Foreign Affairs	2019	Czech Republic	Russia	espionage	public

Thus, the following can be stated based on the collected data on cyberattacks. Countries affected by cyberattacks include Austria, Poland, Italy, Germany, Lithuania, Latvia, Czech Republic, Norway, France, Belgium, Luxembourg, Netherlands, Switzerland, Bulgaria, Turkey, Denmark, Sweden, Denmark, Finland, Hungary, Spain. The countries that initiated cyberattacks on the territory of the European Union include Russia, China, North Korea, Vietnam, Lebanon, Iran, Kazakhstan, and the United States. In addition, the following types of cyberattacks were detected: espionage, damage or destruction of information, deface, sabotage, doxing, financial

theft, and denial of service. These cyberattacks were carried out on objects in various spheres: the public and private sectors, the military sector, and civil society.

The next step is to conduct an in-depth analysis of cyberattacks on the territory of the European Union based on the use of association rules. The STATISTICA 10 software product was used to implement this stage. The results obtained are presented in the form of Figure 1.10.

Summary of association rules (cyber-operations (EC).sta)						
Min: support = 20,0%, confidence = 10,0%						
Max. size of an itemset = 10						
	Body	==>	Head	Support(%)	Confidence(%)	Lift
1	Government	==>	Russia	40,32258	64,10256	1,135531
2	Russia	==>	Government	40,32258	71,42857	1,135531
3	Government	==>	Russia, Espionage	30,64516	48,71795	1,118708
4	Espionage	==>	Russia, Government	30,64516	36,53846	0,906154
5	Espionage, Government	==>	Russia	30,64516	59,37500	1,051786
6	Russia	==>	Espionage, Government	30,64516	54,28571	1,051786
7	Russia, Government	==>	Espionage	30,64516	76,00000	0,906154
8	Russia, Espionage	==>	Government	30,64516	70,37037	1,118708
9	Espionage	==>	Russia	43,54839	51,92308	0,919780
10	Russia	==>	Espionage	43,54839	77,14286	0,919780
11	Germany	==>	Espionage	24,19355	88,23529	1,052036
12	Espionage	==>	Germany	24,19355	28,84615	1,052036
13	China	==>	Espionage	24,19355	93,75000	1,117788
14	Espionage	==>	China	24,19355	28,84615	1,117788
15	Private sector	==>	Espionage	35,48387	84,61538	1,008876
16	Espionage	==>	Private sector	35,48387	42,30769	1,008876
17	Government	==>	Espionage	51,61290	82,05128	0,978304
18	Espionage	==>	Government	51,61290	61,53846	0,978304

Figure 1.10. Results of analysis of cyberattacks on the territory of the European Union using association rules

Based on the data obtained by constructing association rules shown in Figure 1.10, the following conclusions can be drawn: in 77.14% of cases, espionage is carried out by intruders from Russia, in 88.24% – from Germany, in 93.75% – from China. It was found that 84.62% of espionage is observed in the private sector, 82.05% in the public sphere. At the same time, the share of observations for which espionage is carried out from Russia is 43.55%. The share of observations for which espionage is carried out from both Germany and China is 24.19% of the sample. In 76% of cases, espionage is carried out from Russia in

the sphere of public activities. Turning to the analysis of the frequency of detected cases of cyberattacks, which is a significant addition to the above association rules (Figure 1.11).

Frequent itemsets computed (cyber-operations (EC).sta)				
Min: support = 10,0%, confidence = 10,0%				
Max. size of an itemset = 10				
	Frequent itemsets	Number of items	Frequency	Support(%)
1	(Espionage)	1,000000	52,00000	83,87097
2	(Government)	1,000000	39,00000	62,90323
3	(Military)	1,000000	9,00000	14,51613
4	(EU)	1,000000	7,00000	11,29032
5	(Private sector)	1,000000	26,00000	41,93548
6	(Civil society)	1,000000	9,00000	14,51613
7	(Germany)	1,000000	17,00000	27,41935
8	(France)	1,000000	7,00000	11,29032
9	(Espionage, France)	2,000000	7,00000	11,29032
10	(Espionage, Germany)	2,000000	15,00000	24,19355
11	(Espionage, Private sector, Germany)	3,000000	7,00000	11,29032
12	(Espionage, Government, Germany)	3,000000	8,00000	12,90323
13	(Espionage, Civil society)	2,000000	7,00000	11,29032
14	(Espionage, Private sector)	2,000000	22,00000	35,48387
15	(Espionage, Government, Private sector)	3,000000	6,00000	9,67742
16	(Espionage, EU)	2,000000	7,00000	11,29032
17	(Espionage, Military)	2,000000	7,00000	11,29032
18	(Espionage, Government)	2,000000	32,00000	51,61290
19	(Government, Germany)	2,000000	9,00000	14,51613
20	(Government, Civil society)	2,000000	6,00000	9,67742
21	(Government, Private sector)	2,000000	7,00000	11,29032
22	(Government, Military)	2,000000	7,00000	11,29032
23	(Private sector, Germany)	2,000000	8,00000	12,90323

Figure 1.11. Frequency of detected cases of cyberattacks

Analysis of Figure 1.11 allows stating that the largest share of cybercrime (62.90%) occurs in state structures. The next most frequent industry is the private sector (41.94%). The lowest share of cybercrime occurs in the military and public spheres and accounts for 14.52%.

Graphical representation of cause-and-effect relationships between cyberattacks is based on the use of visualization and graphic design methods. As part of this stage, a graph of the association rules identified at the second stage is built, shown in Figure 1.12, which allows getting a visual representation of the entity (the Head axis means the cause, the Body axis – the

effect), the degree of confirmation of the identified relationships (the color of the corresponding ellipse), as well as the proportion of the studied population, for which the corresponding association rule is characteristic (the size of the ellipse).

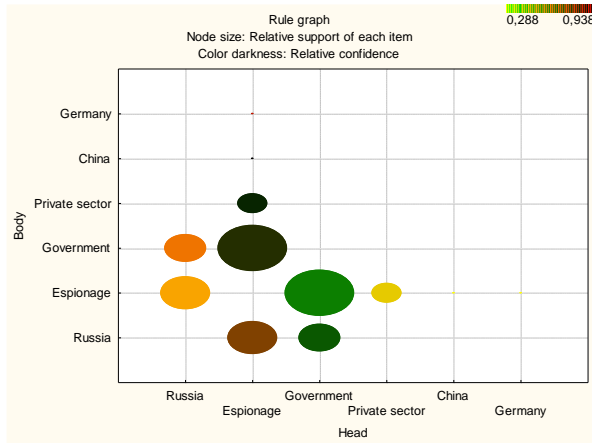


Figure 1.12. The graph of association rules

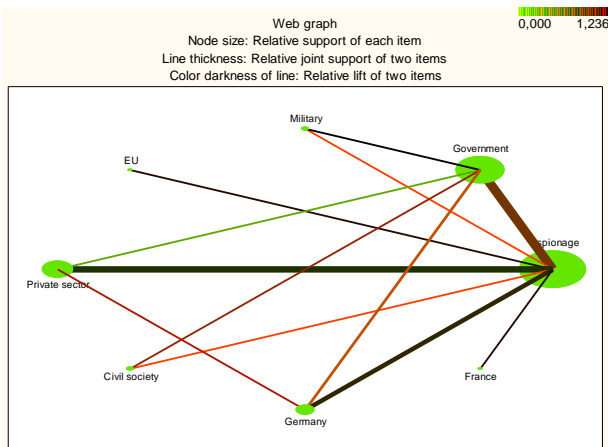


Figure 1.13. Web graph of support for identified association rules in the context of cyberattacks carried out within EU countries

Turning to the analysis of Figures 1.12 and 1.13, the highest frequency of detected cases of cyberattacks (83.87%) is espionage. Among the countries that have become victims of cybercrime, it is necessary to mention Germany, which accounts for 27.42% of cases, while for France, this figure is at the level of 11.29% (which was due to espionage). On average, 11.29% of EU countries were affected by cyberattacks between 2005 and 2020.

It should be noted that cyberattacks, in which personal, commercial, and financial information is lost, cause significant losses for participants in the financial and economic system. In the absence of innovative, improved measures to counter such cybercrime, the scale of these illegal acts in the world is constantly growing. It causes severe threats to the economic security of countries.

The chosen methodology makes it possible to process large databases by forming specific economic algorithms, which contributes to the search for a solution to the problem with low time costs. This will further enable countries to make effective decisions to anticipate cyber threats, counter cyberattacks, and ensure the national security of EU countries.

Ensuring the security of information technologies of financial institutions and their databases is an ever-growing challenge for the top management of both financial institutions and the national regulator. Although the program is gradually becoming more secure, and developers are creating new approaches to cybersecurity, attackers are also improving malicious technologies. To counter cyber threats in the economy's financial sector, it is advisable to identify trigger factors leading to an increase in cyber fraud in financial services.

The main purpose of the research is to improve cyber security management through analyzing large data volumes of information that helps to identify potential cyber threats at an early stage. The paper proposes a scientific and methodological

approach to formalizing the factors of the rapid spread of cyber fraud based on SVM machine learning methods. 21 European countries were selected as the object of the research. The source of primary information was data from Comparitech (2020), European Commission. (2020). Statistica software package for statistical analysis was used to carry out mathematical calculations.

Starting from the basic subject and issues as well as the research objectives of this study, there have been defined the following hypotheses:

H1: There is a significant correlation between online financial activities factors and cyberattacks.

H2: Digital skills factors have a significant influence on combating cyberattacks.

Testing the above hypotheses involves performing the following consequent steps:

–Collection and processing of statistical data characterizing the volume of cybercriminal operations in the context of various cyberattack methods.

To reflect the intensity of cyberattacks in the context of European countries, the following indicators were used:

- share of mobiles infected with malware, % (I₁);
- share of users attacked by mobile banking trojans, % (I₂);
- users attacked by mobile ransomware trojans, % (I₃);
- share of users attacked by banking malware, % (I₄);
- share of users attacked by ransomware trojans, % (I₅);
- share of computers infected with at least one malware attack, % (I₆);
- share of computers facing at least one local malware attack, % (I₇);
- share of mobile users attacked via web sources, % (I₈);
- share of telnet attacks by originating country, % (I₉);
- share of attacks by cryptominers, % (I₁₀);
- share of SSH-based attacks by originating country, % (I₁₁);

- share of all Spam Emails by Originating Country (I₁₂);
- share of countries targeted by malicious mailings, % (I₁₃);
- share of computers attacked by phishing (yearly), % (I₁₄).

Systematized data on cases of cyber fraud in the context of various methods of their implementation using data from Comparitech (2020) are presented in the Table 1.

Based on the types of cyberattacks analyzed in Table 1.5, we note that the largest victim countries in 2020 were Spain, Portugal, and Latvia, while the lowest number of cyberattacks was recorded in countries such as Denmark, Sweden, and Ireland. In particular, 19.73% of computers in Portugal were attacked by Internet scams such as phishing, while in Denmark, it was only 3.26%. The shift to telecommuting and the intensive use of e-services caused by the COVID-19 pandemic has led to an increase in cyber fraud worldwide. As for the European countries, the largest number of detected malicious files associated with the Covid-19 pandemics were found in Spain, Italy, and Germany.

Table 1.5 – Information on the state of cybercrime in European countries as of 2020 (fragment)

Indicator	Top 3 countries			Bottom 3 countries		
	1	2	3	1	2	3
I ₁	Romania (5,04%)	Spain (4,31%)	Slovakia (3,5%)	Finland (1,06%)	Denmark (1,33%)	Germany (1,63%)
I ₄	Portugal (0,9%)	Greece (0,5%)	Bulgaria (0,5%)	Ireland (0,1%)	Denmark (0,1%)	Hungary (0,2%)
I ₁₀	Latvia (0,73%)	Bulgaria (0,56%)	Slovakia (0,5%)	Denmark (0,11%)	Germany (0,12%)	Romania (0,14%)
I ₁₂	Germany (10,97%)	France (5,97%)	Netherlands (4,00%)	Denmark (0,07%)	Slovakia (0,19%)	Sweden (0,19%)
I ₁₄	Portugal (19,73%)	France (17,9%)	Belgium (16,4%)	Denmark (3,26%)	Sweden (3,35%)	Ireland (3,42%)

Bringing input indicators to a single comparable form. To standardize static indicators, the Z-normalization method was used, which provides for weighting the deviation of the actual

level of each indicator from the average level for the set of countries under consideration to the standard deviation, according to the following formula:

$$k_{cj} = \frac{I_{cj} - \bar{I}_j}{\sigma_j} \quad (1.4)$$

where k_{cj} – the standardized value of the j -th indicator of the spread of cyber threats in the context of the c -th country;

I_{cj} – the actual value of the j -th indicator of the spread of cyber threats in the context of the c -th country;

\bar{I}_j – arithmetic mean of the j -th indicator of the spread of cyber threats on the set of values of the considered set of countries;

σ_j – the average square deviation in the context of the j -th indicator of the spread of cyber threats on the set of values of the considered set of countries.

Aggregation of standardized levels of indicators of the spread of cyber threats to a single integral indicator. Analysis existing approaches to the construction of an integral indicator, the group method of data handling by Ivakhnenko is used, i.e., calculating the sum of the sums of squares of standardized values of input indicators as follows:

$$IK_c = \sum_{j=1}^J \sum_{j=1}^J (k_{cj})^2 \quad (1.5)$$

where IK_c – integral index of cyber threats in the context of the c -th country

The existing array of statistical data was standardized based on the Z-normalization method (formula 1.4), which made it possible to aggregate into a single generalizing indicator – the

cyber threat index. The results of calculating the cyber threat index using Formula (1.5) are shown in Figure 1.14.

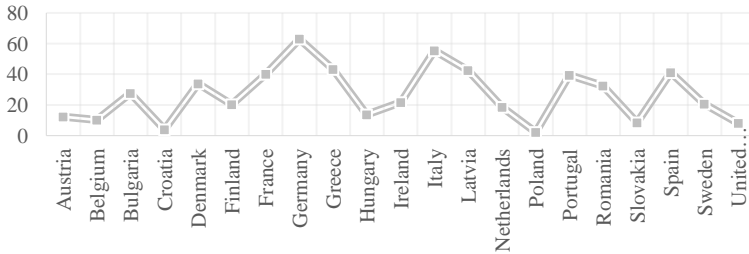


Figure 1.14. Dynamics of the cyber threat index in European countries in 2020

The calculations demonstrated the unevenness of the implementation of cyberattacks in the context of European countries since the cyber threat index in 2020 varies from 2.4 conventional units up to 74.9 conventional units. Based on the aggregation of 15 input indicators characterizing various ways of carrying out fraud in the information space, it was found that the highest level of cyber threats in 2020 was observed in countries such as Spain (74.9 conventional units), Germany (63.3 conventional units), Italy (57.7 conventional units), Latvia (42.9 conventional units), and France (40.2 conventional units).

Identification of potential factors influencing the spread of cyber fraud and collection of statistical data on them. To formalize the drivers of cybercrime spread, it is proposed to use the following variables:

- people who used the Internet to use online banking (Z1);
- mobile broadband index (Z2) calculated as the weighted average of the normalised indicators: 4G coverage (25%), Mobile broadband take-up (25%) and 5G readiness (50%);
- Internet user skills (Z3) calculated as the weighted average of the normalised indicators: At least Basic Digital Skills (33%),

Above basic digital skillst (33%) and At least basic software skills (33%);

- advanced skills and development (Z4) calculated as the weighted average of the normalised indicators: ICT Specialists (33%), Female ICT specialists (33%) and ICT graduates (33%);
- activities online (Z5) calculated as the weighted average of the normalised indicators: News (16.6%), Music, Videos and Games (16.6%), Video on Demand (16.6%), Video Calls (16.6%), Social Networks (16.6%), and Doing an online course (16.6%);
- business digitisation (Z6) weighted average of the normalised indicators: Electronic Information Sharing (16.7%), Social media (16.7%), Big data (33.3%) and Cloud (33.3%).

In 2020 the values of the above indicators in terms of European countries are given in Table 1.6.

Table 1.6. – Determinants of the spread of cyber threats in EU countries

	Z1	Z2	Z3	Z4	Z5	Z6
Austria	71,54	50,15	64,49	48,97	41,82	35,75
Belgium	78,85	34,16	58,29	42,49	48,29	67,34
Bulgaria	12,62	31,33	25,80	42,03	40,90	20,54
Croatia	58,75	33,70	54,31	44,00	53,85	39,57
Denmark	93,53	57,93	71,29	51,26	65,33	65,57
Finland	95,20	76,59	76,46	80,42	69,34	79,35
France	73,33	51,50	54,74	40,13	33,39	46,93
Germany	65,72	65,31	66,92	45,92	45,46	38,95
Greece	40,33	33,02	47,25	22,33	49,34	34,48
Hungary	58,11	61,13	45,91	37,76	53,92	21,78
Ireland	74,59	50,82	53,32	59,48	53,39	64,66
Italy	48,05	63,36	40,08	24,83	40,11	34,11
Latvia	83,10	56,13	41,30	28,74	45,53	30,45
Netherlands	94,36	34,45	78,17	50,15	63,36	75,68
Poland	58,76	46,32	40,93	33,61	41,46	25,03
Portugal	55,67	35,42	51,80	23,73	48,53	40,50
Romania	11,35	40,73	27,23	39,08	35,70	25,41
Slovakia	66,11	48,81	50,15	33,47	40,57	33,25

Continuation of table 1.6

Spain	60,50	49,39	57,06	38,06	56,31	43,44
Sweden	86,59	49,43	71,90	71,55	68,78	62,11
United Kingdom	81,30	46,77	74,46	51,55	62,98	58,61

Source: European Commission (2020b)

A more detailed in-depth analysis of the determinants of the spread of cyber threats will allow the Figure 1.16, which shows the highest volatility of the indicator Z1 (share of the population using online banking), the value of which in 21 countries ranges from 11 to 95. The lowest volatility is the Z5 indicator (online activity indicator), which ranges from 33 to 69. These conclusions can also be drawn by analyzing the descriptive statistics of the determinants of the spread of cyber threats in Europe by 2020, as shown in Figure 1.15-1.16.

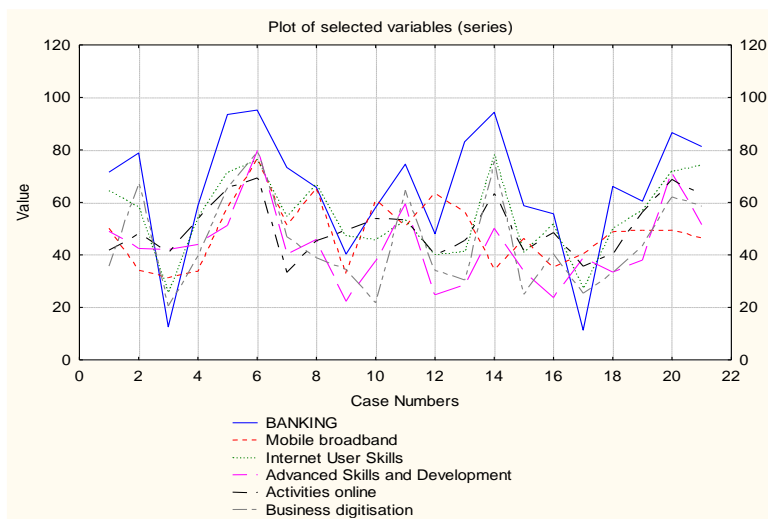


Figure 1.15. Variation of the indicators

Variable	Descriptive Statistics (cyber threat index SVM.sta)								
	Valid N	Mean	Median	Mode	Sum	Minimum	Maximum	Std.Dev.	Coef. Var.
Banking	21	65,15940	66,10540	Multiple	1368,348	11,34820	95,20090	23,23360	35,65656
Mobile broadband	21	48,40276	49,38920	Multiple	1016,458	31,33480	76,58660	12,27426	25,35860
Internet User Skills	21	54,85063	54,30810	Multiple	1151,863	25,80109	78,17180	15,14183	27,60557
Advanced Skills and Development	21	43,31189	42,03000	Multiple	909,550	22,32950	80,42470	14,68055	33,89505
Activities online	21	50,39805	48,53089	Multiple	1058,359	33,38751	69,33851	10,77735	21,38445
Business digitisation	21	44,92810	39,56651	Multiple	943,490	20,54443	79,34860	18,14500	40,38675
cyber threat index	21	28,57143	21,82482	Multiple	600,000	2,41716	74,92434	20,09377	70,32818

Figure 1.16. Descriptive statistics of the indicators

Based on Figure 1.16, it can be stated that among the 7 determinants of cyber threat spread in the context of only 3 (level of mobile broadband access, level of Internet skills, online activity) there is homogeneity of the sample, as the coefficient of variation does not exceed 33%. In terms of other determinants, especially the integrated cybersecurity index, there is a fairly high unevenness and diversity of countries.

The next stage of the proposed scientific and methodological approach is to determine the determinants of the spread of cyber threats by building 8 SVM machine learning models: two types (epsilon-SVM regression and nu-SVM regression) in the context of four specifications of reference vectors: linear, polynomial, radial basis functions (RBF) and sigmoid. In regression, it is necessary to estimate the functional dependence of the dependent variable y on the set of independent variables x . It provides, like other regression problems, that the relationship between the independent and dependent variables is given by a deterministic function f , taking into account some additive noise:

$$y = f(x) + noise \quad (1.6)$$

SVM regression type 1. For this type SVM model:

$$\frac{1}{2}w^T w + C \sum_{i=1}^N \xi_i + C \sum_{i=1}^N \xi_i^* \rightarrow \min \quad (1.7)$$

$$\begin{cases} w^T \phi(x_i) + b_i - y_i \leq \varepsilon + \xi_i^* \\ y_i - w^T \phi(x_i) - b_i \leq \varepsilon + \xi_i \\ \xi_i^*, \xi_i \geq 0, i = 1, \dots, N \end{cases}$$

where C – the capacitance parameter (used for grid cross-validation).

SVM regression type 2. For this type SVM model:

$$\frac{1}{2}w^T w - C \left(\nu \varepsilon + \frac{1}{N} \sum_{i=1}^N (\xi_i + \xi_i^*) \right) \rightarrow \min \quad (1.8)$$

$$\begin{cases} w^T \phi(x_i) + b_i - y_i \leq \varepsilon + \xi_i \\ y_i - w^T \phi(x_i) - b_i \leq \varepsilon + \xi_i^* \\ \xi_i^*, \xi_i \geq 0, i = 1, \dots, N, \varepsilon \geq 0 \end{cases}$$

Using the reference vector method, it is possible to construct various types of functional dependencies between variables (linear, polynomial, radial basis, sigmoid):

$$\phi = \left\{ \begin{array}{ll} x_i \cdot x_j & \text{Linear} \\ (\gamma x_i \cdot x_j + \text{coefficient})^d & \text{Polynomial} \\ \exp(-\gamma(x_i - x_j)^2) & \text{RBF} \\ \tanh(\gamma x_i \cdot x_j + \text{coefficient}) & \text{Sigmoid} \end{array} \right\} \quad (1.9)$$

where d – the degree of the polynomial kernel;

γ – gamma parameter for polynomial, RBF and sigmoid nuclei;

coefficient – coefficient for polynomial and sigmoid nuclei.

Based on comparing the actual and predicted levels of the cybersecurity spread determinants and the cyberthreat index for the test sample of countries, we calculate the standard deviation (Table 1.7).

Table 1.7. – Comparison of 8 built SVM models

	Denmark	Italy	Latvia	Nether-lands	Slovakia	Spain	Standard deviation
Cyberthreat Index	63,33	57,71	42,91	18,81	8,90	74,92	
Epsilon-SVM regression: Linear	23,92	32,11	9,87	36,23	19,74	32,50	21,15
Epsilon-SVM regression: Polynomial	24,08	26,02	25,38	17,44	25,21	24,81	20,69
Epsilon-SVM regression: Radial	17,09	27,93	19,68	23,59	21,38	22,23	21,24
Epsilon-SVM regression: Sigmoid	27,69	32,03	22,62	21,15	24,34	29,82	20,15
Nu-SVM regression 2: Linear	33,39	42,77	21,84	16,20	25,87	27,74	20,51
Nu-SVM regression 2: Polynomial	26,03	26,03	25,98	15,91	25,39	24,52	20,71
Nu-SVM regression 2: Radial	29,48	37,48	28,72	16,45	28,24	24,30	20,20
Nu-SVM regression 2: Sigmoid	27,84	33,34	28,04	19,77	27,46	25,30	20,00

Thus, the sigmoid nu-SVM regression model is the most accurate for determining the determinants of the spread of cyber threats. This model has the following characteristics: the number

of independent variables in the model is 6, the model type is nu-SVM regression, the Kernel type is sigmoid, the number of reference vectors that allow the pattern recognition algorithm is 9, among which the boundary ones are 3 (Table 1.8).

Table 1.8. – SVM model specification for determining the determinants of cyber threats spread

№	Weights	Z1	Z2	Z3	Z4	Z5	Z6
1	-9,9177	0,8050	0,0624	0,6413	0,3470	0,4146	0,7958
2	-10,0000	0,5653	0,0524	0,5627	0,3730	0,5692	0,3235
3	9,2885	0,9800	0,5878	0,8980	0,4980	0,8886	0,7657
4	9,2038	0,7392	0,4457	0,5712	0,3063	0,0000	0,4487
5	10,0000	0,3456	0,0373	0,4235	0,0000	0,4438	0,2369
6	-1,8307	0,5576	0,6584	0,3970	0,2656	0,5710	0,0210
7	-10,0000	0,5655	0,3311	0,2987	0,1942	0,2245	0,0762
8	9,0077	0,5286	0,0902	0,5133	0,0241	0,4212	0,3393
9	-5,7516	0,8343	0,3410	0,9606	0,5029	0,8230	0,6473

Based on the results of the calculations, we note the following: among the 9 constructed reference vectors, vectors 2, 5, and 7 have the most significant weight in absolute value. Thus, to determine the determinants of the spread of cyber threats, in the context of each reference vector, we will calculate the arithmetic mean value for the three selected reference vectors. Thus, we get the following ranking of the importance of the determinants of the spread of cyber threats:

Thus, having built a neural model using the reference vector machine based on data from the European Union countries, we found a strong functional relationship between the level of cyber threats and factors such as the proportion of the population using online banking (0.49), an indicator of the level of skills on the Internet (0.42), and an indicator of online activity (0.41).

So, financial market participants need confidence in data security, the ability to minimize cyber risks and defend against

cyber threats. Increasing financial damage from cyberattacks, combined with the growing volume of information data stored in the network infrastructure necessitate the development of new tools to ensure information security. To combat cybercrime, a combination of traditional and non-traditional strategies and tactics using digital information technology. To make managerial decisions in the field of cybersecurity, the development of tools is gaining ground, which involves the accumulation of large amounts of information and the use of modern approaches in the field of artificial intelligence. Having built a neural model using the reference vector machine based on data from the European Union countries, we found a strong functional relationship between the level of cyber threats and factors such as the proportion of the population using online banking (0.49), an indicator of the level of skills on the Internet (0.42), and an indicator of online activity (0.41). An important step in the cybersecurity system is the timely identification of cyber threats and taking rapid action to neutralize them. In the conditions of constantly growing cyber risks it is expedient to create conditions for ensuring cyber resilience by strengthening the control of the level of banking and financial operations performed without the consent of clients; training of employees responsible for information protection and response to cyber threats; informing employees who are not involved in the organization of cybersecurity, as well as bank customers; use the technology of cryptographic information protection.

1.4. Assessing the cyber vulnerability of financial service consumers

Expanding digital opportunities and improving customer experience is an inevitable choice for banks and financial institutions that want to remain competitive and meet customer needs over the next decade. At the same time, this leads to an

increase in the number of cybercriminal attacks. Insights, a cyber threat intelligence company, reported that 25% of all malware attacks target banks and other financial services companies, far more than any other industry.

The safe and efficient functioning of the financial market infrastructure is essential for maintaining and promoting financial stability, increasing public confidence in financial institutions. Today, the issue of ensuring the information security of financial market entities is gradually becoming a priority vector of activity of both the national regulator and financial service providers. In March 2017, the European Central Bank's Board of Governors approved the Eurosystem Cyber Resilience Strategy for Financial Market Infrastructures, which aims to improve the information security of financial institutions in the European Union and strengthen cooperation between national regulators, financial institutions, and counterparties to counter cyber threats.

The National Bank of Ukraine is also strengthening control over the implementation by financial institutions of measures to ensure cyber protection and information security. After adopting the Resolution of the Board of the National Bank of Ukraine No. 4 dated January 16, 2021, financial institutions are obliged to conduct an annual self-assessment to assess their information security risks and submit this information to the national regulator. These regulatory measures will contribute to bringing domestic legislation in the field of cyber protection of the financial system to international standards and principles, namely the Guidance on cyber resilience for financial market infrastructures of the Bank for International Settlements (2016) and Cyber Resilience Oversight Expectations for Financial Market Infrastructures of the European Central Bank (2018). Moreover, starting from August 2021, the National Bank of Ukraine and the cyber police will cooperate to strengthen countering cybercrimes in the financial sector.

In the context of rapidly growing cyber threats and a variety of forms of their implementation, an essential condition for effectively combating them is the development of communication, coordination, and partnerships in the field of cyber protection between financial institutions and the national regulator, which implies the exchange of relevant information on cyber threats between banks.

In current conditions, financial institutions in some countries conclude a preliminary agreement with clients, which clearly indicates the necessary method of identifying and authenticating the client when confirming a financial transaction (Bank for International Settlement, 2018).

Given the massive transition of users to online payment services during the quarantine period, an important priority for the central bank is the need to protect them as much as possible from possible information security incidents. One of the most vulnerable links in ensuring information security of the financial system is consumers of financial services, which has led to the relevance of the chosen research area.

The purpose of the proposed scientific and methodological approach is to assess the integral level of cyber vulnerability of financial service consumers in different European countries, which provides for the implementation of the following stages:

- collection and processing of statistical data that directly and indirectly characterize the degree of awareness of clients of financial institutions about possible cyber fraud and ways to protect against cyber threats in the implementation of financial transactions;
- prioritizing variables selected in the previous step;
- selection of a synthesizing function to determine the generalizing level of cyber vulnerability of financial services consumers.

The initial stage of the developed scientific methodological approach is the collection and systematization of indicators that

directly and indirectly characterize the vulnerability of financial services consumers to cyber threats (awareness of the signs of suspicious cyber fraud, cyber protection methods, information channels about cyberattacks). The source of the primary data was a survey of citizens of the European Union regarding their attitude to cybersecurity issues, which was conducted in 2020 (European Commission, 2020). For the needs of this study, 17 indicators were selected that exclusively relate to financial transactions and the protection of personal data, namely: the share of the population worried about the security of online payments (R1); the proportion of the population who are worried about the unauthorized use of their personal data (R2); the share of the population who changed their Internet banking password in the last 12 months (R3); proportion of the population indicating low awareness of cybercrime risks (R16); the proportion of the population who know at least one method of reporting cybercrime (R17), as well as a group of indicators reflecting the preventive measures of citizens to increase their level of protection in the virtual space (R4-R15): the proportion of the population that has reduced the number of Internet banking operations (R4); the proportion of the population that less frequently enters personal information on websites (R5); the proportion of the population that changed the security settings (for example, in the browser, social network, search engine) (R6); proportion of the population visiting only those websites that they know and trust (R7); the proportion of the population using different passwords for different sites (R8); the proportion of the population that does not open emails from unknown people (R9); proportion of population with current antivirus software installed (R10); the proportion of the population who canceled an online purchase due to suspicions about the seller or website (R11); the proportion of the population using more complex passwords than before (R12); proportion of the population using biometric functions (e.g., face recognition,

fingerprint) (R13); the proportion of the population not connected to the Internet through unsecured access points (R14); percentage of the population not concerned about Internet safety (R15). 30 European countries were selected as the object of the study. Summary information in the context of 17 indicators as of 2020 is presented in the appendix, and the main results are shown in the Table 1.9.

Table 1.9. – Information on citizens’ awareness of cyberattacks and ways to protect against them in European countries in 2020

	EU average	Top 3 countries with the highest rates			Top 3 countries with the lowest rates		
		1	2	3	1	2	3
R1	41%	Ireland (52%)	Spain (49%)	Great Britain (46%)	Poland (24%)	Estonia (25%)	Denmark (27%)
R2	46%	Cyprus (60%)	Greece (57%)	Germany (57%)	Hungary (31%)	Slovakia (31%)	Poland (32%)
R3	30%	Latvia (49%)	Great Britain (42%)	Austria (41%)	Romania (10%)	Hungary (13%)	Portugal (15%)
R16	22%	Malta (44%)	Greece (40%)	Austria (34%)	Romania (14%)	Spain (14%)	Denmark (14%)
R17	17%	Sweden (30%)	Austria (29%)	Netherlands (25%)	Portugal (5%)	Latvia (7%)	Greece (8%)

According to a survey of citizens of the European Union regarding their level of awareness of the importance of protecting financial transactions in the virtual space, the following facts were established: about half of the population of Ireland, Spain, and the UK are worried about the security of their online payments; in Cyprus, 60% of the population is concerned about the unauthorized use of their personal data for settlements.

In the countries of the European Union, on average, 22% of the population note a low level of awareness of the risks of cybercrime, while the highest values are in countries such as

Malta (44%), Greece (40%), Austria (34%), and the lowest – Romania, Spain, Denmark (14%).

An essential element in countering cybercrime is the timely notification of violations to the relevant regulatory authorities. However, only 17% of Europeans know about at least one way to report cybercrime. The highest rates are in Sweden (30%), Austria (29%), The Netherlands (25%), and the lowest – Portugal (5%), Latvia (7%), Greece (8%).

The next stage of the proposed methodological approach is to prioritize cyber vulnerability indicators of financial service consumers based on a combination of the principal component method (when determining the limits of indicators' values) and linear programming by the generalized downward gradient method. The implementation of this stage is complex, so there is a need to carry out several intermediate steps. Thus, for the formulation and solution of the linear programming problem for optimizing the weighting coefficients of cyber vulnerability indicators of financial service consumers, the following intermediate calculation steps are carried out in the further calculation of the single integral cyber vulnerability index:

Step 2.1. Formalization of the objective function as the sum of the weight coefficients of the variables R_1, \dots, R_{17} – indicators of cyber vulnerability, which must be equal to a unit value:

$$F(w(R_1), \dots, w(R_{17})) = \sum_{i=1}^{17} w(R_i) \rightarrow 1 \quad (1.10)$$

where $F(w(R_1), \dots, w(R_{17}))$ – functional relationship between weighting factors $w(R_i)$ of variables R_1, \dots, R_{17} – indicators of cyber vulnerability.

Step 2.2. Formalization of constraints on the problem of optimizing the weighting coefficients of cyber vulnerability indicators for consumers of financial services:

–the sum of the weight coefficients of the indicators of the following list (from the 4th to the 15th inclusive) should not exceed the level of 0.5 unit fractions:

$$\sum_{i=4}^{15} w(R_i) \leq 0.5 \quad (1.11)$$

This condition is introduced in the econometric model since the above-mentioned indicators (R4-R15) reflect the degree of use of preventive measures by citizens to increase their level of protection of the virtual space.

–the values of cyber vulnerability indicators should not exceed and should not be less than the maximum permissible levels:

$$w(R_{i,i=4\div 15}) \leq RO_i \quad (1.12)$$

$$w(R_{i,i=1,2,16,17}) \geq RO_i$$

where RO_i – maximum permissible limits of quantitative values for the i -th indicator of cyber vulnerability characteristics.

To set the maximum permissible levels of cyber vulnerability indicators, we will use the method of the main components of the Statistica software package. In essence, the method consists in choosing a new system of orthogonal coordinates in the observation space. The direction along which the array of observations has the greatest variance is chosen as the first principal component. Each subsequent component is also selected based on the condition of maximizing the remaining fraction of the variance along it, supplemented by the condition of orthogonality to all previously selected components. At the same time, as the component number increases, the associated

share of the total variance will decrease. The results are shown in Figure 1.17.

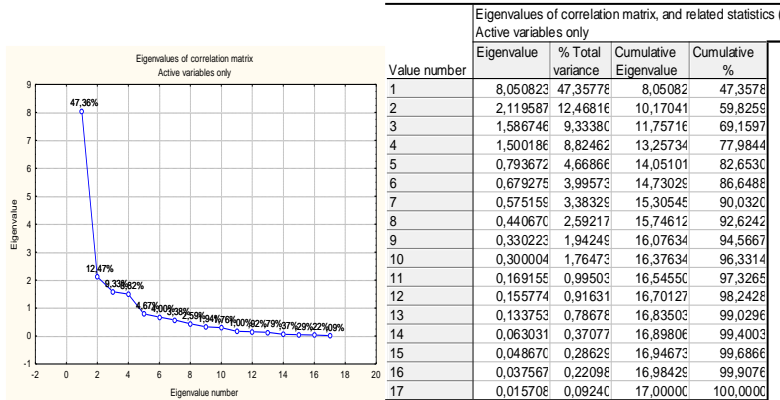


Figure 1.17. Screenshot of a fragment of the Statistica software of scree plot, the eigenvalues of the correlation matrix, and related statistical indicators

Based on the analysis of Figure 1.17, it can be concluded that it is advisable to take into account the first four main components, represented by the first four factors, for assessing the limits of cyber vulnerability indicators, the variation of which accounts for 77.98% of the total variation, as evidenced by the scree plot (left fragment of Figure 1.17), and tabular values of the eigenvalues of factors in the context of indicators (right fragment of Figure 1.17). Taking into account the data in Figure 1.17 and the contribution of variables based on the correlation of indicators of cyber vulnerability of consumers of financial services (Table 1.10, columns 1-4), we define the restrictions for prioritization RO_i based on the weighted arithmetic mean:

$$RO_i = \frac{\sum_{j=1}^4 F_{ij} \cdot v_j}{\sum_{j=1}^4 v_j} \quad (1.13)$$

where RO_i – restriction imposed on the i -th variable -an indicator of cyber vulnerability;

F_{ij} – the value of the contribution of the i -th variable in the context of the j -th factor (main component) based on correlation;

v_j – % of the total variation of the eigenvalues of the correlation matrix in the context of the j -th factor (main component).

The results of calculations using Formula (1.13) are presented in Column 5 of Table 1.10.

Table 1.10. – Contribution of variables based on correlation, limiting priority and weight of indicators of the cyber vulnerability of consumers of financial services

Indicator	Factor1	Factor2	Factor3	Factor4	Restrictions to determine priority RO_i	Weights $w(R_i)$
	47.36	12.47	9.33	8.82		
A	1	2	3	4	5	6
R1	0.0011	0.1829	0.2279	0.0164	0.0590	0.104
R2	0.0030	0.3253	0.0225	0.0812	0.0657	0.111
R3	0.0404	0.0043	0.0582	0.0004	0.0323	0.077
R4	0.0267	0.1753	0.0108	0.0237	0.0483	0.011
R5	0.0772	0.0331	0.0036	0.0446	0.0576	0.021
R6	0.0949	0.0032	0.0189	0.0028	0.0607	0.029
R7	0.0259	0.1418	0.1851	0.0170	0.0625	0.038
R8	0.1127	0.0007	0.0019	0.0059	0.0694	0.045
R9	0.0941	0.0100	0.0619	0.0072	0.0669	0.045
R10	0.0784	0.0040	0.0147	0.0002	0.0500	0.045
R11	0.0468	0.0239	0.1518	0.0246	0.0532	0.049
R12	0.1023	0.0008	0.0103	0.0097	0.0646	0.053
R13	0.1007	0.0264	0.0079	0.0045	0.0668	0.055
R14	0.1009	0.0020	0.0204	0.0005	0.0641	0.055
R15	0.0016	0.0188	0.1293	0.3758	0.0619	0.055
R16	0.0895	0.0064	0.0200	0.0084	0.0587	0.104
R17	0.0039	0.0411	0.0547	0.3770	0.0582	0.103

Thus, taking into account formulas (1.10) – (1.13), the formulation of the problem of optimizing the weighting coefficients of cyber vulnerability indicators for consumers of financial services takes the following form:

$$F(w(R_1), \dots, w(R_{17})) = \sum_{i=1}^{17} w(R_i) \rightarrow 1 \quad (1.14)$$

$$\left\{ \begin{array}{l} \sum_{i=1}^{17} w(R_i) \leq 0.5 \\ w(R_{i,i=4\div 15}) \leq RO_i \\ w(R_{i,i=1,2,16,17}) \geq RO_i \\ w(R_i) \geq 0 \end{array} \right.$$

where $F(w(R_1), \dots, w(R_{17}))$ – functional relationship between weighting factors $w(R_i)$ of variables R_1, \dots, R_{17} – indicators of cyber vulnerability.

It is proposed to optimize the weighting coefficients of cyber vulnerability indicators for consumers of financial services as a linear programming problem using the “Search for a solution” toolkit in MS Excel, particularly the generalized decreasing gradient method. The results of the calculations are presented in Column 6 of Table 1.10. Thus, the most influential indicator in assessing the cyber vulnerability of financial service consumers is R2, which accounts for 11.1% of the impact. The following relevant indicators are R1 and R16, the weighting coefficients of influence in the context of which reach 10.4%.

The final stage is the calculation of the integral cyber vulnerability index based on the use of multiplicative Kiri convolution. Taking into account the weights obtained at the previous stage for the influence of cyber vulnerability indicators of financial service consumers, as well as the nature of these

indicators as stimulants or disincentives (designation + and -, respectively, in Table 1.9), we will convolve them into a single integrated cyber vulnerability index based on the use of a multiplicative

$$\begin{aligned}
 & ICR_i(R_1, \dots, R_{17}) \tag{1.15} \\
 &= \frac{1}{k} \left\{ \prod_{i=1 \div 3, 16} [1 + k \cdot w(R_i^+) \cdot R_i^+] \right. \\
 &\quad \cdot \prod_{i=4 \div 15, 17} [1 + k \cdot w(R_i^-) \cdot (1 - R_i^-)] \\
 &\quad \left. - 1 \right\}
 \end{aligned}$$

where $ICR_i(R_1, \dots, R_{17})$ – cyber vulnerability index for the first country (absolute estimate);

k – a constant that determines the number of cyber vulnerability indicators;

R_i^+, R_i^- – accordingly, i -th indicator of cyber vulnerability incentive and disincentive.

The results of calculations performed using the Kini formula (1.15) are systematized in tabular form, particularly in columns 1 and 2 of Table 1.11.

Table 1.11. – Absolute and relative levels of cyber vulnerability of financial service consumers in a set of selected 28 European countries

Country	Absolute level of cyber vulnerability	Country	Absolute level of cyber vulnerability
Belgium	287,378%	Liechtenstein	331,317%
Bulgaria	435,179%	Luxembourg	214,931%
Czech Republic	349,618%	Hungary	393,596%
Denmark	125,357%	Malta	192,096%
Germany	256,822%	Netherlands	120,042%
Estonia	172,125%	Austria	208,011%
Ireland	366,930%	Poland	309,972%
Greece	336,109%	Portugal	376,243%
Spain	526,414%	Romania	491,389%
France	299,869%	Slovenia	366,733%
Croatia	447,456%	Slovakia	365,780%
Italy	519,764%	Finland	148,774%
Cyprus	394,184%	Sweden	117,005%
Latvia	361,841%	United Kingdom	282,798%

The absolute value of the index of the cyber vulnerability of consumers of financial services in many European countries under consideration does not allow for an objective assessment and comparison of countries with each other, which leads to the need to determine a relative assessment of the cyber vulnerability of consumers of financial services. For this purpose, we define the relative level of cyber vulnerability of consumers of financial services as the ratio of the absolute assessment to the maximum possible level observed on the studied set of values of the constituent indicators. Therefore, the maximum possible value of the absolute cyber vulnerability index is calculated as follows:

$$\begin{aligned}
ICR_{max}(R_1, \dots, R_{17}) & \quad (1.16) \\
&= \frac{1}{k} \left\{ \prod_{i=1 \div 3, 16} \left[1 + k \cdot w(\max_{i=1 \div 17} R_i) \right. \right. \\
&\quad \cdot \max_{i=1 \div 17} R_i \left. \right] \\
&\quad \cdot \prod_{i=4 \div 15, 17} \left[1 + k \cdot w(\min_{i=1 \div 17} R_i) \cdot (1 \right. \\
&\quad \left. \left. - \min_{i=1 \div 17} R_i) \right] - 1 \right\}
\end{aligned}$$

where $ICR_{max}(R_1, \dots, R_{17})$ – the maximum possible value of the absolute cyber vulnerability index.

Taking into account the above formulas (1.15) and (1.16), namely, determining their ratio, we obtain the desired relative index of the cyber vulnerability of financial services consumers:

$$VICR_i(R_1, \dots, R_{17}) = \frac{ICR_i(R_1, \dots, R_{17})}{ICR_{max}(R_1, \dots, R_{17})} \quad (1.17)$$

where $VICR_i(R_1, \dots, R_{17})$ – cyber vulnerability index for the first country (relative assessment).

We present the results of the calculations performed using formula (1.17) in the figure

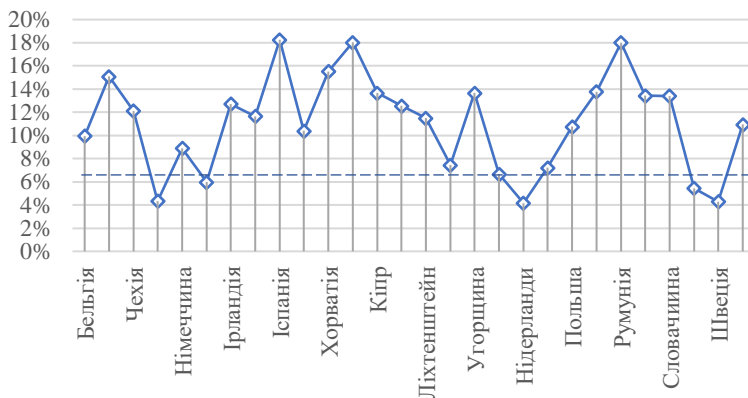


Figure 1.18 – The results of assessing the level of cyber vulnerability of consumers of financial services in Europe as of 2020

The study showed that the level of cyber vulnerability of EU citizens is on average 11%, which makes it possible to assert that the population of European countries is aware of threats in the virtual space, ways of protecting against cybercrime. However, the level of cyber vulnerability of consumers of financial services in the context of the EU countries is not uniform. Namely, citizens of countries such as Denmark, the Netherlands, and Sweden have the lowest risk of becoming victims of cyber fraud. Countries with high values of the calculated level of cyber vulnerability of consumers of financial services (18%) include Spain, Italy, Romania.

Thus, the analysis of the level of cyber vulnerability of consumers of financial services based on the example of EU countries shows the effectiveness of the regulatory and educational measures to inform the population about potential threats in the virtual space and ways to protect against cyber threats. It should be noted that monitoring the level of cyber vulnerability of citizens in their financial settlements requires

making calculations on an annual basis since there is a constant intellectualization of the cyber fraud methods.

1.5. Criterias for informal financial transactions mediated by financial institutions

Over the past decade, with the development of technologies used in the financial sector and the expansion of the range of services provided by economic agents, fraudulent schemes for committing financial crimes have also been improved. Illegal financial transactions have already become a severe problem for most of the world's economies. As they undermine the fundamental foundations of the economic system and negatively affect the development of the national economy. Although experts worldwide are constantly making efforts to stop illegal financial transactions and counter and combat financial and economic crimes, they are still a severe problem for economic development and ensuring economic security. The existing unresolved problems of financial crime require the development of combinations of methods and models that can (taking into account certain factors and priorities) effectively identify possible financial violations at an early stage. This can be achieved by building effective cause-and-effect models that can link and combine the causes and consequences of financial transactions and financial crimes into a single set of practical actions.

To build a model for assessing the causal relationships between financial transactions and financial crimes, it is necessary to understand which financial transactions can be used by financial criminals. There are specific characteristics of financial transactions that may be related to financial crimes. Such financial transactions, depending on their characteristics, are grouped according to the following criteria:

1. Client behavior: the client does not provide the information necessary for the economic agent; the client provides incomplete information; the client provides inaccurate, questionable, false information; the client does not provide supporting documents; the contact information provided by the client regarding phone numbers, addresses, e-mail is invalid; data from the client differ from those available in public sources; the age of the client does not correspond to the nature of the monetary transactions; the client's profession is not typical for a financial transaction; the client's income level does not match the amount of the financial transaction; the client cannot clearly formulate the nature of his activities; the client does not understand the nature of financial transactions; the client behaves unreasonably atypical, unusual, suspicious, nervous; the client unreasonably requests an urgent transaction; the client is suspiciously interested in the requirements of financial monitoring; the client offers a reward for conducting a financial transaction; the client refuses to carry out a financial transaction upon request to provide additional documents; the client requires service from a specific employee of an economic agent, refusing to carry out a financial transaction in the absence of such an employee; the client has an unreasonably large number of accounts; incomprehensible nature of the purpose of opening accounts; discrepancy between the amounts of taxes and the size of transactions; there are suspicions about performing an operation in favor of an unknown third party or exercising control over the transaction by such a person; the client's legal representative deliberately does not contact the employees of the economic agent; one person manages unrelated accounts; the client specifies a card delivery address that is not associated with the client.

2. Financial transactions: carrying out a significant turnover of funds on the account during the day with small balances at the end of the day; financial transactions do not correspond to the

client's activities; rapid leaps in the amount of funds on the client's accounts; frequent transfers without opening an account; crediting of frequent small amounts with their subsequent cumulative transfer to another person; the movement of funds on the account assumes only non-cash transfers with their subsequent cash withdrawal from the account; carrying out cash transactions for a significant amount that does not correspond to the client's main class of economic activity; large number of transactions on card accounts; conducting financial transactions under agreements on the assignment of claims; expenditure financial transactions to reinforce the cash desk for collection transactions in large volumes, with the subsequent issuance of loans to individuals, and the funds enter the account in large amounts as payment for transactions of assignment of rights of claim; non-cash transfers from the account of funds for issuing loans to individuals, the volumes of which are unreasonably higher than the market average; the issuance of short-term loans to several individuals for significant amounts from one legal entity, and the funds by individuals are immediately withdrawn in cash, and then there are no payments to repay such loans, and according to available data, these individuals do not have sufficient funds and income to repay loans; obtaining a loan by an individual for a large amount, which is more than the income of an individual, with the subsequent repayment of the loan not at the expense of an individual, but of other persons; receipt of exclusively state funds into the account of a non-profit legal entity; lack of collection of proceeds from a client whose main class of economic activity is retail; most of the receipts to the account are funds from online systems, but the client does not work in online trading or online activities; settlements from commercial activities through the account of an individual; differences between payment details and supporting documents; artificial replenishment and increase of the authorized capital by gradual periodic transfer of funds to the account of a legal entity;

carrying out transactions for the purchase or sale of assets, receiving or paying off debts on transactions, providing or returning financial assistance by periodically circulating one amount on the client's account; providing services for financial transactions within one day deliberately with different employees of the economic agent; transfer of funds from the account of a legal entity to individual accounts of individuals of employees or persons related to employees that are not payment of wages or other understandable payments; the client's partners have a negative reputation; the sender and recipient of funds do not have basic information about each other; refund of funds by the receiving bank; groundless refusal to provide information on the participants in a financial transaction; payment of transfers in branches located geographically near the borders of countries with a high risk of terrorism; frequent circulation of borrowed funds from persons who are not a group of related persons; unspecified purpose of payment; profitable and expense transactions have an unsuitable purpose; periodic payments to persons who have no explicit connection with the client's business activities; receipt of funds from a non-profit institution with their subsequent urgent expenditure on the acquisition of assets; linking a financial transaction to the purchase or sale of dual-use goods; use of the client's POS terminal by third parties; purchase by the client of an unreasonable amount of instant non-personalized cards; incomprehensible amounts and volumes of financial transactions that are not inherent in a certain type of economic activity; financial transactions to reimburse funds to persons from whom payments actually came; transfer of funds by a resident legal entity to the account of a non-resident legal entity opened with a bank in Ukraine; receipt of funds by a non-resident legal entity from a resident legal entity to an account opened with a bank in Ukraine; partners in foreign economic contracts have a negative assessment; payment under foreign economic contracts for which violations have already been

detected; fuzzy essence of financial transactions from abroad or abroad; foreign transfers within one day by different persons, but with similar details; fundraising by various non-profit organizations for subsequent transfer to certain non-resident persons; receiving funds from abroad with the subsequent transfer of these funds abroad (to the same country) or in the name of the same person abroad (to another country).

3. Financial transactions of insurance companies: unjustified increase in the amount of the insured amount; the amount of insured amounts is incomparable with the possible risk; the amount of insurance premiums paid incomprehensibly more than those indicated in the transaction; large cash volumes of payment of insurance premiums; private payment of insurance compensation in cash; cash lump sum insurance premium according to the life insurance contract; termination of the insurance agreement ahead of schedule with the subsequent transfer of funds to a third party; third parties pay insurance premiums; unreasonably large amounts of payments (for services rendered) to individual entrepreneurs; unreasonably large amounts of agency fees under a power of attorney agreement; transactions with clearly unfavorable conditions for the parties; significant changes in previously concluded deals for a short period of time; the amount of the insured property does not correspond to the client's financial income; insurance of an object against risks that are not inherent in it; re-insurance of financial risks of a person who had insurance compensation in the past; insurance of financial risks of a person who had insurance compensation in the past; insurance of financial risks of persons bearing financial risks for uninsured persons; an insured event occurs in a short time after the insurance; invalid, fake documentation on the payment of insurance premiums, insurance premiums, insurance payments; conclusion of a short-term deposit agreement with an end date – the last day of the quarter; implementation of an early termination of the deposit

agreement after the last day of the quarter; a limited list of supporting documents for payment of compensation under an insurance agreement; financial transactions of reinsurance of a person whose cash flow amounts for previous periods are significantly less; reinsurance of persons with an unsatisfactory financial situation; reinsurance of a person located in a state atypical for such an agreement; reinsurance of persons from countries whose persons were not reinsurance in the past; the reinsurer cannot fulfill financial obligations with own funds.

4. Cash financial transactions: cash deposit of proceeds from sold assets to an account without supporting documents; frequent small financial transactions for depositing cash into accounts in various branches of the bank to transfer funds to one account; small financial transactions of a significant amount to deposit cash in one bank branch at the same time by different persons in order to transfer funds to one account; withdrawing large amounts of cash from the account for cash settlements with partners without supporting documents; frequent small financial transactions to withdraw cash from accounts in one bank branch at the same time by different persons; small financial transactions for withdrawing cash from an account in different branches of the bank; cash financial transactions to withdraw a large amount of funds from an account that has been inactive for a long time; cash financial transactions to withdraw a significant amount of funds from an account to which funds came from abroad; repeated cash financial transactions for significant sums; financial transactions for the full withdrawal of cash immediately from the accounts of different customers through one ATM; currency financial transactions in cash for buying, selling, converting; discrepancy between the amounts of transactions in cash on the client's account with its economic activity and the volume of economic activity; significant circulation on the cash account not typical for the client's economic activity; constant exchange of a significant amount of

small cash for large ones; ongoing financial transactions to deposit small amounts into accounts with subsequent withdrawal of one significant amount from the account; circulation of funds on the client's account with signs of cyclicity; conducting financial transactions in cash in such a way as to avoid the mandatory requirements for threshold financial transactions; execution of cash financial transactions through self-service terminals or ATMs in large volumes within one day.

5. Credit financial transactions: a person's indifference to the terms of the loan, interest rate, amount of payments, overpayment of a loan, penalties, etc.; unjustified payment of the loan by a third party; inappropriate use of credit funds; direction of credit funds for purposes that do not correspond to the client's activities; the unclear economic purpose of obtaining a loan; unreasonable loan secured by a deposit of a significant amount; the loan is secured by the property of third parties not related to the client; repayment of an overdue loan at the expense of funds received by the client from unknown sources; repayment of a long-term loan in a short time.

6. Foreign economic financial transactions: the place of delivery of goods, according to the foreign economic contract, is in a country with a high level of terrorism financing risk, money laundering; the country of transit of goods, according to the foreign economic contract, belongs to the countries with a high level of risk of terrorism financing, money laundering; incomprehensible passage of the product in transit through certain countries; incomprehensible complication of the structure of the financial transaction; economically unjustified import or export of goods; unreasonably high or low price for a product or service; inaccurate information on the number of exported or imported goods; false data on the type of imported or exported goods; suspiciously frequent or significant changes in terms of the letter of credit.

7. Financial transactions with securities: financial transactions for the purchase/sale of financial instruments at non-market prices; regular execution of financial transactions in financial instruments in a short period of time, at a non-market price, with specifically selected counterparties; financial transactions of large amounts for the purchase or sale of securities that are illiquid; financial transactions in large amounts for the purchase or sale of securities for which it is difficult to establish a market price; regular implementation of unprofitable financial transactions for the purchase and sale of securities in a short period of time at a purchase price that is high enough and a sales price that is low enough; regular implementation of financial transactions for the purchase and sale of securities in a short period of time at a sales price significantly higher than the purchase price; economically inexpedient transactions for the purchase/sale of securities; unreasonably complex, confusing or economically impractical nature of financial transactions with securities; significant amounts of financial transactions for the purchase or sale of closed issue securities with an unknown issuer; significant volumes of financial transactions for the purchase or sale of closed issue securities with the issuer associated with the client; unreasonably rapid growth of the securities portfolio within a short period of time; over-the-counter financial transactions for the purchase or sale of securities without payment against delivery; receiving or transferring securities from one counterparty on an ongoing basis to unrelated clients; atypical settlement period (more than two weeks); the lack of financial transactions on the client's account, constantly receiving transfers for investment profit, to transfer the corresponding amounts of funds for the purchase of securities to the broker; obvious inconsistencies, inaccuracies in the client's supporting documents on financial transactions with securities; not a reliable beneficiary of securities transactions, conducting a

transaction in favor of an unknown third party; the subject of financial monitoring, the state financial monitoring service, law enforcement agencies, official inquiries regarding the threats to conduct a transaction for money laundering.

8. Custody services: use of a safe by proxy; one client uses three or more safes at the same time; atypical behavior of the client when using the depository; sharp apparent changes in the nature and timing of the client's visit to the depository; being in the depository for an unreasonably long period; use of the safe by a legal entity or an entrepreneur, for whose economic activity it is not inherent to use such a service; the client first visits the depository and immediately afterward deposits cash into the account.

9. Online financial transactions: the use of the IP address by unrelated clients when making transactions using the Internet client bank; access to the Internet-banking of a third person from an unknown bank; use of the Internet client bank by a user outside of Ukraine without notifying the bank.

10. Situational financial transactions: transfer of travel funds by a business entity to the accounts of individuals, while such individuals do not work, involved in criminal cases; opening salary cards for non-existent workers or opening card accounts for employees of a fictitious business entity, with the subsequent regular crediting of significant amounts of wages to these accounts, and then the withdrawal of cash from these accounts at an ATM or at the bank's cash desks; withdrawing cash for the further purchase of agricultural goods with a short shelf life and the possibility of a fairly quick write-off as expired, and such goods are then bought by proxy in a significant number of agricultural entities in far-away areas for insignificant amounts, which is quite difficult to be checked by the relevant structures; operations when funds are withdrawn from the account for non-specified business expenses, the purchase of clearly not specified goods, services, inventory items, the true purpose of which is to withdraw non-cash funds into cash; cash withdrawal

operations in accordance with a deposit agreement with an individual, the issuance of dividends, the payment of interest-free financial assistance, made in a short time after the conclusion of the transaction; specific operations for the withdrawal of funds from payment cards (the purpose of withdrawing cash is the further purchase of securities of the subjects, which are actually fictitious; first, the funds go non-cash into the account as refundable financial assistance, and then are withdrawn in cash; withdrawal of cash from an account by an individual as personal savings; opening and subsequent withdrawal of cash from corporate cards in different regions for fuel, agricultural products, but the real purpose of such operations is prompt access to cash); issuance of funds for other purposes without specifying; payment of rent for shares, without specifying to whom, in what amounts, according to which the agreement, etc.; issuance of funds for scrap metal, waste paper, which is almost impossible to verify; payment of funds to pay for unspecified services; payment of funds for charitable assistance; conducting transactions with signs of splitting operations into smaller amounts for this purpose to avoid legal restrictions on financial monitoring, etc.

11. Scheme financial transactions:

- Transfer of funds from the account of a business entity in one bank to the account of the same business entity in another bank, and the purpose of the payment is to transfer funds to its own account → the business entity transfers funds to some of its employees – individuals to corporate cards as financial assistance → individuals withdraw funds from the account in cash.
- Transfer of funds between the accounts of a range of entities as payment for scrap metal, agricultural goods, inventory holdings, financial assistance, construction goods → funds to accounts are accumulated in total amounts → cash in the total amount is withdrawn by power of attorney at bank cash desks or ATMs (moreover, the overwhelming majority of economic

entities have recently been created; officers and founders are one person; there is a kinship between officials and proxies; persons to whom a power of attorney has been provided are official founders, managers, accountants of other business entities; a person acting under a power of attorney is not officially employed by a business entity; tax payments have not been paid, there are no officially recorded incomes in the submitted statements; cash withdrawal operations were carried out on the same day when the funds entered the account; there is a cash withdrawal by one person through the bank cash desks, ATMs).

–Transfer of funds from some economic entities to a number of other business entities (moreover, for business entities, the official and the founder are one person, the authorized capital of which is small enough, whether they have unpaid taxes, or undeclared income), with a certain different purpose for services, for gas, for wheat, financial assistance → withdrawal of such funds for the purchase of agricultural goods or transfer as financial assistance to certain individuals with their subsequent cash withdrawal.

–etc.

Thus, a correct assessment of the causal relationships arising between financial transactions and financial crimes in the system of financial and economic relations between economic agents, individuals and legal entities, regulatory and supervisory bodies, both at the micro and macro levels, the construction of effective assessment models such relationships must correspond to certain features, characteristics, and requirements. This will make it possible to identify as objectively as possible, determine, reflect the existing processes and actions in this system, realize the possible consequences, provide protection against threats, and ultimately form certain vectors and directions for minimizing risks, developing the financial market, the national economy, stabilizing the economic system in general.

2. CONCEPT OF CONVERGENCE OF FINANCIAL MONITORING AND CYBERSECURITY SYSTEMS

2.1. Fundamentals of convergence processes of financial monitoring and cybersecurity systems

The rapid development, growth and accumulation of modern technologies, information support, and digital data create the prerequisites for using information technologies in various fields and areas of activity. In Ukraine and the world, comfortable conditions have been created for online work with the latest financial and economic industry technologies. Thus, individuals and business entities received almost unlimited opportunities to use financial services remotely, connect to online banking, currency exchanges, stock market, and other financial and credit institutions and organizations. At the same time, each innovation process is accompanied by certain threats. Thus, there will be a threat of increased crime rate in the virtual information cyberspace due to its availability to legal participants and criminals. Such modern opportunities in the economic sphere create the need to ensure the proper economic security of financial transactions passing through the corresponding systems.

Over the past ten years, a system has been formed in Ukraine to combat money laundering, terrorism financing, the proliferation of weapons of mass destruction, including cyber threats, in the form of a set of measures for financial monitoring and a cybersecurity system. It provides for verification of clients and their financial transactions to control economic purity and transparency of financial transactions.

Therefore, in modern market conditions, the issue of convergence of financial monitoring and cybersecurity systems is especially relevant and requires detailed study and analysis.

General theoretical issues of financial monitoring and its specific practical features are disclosed by both domestic and

foreign scholars, including Morse (2019), covering the global regime of combating terrorism financing under the influence of the transnational market; Radygin et al. (2021) suggest ways to solve the problems of primary financial monitoring; Yashina et al. (2021) cover some aspects of financial monitoring, financial stability, and digitalization; Hrabchuk & Suprunova (2020) reveal the concepts, components, stages of development of financial monitoring as a condition for ensuring the state security; Pershyn (2019) considers the issue, determines the role of financial monitoring in combating money laundering, suggests ways to improve the financial monitoring system; Rysin & Stepanova (2020) describe the tools to counter terrorism financing using financial institutions; etc.

Issues of study, research, use, improvement of the concept of cybersecurity in modern scientific economic literature are considered by such scientists as Shackelford et al. (2021), who study cybersecurity in a crisis; Uchendu et al. (2021) summarize the development of a culture of cybersecurity; Han & Han (2021) suggests using a semi-quantitative cybersecurity risk assessment by analyzing the level of blocking and protection; Mokhor et al. (2021) introduce an assessment of the cybersecurity risks of information systems; Gimenez-Aguilar et al. (2021) highlight the practical advances in cybersecurity in blockchain-based systems; Repetto et al. (2021) analyze autonomous cybersecurity for next-generation digital service chains; etc.

The results of the influence of convergence on the efficiency of the processes under study were revealed by the following scientists: Madeira et al. (2021) propose a combination of the strategy of reasonable specialization and regional convergence in the economy; Ibrahim et al. (2021) describe the convergence of vast data and accounting in forecasting; Dong et al. (2021) investigate the impact of industrial convergence on the efficiency of environmental development; Guilbeault et al.

(2021) highlight experimental evidence of convergence of the categories under investigation; etc.

Thus, the issues of finding methods and ways to prevent, counteract, and combat financial crimes, which commission involves information, technological, communication, and technical systems, are a concern of national government agencies and the global community.

Considering the features of financial monitoring, it is necessary to consider its definition. Thus, according to the Law of Ukraine On Prevention and Counteraction to Money Laundering, Terrorism Financing and Financing the Proliferation of Weapons of Mass Destruction, “financial monitoring is a set of measures taken by the subjects of financial monitoring in the field of prevention and counteraction, including the conduct of state financial monitoring and primary financial monitoring” (Verkhovna Rada of Ukraine, 2021). In a general interpretation, financial monitoring is a complex system of principles, measures, methods, techniques carried out by subjects and participants of financial monitoring to identify, counteract, prevent the use of the financial and banking system for money laundering, terrorism financing, and proliferation of weapons of mass destruction; a set of actions to identify transactions that may be associated with money laundering, their thorough study and the performance of appropriate actions; it is a system for monitoring financial transactions to prevent money laundering. Money laundering is actions, measures, operations with means related to illegal activities, having illicit origin sources, hiding illegal possession of funds, providing for their illegal movement, use, change of form.

Considering the above, the interpretation of the concept of a financial monitoring system is being formed – a set of measures (at the state and primary levels) performed by the subjects of primary financial monitoring and the specially authorized body for financial monitoring in terms of identification, study, and

analysis of financial transactions, additional information about them, about clients, to identify attitudes towards illegal activities, terrorism financing, accounting for such financial transactions, assessing the risks from such transactions. The decisive role in the financial monitoring system is assigned to the subjects of primary financial monitoring, which include (Verkhovna Rada of Ukraine, 2021): banking institutions, insurance companies, reinsurance organizations, organizations that are financial service providers, payment institutions, organizations acting as members of payment systems, pawnshops, credit unions, securities market participants, commodity exchanges, mail order operators, institutions conducting foreign exchange transactions, audit companies, organizations that are accounting service providers, notaries, lawyers, legal service providers, education and management service providers for business entities, real estate agencies, business entities – lottery sellers, gambling organizers, virtual asset sellers, other financial service providers. The leading role belongs to the subjects of state financial monitoring (Verkhovna Rada of Ukraine, 2021): National Bank of Ukraine, Ministry of Justice of Ukraine, National Commission on Securities and Stock Market, Ministry of Digital Transformation of Ukraine, Specially Authorized Body.

Organization of effective financial monitoring presupposes the identification and achievement of strategic priority goals, i.e. countering money laundering; combating terrorism financing; countering the financing of the proliferation of weapons of mass destruction; proper organization, implementation and control of the internal banking system for combating money laundering, terrorism financing; functioning of an appropriate risk management system in the field of financial monitoring; protection of state, public, civil interests from money laundering, terrorism financing; adherence to a risk-based approach in the implementation of financial monitoring;

ensuring the coordination of cooperation between participants in the financial monitoring system; taking punitive measures against violators of legislation in the field of financial monitoring.

The specified goals of financial monitoring form the tasks of financial monitoring that are set to achieve the effectiveness of financial monitoring: to develop and comply with the requirements of legislative acts, other legal documents, and the internal regulatory framework under financial monitoring; organize appropriate structural bodies and financial monitoring units at the state level, at the level of primary financial monitoring entities, at the level of business entities; organize an intrabank financial monitoring system; ensure the sufficiency of the resource base for the proper operation of the financial monitoring system; ensure the effective functioning of the system of measures to manage the risks of money laundering and terrorism financing; ensure sufficient awareness, the competence of individuals, business entities, employees of primary financial monitoring entities and government agencies regarding the risks of money laundering; organize and permanently improve internal and external control over the counteraction to money laundering; to develop and implement a set of measures for due diligence of clients – to carry out current and additional verification of the client, to verify financial transactions of the client, to identify discrepancies between the clients' financial transactions and the information available to the bank about such clients, about the specifics of their business, the essence of the client's activities, goals and expectations from business cooperation with the client, to investigate the sources of origin of funds, to determine the condition of clients, to identify and establish the ultimate beneficiaries of clients, assess the economic and financial feasibility of client's transactions; to identify the unusual actions and operations of the client; to prevent the use of banking services for money laundering; to

identify threshold money transactions; to identify suspicious financial transactions; to freeze the assets of unreliable clients, fraudsters, terrorists; to promptly report risky and suspicious financial transactions to the Specially Authorized Body; to conduct a proper exchange of relevant data between the subjects of primary financial monitoring and the Specially Authorized Body; to ensure the operation of an effective system for the escalation of certain suspicions and threatening issues in the field of preventing money laundering; to timely consider suspicions and facts of violations in the field of combating money laundering; report criminal activities of clients to law enforcement agencies; timely provide the necessary data, explanations, documents, information at the request of the National Bank in terms of compliance with financial monitoring; to develop, use and constantly improve the automated systems of participants in financial monitoring; to freeze assets to persons associated with terrorist activities; to protect data and information in the field of financial monitoring; to provide the subjects of financial monitoring with necessary access to the necessary information for conducting financial monitoring; to organize the timely exchange of information between the participants of the financial monitoring system; to organize and ensure international cooperation in combating money laundering, and terrorism financing; etc.

In turn, the key areas of financial monitoring are highlighted during the formation of an appropriate system of financial monitoring:

–due diligence of clients (carried out when establishing a business relationship with a client, in case of suspicions and doubts about the veracity of the data submitted by the client, the reliability of information about the essence of the client's activities and financial transactions, in the case of a one-time financial transaction without concluding a business relationship with the client, transferring without opening an

account in the amount of UAH 30 thousand or more, transactions on virtual assets in the amount of UAH 30 thousand or more): identification (measures and actions taken by the bank to determine the identity of the client through the identification of client data, before establishing a business relationship with a potential client), verification (measures and actions of the bank in relation to the client to confirm the correspondence of the information available in the bank about the client to such a client, and for identification of the ultimate beneficiaries of the client before and during the establishment of a business relationship with a potential client) and video verification of the client (verification of clients by video broadcasting) – during identification, verification, video verification of clients, the identification data concerning passport data, identification codes, constituent data, place of registration and location, bank details are established; determination of the final beneficiaries of the client (i.e. persons who have priority, decisive control and influence on the functioning of clients and their financial transactions in the form of direct ownership of shares of 25 percent or more in the authorized capital, or in voting rights, or indirect influence of owning less than 25 percent in the authorized capital, or in rights voices, while maintaining the decisive power of the voice); determination of the purpose and features of business cooperation with a client (to determine the type of banking services that are of interest to the client, special conditions for concluding transactions, tariffs, scale of transactions, client's reputation); enhanced client verification (these are measures to minimize the level of risk that may be inherent in a client, business relationship with such client; applied to clients with high risk, clients with suspicion of conducting transactions for the purpose of money laundering or terrorism financing; performed in the following ways: increasing the number of actions to verify the client, updating information about it and

the frequency of such actions; the client's need for additional data, clarifications, supporting documents on the client's ownership structure, sources of funds, income, on the availability of licenses and permits for certain activities; search for additional data about the client in open official information sources, including about economic activities, ultimate beneficial owners, about initiated criminal proceedings, about existing financial, economic ties with other persons and business entities; visits to the place of registration and conduct of the client's business, etc.); simplified client verification (these are measures to minimize the level of risk that may be inherent in the client, business relationship with such client; apply to low-risk clients, including individuals who pay utility bills for small amounts; individuals who have accounts that have been opened for the payment of social benefits, pension payments, payments for wages, scholarships, which conduct rationally substantiated, ordinary, typical financial transactions in small volumes; enterprises – providers of housing and communal services, television services, Internet services, with which an agreement on acceptance of payments has been concluded; association of co-owners of apartment buildings; legal entities and sole proprietors paying obligatory tax payments; public authorities; local government agencies; social insurance funds; EU bodies, diplomatic missions of members of the Organization for Economic Cooperation and Development; such measures include: reducing the number of actions to verify the client, updating information about it and the frequency of such actions; application of simplified customer verification methods; reducing the demand from the client for additional data, clarifications, supporting documents; application of information from the Unified State Register of Legal Entities and Individuals (Entrepreneurs); updating customer data (i.e. updating previously received data, documentation, information, as well as current information and

documents; updating is carried out at different intervals for different types of clients' risk – once a year for high risk, once every three years for medium risk, once every five years for low risk, or as necessary in certain cases; updating occurs by filling out a questionnaire by the client when visiting a banking institution; by sending a postal letter to the client about updating information and documents with a questionnaire; by sending an e-mail to the client about updating information and documents with a questionnaire; updated information is recorded in the automated bank system on the client's card, and the documents are filed in the client's personal file); the client's bank refusal to establish or continue business interaction, refusal to conduct financial transactions of the client (the banking institution must refuse the client to establish or maintain business cooperation in the following cases: if the client has not provided the data necessary for identification, verification or proper verification; the provision of false data by the client; presentation by the client of information that confuses the bank, misleads it; when it is impossible to determine the ultimate beneficiaries of the client; if the banking institution has doubts about the conduct of financial transactions by the client on its own behalf; determination of an unacceptably high risk for the client; if the participant of the financial transaction is a shell bank; if the customer maintains a certain relationship with the shell bank; a banking institution is prohibited from entering into business cooperation with the following clients: clients from the List of persons to whom special sanctions have been applied by the Ministry of Economic Development and Trade of Ukraine; clients who conduct financial transactions, the ultimate beneficiaries of which are persons from the List of persons to whom special sanctions have been applied by the Ministry of Economic Development and Trade of Ukraine; shell banks; individuals with specific relationships with shell banks; clients located or

belonging to states that do not comply with FATF recommendations; clients whose banks are located in countries that do not comply with the FATF recommendations);

- financial monitoring risk management: identifying the risks of money laundering and terrorism financing (assessment and reassessment of the risk portfolio of a banking institution (identification and assessment of the risks of money laundering and terrorism financing, which are characteristic of the work of a banking institution by determining the risks associated with them for each banking service, depending on the specifics, focus, the scale of the bank's functioning in terms of focusing on servicing individuals, retail business, business entities of micro, small, medium-sized businesses, large corporate clients, services provided by the bank, types of clients, their risk portfolios, geographic characteristics of the bank, methods of providing banking services, targeted use of banking services, specific opportunities for using certain bank services for money laundering, targeted segment for various services, possible volumes of circulation of funds, other factors important for the bank; analysis of the measures and methods of risk management available to the banking institution to minimize them); assessment and reassessment of the client's risk portfolio (determination of risk criteria; identification of the primary risk of establishing business relations with a client; application of a scoring risk model to assess the level of risk for a client; analysis of the measures and methods of risk management available to the banking institution to minimize them; assessment of the residual risk from establishing a business relationship with the client); calculation of the risk appetite of a banking institution (determining the risks that the bank can accept; risks that the bank is ready to accept only after minimizing them; risks that the bank cannot accept – clients with an unacceptably high risk, criminal activity, clients from sanctioned and prohibited lists, clients with indicators of

suspicion determined by the bank)); measures to minimize the risks of money laundering and terrorism financing (research and analysis of new services for the presence of risks; introduction of limits and restrictions on services; granting permission for relationships with public and related persons); granting permission for certain risky financial transactions; use of automated systems to determine risks for clients and their financial transactions according to risk criteria; conducting due diligence of clients to understand the nature and characteristics of the economic activities of clients; implementation of constant study and analysis of information about the client; constant research of the correspondence of the client's financial transactions to the essence of its work; research of the sources of origin of the client's financial resources; special study and monitoring of high-risk clients; a separate study of non-profit and charitable organizations for the possibility of their use for illegal purposes for money laundering); proper risk management (conducting a comprehensive assessment of the risks of money laundering and terrorism financing and its periodic reassessment; carrying out due diligence of customers; organizing a proper assessment and reassessment of risks that may arise when establishing or maintaining business relationships with customers; appropriate awareness of the risk of money laundering by the bank; taking differentiated measures for clients with different levels of risk; taking certain actions to bring risks to a level that is acceptable for the bank; developing and using effective tools to discourage the systematic and large-scale conduct of suspicious financial transactions; establishment of effective internal bank control and audits for financial monitoring; availability of a transparent system for the timely identification of politically exposed and related persons; availability of an effective system for identifying and studying the ultimate beneficial owners of clients);

- international cooperation (provides for cooperation based on reciprocity between different countries in the field of prevention, obstruction, combating money laundering, terrorism financing, the proliferation of weapons of mass destruction, including on the following issues: provision of proposals for the inclusion of individuals and business entities and complete information about them in the sanctions lists of foreign states; submission of proposals for the exclusion of individuals and business entities from the sanctions lists of foreign states; enforcement of court decisions on confiscation of illegal proceeds; crediting of confiscated funds to the state budget; observance of the principle of confidentiality and secrecy of the information; ensuring permission for specialized bodies of foreign countries to disclose certain information, etc.);
- organizing and ensuring liability for violation of regulatory legal and legislative acts on financial monitoring in terms of countering money laundering, terrorism financing, the proliferation of weapons of mass destruction (determination of liability for certain types of offenses, such as written reservations and warnings, revocation and cancellation of licenses, suspension from work, penalties, liquidation; taking into account certain circumstances of committed violations regarding the nature of violations, their duration, the financial condition of a banking institution or other subject of primary financial monitoring, the nature and amount of benefits from unlawful actions, losses incurred by third parties, the repetition of a violation of the same type, the degree of responsibility of persons, the willingness to cooperate on issues of financial monitoring).

The effectiveness of financial monitoring is achieved by using effective models developed by modern scientists and specialists in the field under study. These models are the following:

- scoring risk model – a scoring model for assessing the risk portfolio of clients used by banking institutions using existing software modules; implemented by assessing the bank's client according to certain risk criteria. The bank determines the risk criteria (determined by the bank's responsible employees in accordance with the requirements of the legislation and the internal regulatory framework of the bank; that criteria are introduced in or removed from the corresponding risk criteria for the bank's automated system and each of them is assigned a corresponding code); each of the risk criteria is assigned corresponding points from 0 to 101; the risk level is determined for each of the risk criteria (0 points – a low risk when the client did not match any of the risk criteria; from 1 to 50 points – an average risk; from 51 to 100 points – a high risk; from 101 – unacceptably high risk); according to the results of the assessment, the scores for each criterion of risk inherent in the client are summed up automatically; the total number of points for each client of the bank is determined; the total number of points for the client is compared with a scale of certain risk levels and the client is automatically assigned the level of the corresponding risk portfolio of the client, i.e., the level of risk of business relations with the client. Responsible employees of the bank make changes to the client card information on risk criteria on the day when circumstances that determine the level of risk of the client appear, or on the day of receipt of relevant information from the bank's financial monitoring unit, and also once quarterly, using appropriate software systems, carry out procedures for identifying customer-specific risk criteria;
- automated financial monitoring model – a model for automating financial monitoring processes, such as the automation of identification, verification, video verification of persons carrying out financial transactions subject to financial monitoring; automation of business processes for integrating the results of audits of internal monitoring of banks with state

financial monitoring; automation of the business process of internal verification of financial transactions subject to financial monitoring; automated development of the structure of templates for incoming and outgoing documents related to identification, verification and video verification of persons conducting financial transactions subject to financial monitoring; automated development of a database structure for internal financial monitoring of banks as a data scheme, taking into account key elements and relationships, the structure of regulatory and reference information required for the main financial monitoring procedures; automated development of the structure of templates for incoming and outgoing documents, messages related to the start of inspections and obtained monitoring results; etc.

- business models of the processes of financial monitoring of banks and other economic agents – a complex model, which includes several stages, with specific modeling used at each of them: a model of the business process of automated internal monitoring implemented directly by the economic agents themselves; a business process model for automated monitoring of payments, which filters financial transactions without available financial confirmation of the source of funds through the Internet-Client-Bank system; the business model of automated intra-bank financial monitoring of transactions to determine the risk associated with the use of bank services for money laundering;
- etc.

In general terms, the category of cybersecurity is a set of optimal measures, strategies for preventing, protecting, minimizing threats, risks, losses from the impact and commission of cybercrimes, cyber-attacks, digital attacks on the financial system and public welfare, leveling harmful, unfavorable, unsafe economic systems, effective leadership, capacity development of law enforcement and criminal

authorities, public awareness-raising, national and international cooperation.

The main strategic goals of cybersecurity are: ensuring the security of cyberspace, the effectiveness of cyber defense, effective countering cybercrimes, the development of cybersecurity tools, maintaining cyber resilience, ensuring reliable cyber protection, maintaining cyber readiness for cyber-attacks, ensuring digital security.

The above goals define the following important tasks of cybersecurity: improvement of the legislative framework for the preservation of electronic information, information about the movement of electronic data, collection, interception, accumulation of data, provision and disclosure of information to the relevant authorities about the seizure of computer information; protection against unauthorized interference in the functioning of automated systems, computer equipment, information and computer networks, communication networks; protection against the development, use, sale and purchase, distribution of malicious software systems and technical inventions; protection against unauthorized sale and purchase, distribution of classified information and data with limited access rights; protection from unauthorized, illegal actions of officials with relevant information; protection from improper operation of automated systems, computer equipment, information and computer networks, communication networks; protection against misuse of information resources; protection against violation and obstruction of the functioning of automated systems, computer equipment, information and computer networks, communication networks; fight against illegal actions with financial documents, electronic means of payment, electronic means, specialized equipment for their production; transparent, competent and effective investigation of online financial crimes, electronic and remote banking fraud; criminalization of attacks on information, computer systems,

data, databases, illegal access to them, illegal interference in their functioning, their abuse; criminalization of copyright infringements; criminalization of computer forgeries; criminalization of offenses related to illegal content; development, support and expansion of international integration, cooperation, partnerships through mutual assistance, exchange of information, disclosure of certain data, support of round-the-clock information networks, extradition of criminals, provision of legal and legal assistance, mutual recognition of court decisions, informal cooperation of law enforcement agencies of the countries, consent to specialized investigative actions; etc.

The main areas of cybersecurity are divided into certain groups depending on the areas of their actions: according to cybercrimes – the fight against encroachments on confidentiality, secrecy, integrity, inaccessibility of computer information, systems, networks (combating illegal access, hacking, interception of information; combating criminal interference with a computer system, creating obstacles to its functioning; fight against illegal interference with information, concealment, damage, deterioration, violation, alteration, deletion, destruction of data; combating the criminal use of computer systems, technologies); combating illegal use of computer equipment; combating illegal content of data and information; combating infringement of copyright and related rights to software, information resources, databases, digital products and services; according to criminal cybercrime offenses – the fight against the use of automated systems, computer equipment, information and computer networks, communication networks for the preparation, commission, and concealment of cybercrimes; combating the transmission of illegal data through the use of automated systems, computer equipment, information and computer networks, communication networks; combating illegal economic activity, illegal financial transactions carried out using computer networks; according to

the motivation of cyber fraudsters – the fight against cyber fraud, the purpose of which is the misappropriation of funds; the fight against cyber fraud, the purpose of which is the appropriation of information; combating cyber fraud, the purpose of which is to gain access to an automated system to cause damage, disorganization; according to cybercrimes in the banking sector – combating ATM fraud (combating skimming, i.e. installing reading and copying mechanisms on ATMs to obtain pin codes, as well as information on a magnetic stripe or chip; the fight against "white plastic", i.e. the use of empty unidentified plastic for duplicating client cards; combating fraud when canceling a transaction, i.e., when allegedly for technical reasons funds are credited back to the card, but physically they are withdrawn from the ATM; fight against cash trapping, i.e. theft of cash with the help of special cash withdrawal devices additionally installed by fraudsters); combating cyber fraud of trade and service networks (combating the use of stolen, counterfeit electronic means of payment, including plastic cards; combating fraudsters' appropriation of payment card details; combating the deliberate fragmentation of financial transactions and financial transactions with amounts less than the marginal ones to avoid authorization and identification; the fight against fictitious acquiring agreements, the purpose of which is to carry out transactions using stolen, counterfeit payment cards); combating Internet fraud (combating fraudsters' misappropriation of electronic means of payment via the Internet and carrying out financial transactions with their use); the fight against the development, creation of software designed to hijack the details of electronic means of payment); combating fraud in remote banking systems (combating the opening of accounts for illegal non-cash and cash financial transactions through web banking, mobile banking, and other remote service systems; combating the development and creation of computer viruses to take possession of the computer control system of other persons to

carry out unauthorized financial transactions; combating interference in the work of international money transfer systems and international payment systems to receive unauthorized transfers from abroad); according to the regulatory framework – ensuring changes in the legislation to increase the responsibility of individuals for committing cybercrimes; legislative approval of the legal validity of electronic evidence for cyber intruders; definition of a clear scheme of relations and responsibility of the client-bank, the sender, the recipient, in the event of unlawful write-off of client funds; legislatively regulate the identification of Internet users; to legally approve the need to select identification data by an Internet service provider when concluding transactions for such services; assignment of online stores to specific taxpayers; approve the need to ensure the protection of remote service systems with several levels of protection – logins, passwords, SMS messages, etc.; consolidate a mandatory free service – the provision of mandatory online reporting by financial service providers about all financial transactions and attempts to carry them out, regardless of the amounts and types of transactions; the obligation to banking institutions to make outgoing payments only within the limits of the account balance; approval of an unchanged limit on cash withdrawals from ATMs in the post-transaction time; mandatory certification of all electronic means of payment; equipping the ATM network of banks with anti-skimming means.

Cybersecurity models are complex organizational, technical, managerial, and control measures to ensure cybersecurity, namely: approval of certain standard rules and schemes for identifying typical, atypical, suspicious, questionable transactions in the remote service system; approval of limits for transactions in the remote service system and the Internet; maintaining a database of suspicious and dubious clients; maintaining a "black list" customer base; issuing plastic cards to customers with a chip having a higher level of protection; two-

channel authentication; additional confirmation of remote payments via a financial phone number; the use of secure special tokens for digital signatures of employees and customers; ensuring the possibility of generating an electronic key personally by a client without the participation of employees of a banking institution; ensuring that customers are notified of all financial transactions and attempts to carry them out; binding of an electronic digital signature to a specific list of serial numbers of computer equipment; periodic traffic analysis; systematic review of the ATM network in order to identify foreign devices.

We also note that considering different objects and systems simultaneously, it is worth highlighting the importance of the convergence concept, which means finding compromises, combining and bringing together distinctive concepts. The convergence of systems presupposes the fusion of systems into a single indivisible whole; the process of their universalization by combining common elements, and increasing the number of functions of such systems, their capabilities, and advantages; performance by the elements of systems of different but similar tasks according to the same principles to obtain an additional effect. Thus, the convergence results determine the formation of compromise solutions, achieving an equilibrium position, joint development, common stability and stabilization.

Moreover, the convergence of systems can be implemented based on various models, such as situational-simulation-expert modeling (based on the use of several types of submodels, it involves a multi-aspect consideration of the issue under study, allows simulating both a real situation and an artificial one); model of absolute convergence (convergence and increase in the levels of development of homogeneous objects of research without the introduction of additional conditions); conditional convergence model (provides for a negative relationship between average growth rates when controlling factors appear); direct convergence model (the process of rapprochement and

compromise based on existing traditions under the influence of certain factors); model of indirect convergence (the process of convergence based on the latest borrowed concepts, integration of objects); etc.

In turn, the convergence of financial monitoring and cybersecurity systems implies the development of a financial monitoring system for cyber financial transactions; ensuring cyber protection of financial transactions of the banking system; increasing the cyber resilience of the financial system to money laundering and terrorist financing. Due to the convergence of financial monitoring and cybersecurity systems, the following latest measures are being formed to help prevent, combat and forecast modern financial and cybercrimes: legislative approval of rules, instructions, protocols, regulations, requirements, standards, leverages, responsibility, pricing policy, government programs for financial cybersecurity issues; approval of the obligation to conduct a self-assessment of the state of financial cyber protection by banking institutions; prohibition or restriction of the use of foreign software systems and security systems in the national financial system; digital transformation, and the transition to a modern cloud environment; introduction of information security tools in the banking sector; implementation of artificial intelligence tools; the use of a multi-layered system for protection and combating financial cyber threats; the use of the latest software systems to protect the operating systems of banks; introduction of firewalls; introduction of intrusion detection systems into the automated banking system; provision of enhanced protection of communication with remote structural elements of banking institutions; ensuring enhanced transparency, identification and authorization during the operation of remote online banking services; introduction of the latest developments in automated incident response systems for information, financial and cyber security of banks; introduction of robotization for performing

regular banking procedures in real time; counteraction to social engineering, psychological manipulation of people by committing unconscious or illegal actions; use of anti-fraud services; services to combat financial fraud; using the method of enriching the header of online requests of users of web resources; etc.

The issue of combating money laundering, countering terrorism financing, the proliferation of weapons of mass destruction will remain acute for Ukraine and the world for a long time. Along with this, the problem of cyber security is no less urgent when it becomes necessary to ensure confidentiality, security, integrity, availability, and authenticity of information resources in this area. In-depth studies of these two vectors involve the generalization, structuring of the theoretical achievements of the world and domestic literature in terms of defining the basic concepts, goals, objectives, directions, and models of the issues under study, as well as the development by the authors of their conclusions on these aspects. Moreover, the main focus of the study is on the fact that both sets of measures, financial monitoring, and cybersecurity, are becoming one of the main tasks of the world community, the leaderships of countries, government agencies, and society.

In general, the proposed convergence of financial monitoring and cybersecurity systems can be taken as a basis, adapted to address a wide range of economic and financial security issues and combat money laundering and other problematic issues of the financial market.

2.2. Assessing the convergence level of the cyber security system and counteraction of money laundering

To assess the efficiency of the convergence, we will use the approach proposed by Yarovenko (2020) to evaluate the level of threat to information security, which consists in determining the integral indicator. However, for our study, it is necessary to calculate two composite indicators, one of which will characterize the level of national cybersecurity, and the other will calculate the level of countering money laundering.

At the first stage, we select the input data for calculations. The first group was formed by global indices used to measure individual areas of a country's cybersecurity from the official website of the e-Governance Academy Foundation for 2018: the Global Cybersecurity Index assesses the capabilities of countries worldwide to counter cyber threats in the world and determines their weaknesses and potential opportunities; the National Cyber Security Index determines the state of readiness of an individual country to counter cyber threats and manage cyber incidents; the Networked Readiness Index allows assessing the level of technological readiness of the country to implement modern information systems and technologies to automate various processes of the life of society; the Digital Development Level shows the degree of digitalization of the country. Each of these indicators characterizes the state of the country's cybersecurity, taking into account its various aspects. Therefore, their analysis will form a comprehensive vision of its development and the possibility of integration.

The second group of indicators was formed by indices that allow assessing the state of the system for countering money laundering and the financing of terrorism. They included: the Political Stability Index, which allows assessing the probability of destabilization of the country's government using unconstitutional and violent measures, which is favorable or

unfavorable, depending on the importance of the factor for money laundering; the Government Effectiveness Index, which measures its quality, which consists in its independence from political pressure, the efficiency of government services, the level of trust in its activities; the Ease of Doing Business characterizes the conditions for doing business in the country, which affects the risk of growth in the shadow sector and money laundering; the Crime Index characterizes the level of crime in the country, affecting the instability of the social, political and economic spheres; the Global Terrorism Index indicates the level of terrorist activity, which affects the risks of money laundering and financing of terrorism; the Financial Secrecy Index testifies to the degree of protection of financial transactions used by many countries to create favorable conditions for the concealment of illegal income and the implementation of financial transactions, the sources of which are criminal. Data for selected indicators were taken from the official source of the World Bank. Empirical data from both groups correspond to 76 countries for 2018 since the complete set of values characterizes this period.

Kuzmenko et al. (2021) carried out a preliminary analysis of the convergence of cybersecurity and financial monitoring systems, which made it possible to prove the relevance of these particular indicators for further research.

We will normalize the input data at the second stage to bring them to a comparable form. For this purpose, we use nonlinear normalization, which smooths out data that have different signs and values more efficiently than other methods (Formula (2.1)):

$$Z_{ij} = \left(1 + e^{\frac{\bar{y}_j - y_{ij}}{\sigma(y)}} \right)^{-1}, \quad (2.1)$$

where Z_{ij} – the normalized value of the j -th indicator selected to assess the convergence of the cybersecurity and anti-money laundering (AML) system, in the context of the i -th country;

\bar{y}_j – average value of the j -th indicator within the list of countries under consideration;

y_{ij} – the actual value of the j -th indicator in the context of the i -th country;

$\sigma(y_j)$ – the average square deviation of the j -th indicator within the list of countries under consideration.

All the selected indicators are incentives in terms of their influence on the system's state, except for two – the Crime Index and Financial Secrecy Index, which are disincentives. Therefore, to take their values correctly when forming an integral index, it is necessary to subtract their calculated normalized value from one.

At the third stage, we transform the normalized values of the selected indicators to the dimensionless Harrington desirability scale using the formula (2.2):

$$d_{ij} = \exp(-\exp(-Z_{ij})), \quad (2.2)$$

where d_{ij} - an intermediate value of the j -th indicator selected for assessing the convergence of the cybersecurity and AML systems, in the context of the i -th country, reduced to the dimensionless Harrington desirability scale;

Z_{ij} – a normalized value of the j -th indicator, in the context of the i -th country.

To further form an integral indicator for assessing the convergence of the cybersecurity and anti-financial fraud systems, it is necessary to investigate the behavior of the

Harrington-Mencher transformation curve, which characterizes d_{ij} the dependence on the actual values of each input indicator. For this purpose, we visualize the dependencies at the fourth stage. As a result, it was found that most indicators are characterized by the first type of curve – S-shaped, ascending, symmetrical. The Crime Index and Financial Secrecy Index correspond to the fourth type – S-shaped, descending, symmetric curve. Examples of the obtained curve plots of the first and second types are shown in Figures 2.1 and 2.2.

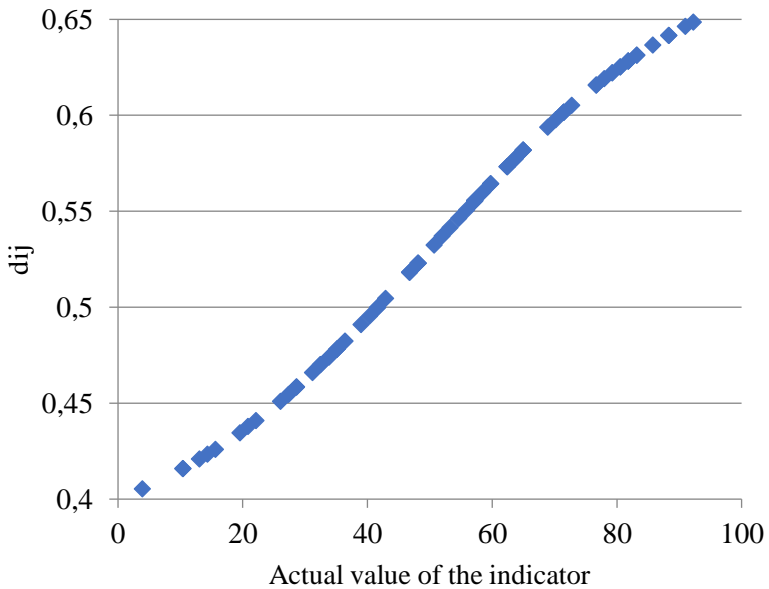


Figure 2.1. Type 1 curve plot for the National Cybersecurity Index

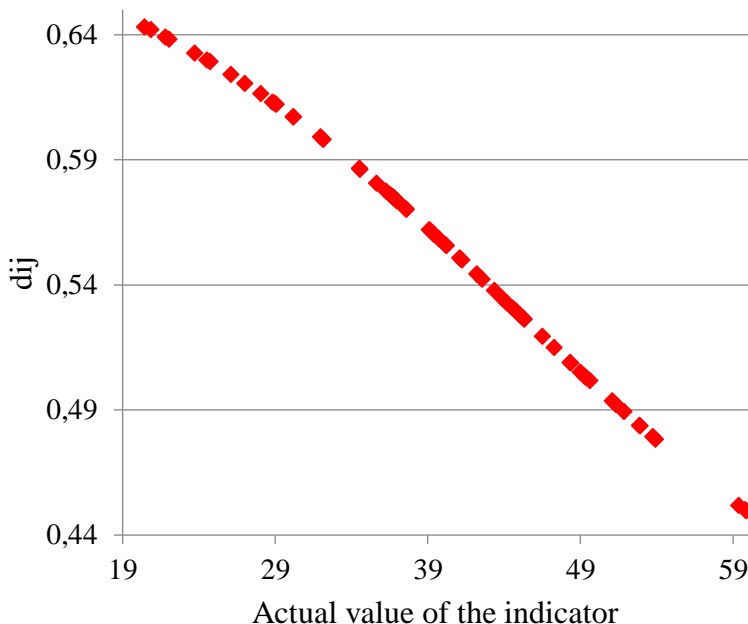


Figure 2.2. Type 4 curve plot for the Crime Index

At the fifth stage, we formalize the Harrington-Mencher transformation within the dependency selected in the previous step d_{ij} from the actual values in the context of each input indicator. Thus, we calculate the intermediate values of indicators for assessing the convergence of cybersecurity and anti-fraud systems, considering their reduction to a dimensionless Harrington-Mencher desirability scale according to a specific curve type.

For indicators, dependencies for which are described by type 1 curve, we use the formula (2.3):

$$d_{ij}^* = \exp \left(- \exp \left(- \left(9 \left(\frac{Z_{ij} - \min_i Z_{ij}}{\max_i Z_{ij} - \min_i Z_{ij}} \right)^{1.927} - 2 \right) \right) \right), \quad (2.3)$$

where d_{ij}^* - the intermediate value of the j -th indicator selected to assess the convergence of cybersecurity and AML systems, in the context of the i -th country, reduced to the dimensionless Harrington-Mencher desirability scale;

$\min_i Z_{ij}$ - the minimum value of the normalized j -th indicator in the context of the i -th country;

$\max_i Z_{ij}$ - the maximum value of the normalized j -th indicator in the context of the i -th country.

For indicators, which dependencies are described by type 4 curve, we use the formula (2.4):

$$d_{ij}^* = \exp \left(- \exp \left(- \left(9 \left(\frac{\max_i Z_{ij} - Z_{ij}}{\max_i Z_{ij} - \min_i Z_{ij}} \right)^{1.927} - 2 \right) \right) \right). \quad (2.4)$$

At the sixth stage, it is necessary to determine the weights of indicators to calculate the generalized function. For this purpose, we conduct a canonical analysis that will determine the degree of dependence between two sets of indicators and calculate their canonical weights used for integral evaluation. The analysis was performed using the canonical analysis module of the

STATISTICA analytical package. The results are shown in Figure 2.3.

Canonical Analysis Summary (Konvergentcia2.sta)		
Canonical R: .93762		
Chi ² (24)=200.41 p=0.0000		
N=76		
	Left Set	Right Set
No. of variables	4	6
Variance extracted	100.000%	83.8201%
Total redundancy	70.3694%	47.9580%
Variables:	1	Global Cybersecurity Index
	2	Political stability index
	3	Networked Readiness Index
	4	Government effectiveness index
	5	National Cyber Security Index
	6	Ease of doing business
		Digital Development Level
		Crime Index
		Global Terrorism Index
		Financial Secre Index

Figure 2.3. Results of the canonical analysis

Figure 2.3 shows that the value of the canonical correlation is $R = 0.93762$. It indicates the presence of a robust correlation between many factors characterizing the level of development of cybersecurity and the anti-fraud system. The statistical significance of the correlation coefficient is confirmed by the high value of the Pearson's test ($\chi^2 = 200,00$), the significance level of which does not exceed 0.05 ($p = 0.0000$). The redundancy value for the left set formed by cybersecurity indices is 70.3694%. It indicates that the factors of the right-wing set that correspond to the indicators related to counteraction to financial fraud explain the volatility of cybersecurity indicators by 70.3694%, which indicates a high value of influence. The development of the AML system in a country to a certain extent depends on its cybersecurity since cybersecurity factors by 47.9580% explain the variability of factors characterizing the level of counteraction to financial fraud. Although the obtained value is moderate, it is sufficient to justify the impact of indicators such as cybersecurity on economic processes in the country.

Specific values of the canonical roots, and the obtained statistical characteristics, allowed concluding that three canonical roots are significant. However, to obtain reliable estimates of their loads for three pairs of canonical variables, it is necessary to have a sample that will exceed the amount of initial data by 40-60 times (Halafyan, 2007). Therefore, it was decided that to determine the weights, it is advisable to use the value of the first canonical root, for which the canonical R^2 will have the largest value of 0.8791. Based on these considerations, we use the canonical weights defined for the first root for further consideration (Figures 2.4-2.5).

Variable	Canonical Weights, left set (Konvergentcia2.			
	Root 1	Root 2	Root 3	Root 4
Global Cybersecurity Index	0,313261	-0,781709	0,63400	1,14199
Networked Readiness Index	0,264381	-0,713150	-1,56282	-0,64848
National Cyber Security Index	-0,021339	0,026080	0,91519	-1,29626
Digital Development Level	0,557799	1,355225	0,21392	0,67528

Figure 2.4. Canonical weights for cybersecurity indicators

Variable	Canonical Weights, right set (Konvergentcia2.			
	Root 1	Root 2	Root 3	Root 4
Political stability index	-0,269140	0,923250	1,32088	0,990101
Government effectiveness index	0,780788	0,200480	-1,68893	0,203985
Ease of doing business	0,341713	-0,672184	0,64477	-0,816572
Crime Index	0,050110	0,111717	0,73583	-0,231753
Global Terrorism Index	0,009265	-0,080100	1,17396	1,219424
Financial Secrece Index	-0,091481	0,070369	0,35190	-0,048788

Figure 2.5. Canonical weights for indicators that characterize the anti-money laundering level

It turned out that the obtained canonical weights are both positive and negative, which indicates a positive and negative contribution of indicators to the value of the root. However, to determine a generalized function, their values must vary from 0 to 1, so their modulus will take the corresponding negative weights.

At the seventh stage, two integral indexes are calculated to evaluate the development of cybersecurity and AML system. For this purpose, it is necessary to use formulas (2.5) - (2.6):

$$IC_i = \sqrt{\sum_{j=1}^n a_j \prod_{j=1}^n (d_{ij}^*)^{a_j}}, \quad (2.5)$$

$$IP_i = \sqrt{\sum_{j=1}^m a_j \prod_{j=1}^m (d_{ij}^*)^{a_j}}, \quad (2.6)$$

where IC_i – an integral index that characterizes the level of development of the cybersecurity system for the i-th country;

IP_i – an integral index that characterizes the level of development of the AML system for the i-th country;

n – a number of cybersecurity indicators of a country ($n = 4$);

m – a number of indicators characterizing the development of the AML system ($m = 6$);

a_j – weights of the corresponding j-th input indicator of cybersecurity or anti-money laundering;

d_{ij}^* – an intermediate value of the j-th indicator of cybersecurity or anti-money laundering in the context of the i-th country, reduced to a dimensionless Harrington-Mencher desirability scale.

We interpret the calculated values of the integral indicators using a qualitative assessment, namely: if the obtained value is in the range of 0.80 - 1.00, then the state of development of the country corresponds to “very good”; from 0.63 to 0.80 – “good”; from 0.37 to 0.63 – “satisfactory”; from 0.20 to 0.37 – “bad”; from 0.00 to 0.20 – “very bad”.

We visualize the obtained values using charts with maps built using the MS Excel software product. The results are shown in Figures 2.6-2.7.

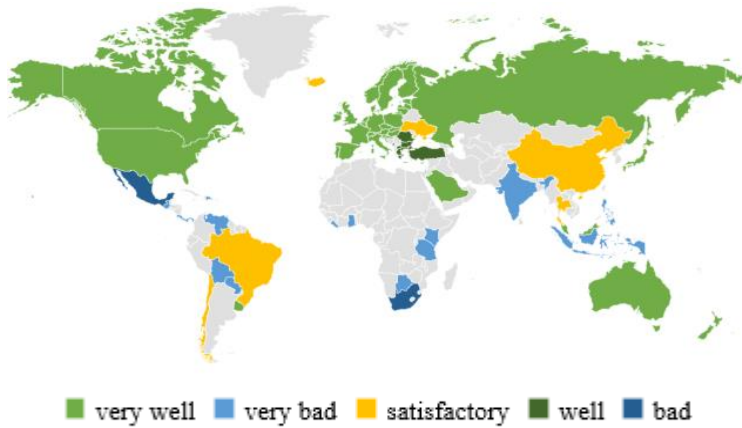


Figure 2.6. Map of the distribution of countries according to the integral index characterizing the development of their cybersecurity system

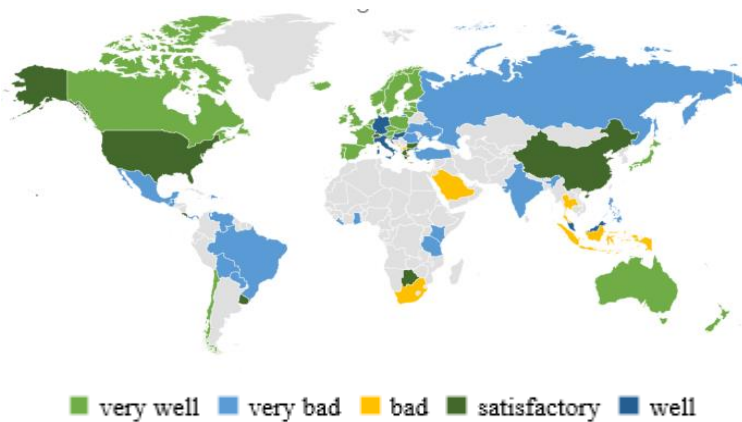


Figure 2.7. Map of the distribution of countries according to the integral index characterizing the development of the AML system

According to the integral level of cybersecurity, 38 countries, such as Austria, Australia, Canada, Denmark, Estonia, Finland, Germany, the United Kingdom, the United States, and others, have a “very good” rating (see Fig. 2.6). Thus, the vast majority of these countries are developed. Bulgaria, Greece, Mauritius, Montenegro, North Macedonia, Turkey, and Romania have a cybersecurity level that meets the “good” rating. A satisfactory level is typical for such countries as Ukraine, Brazil, Chile, China, Iceland, Malta, and Thailand. Twenty-four countries were rated “bad” and “very bad”: Barbados, Bolivia, Botswana, Dominican Republic, Ghana, Guatemala, India, Indonesia, Kenya, Liberia, and other developing or least developed countries. In general, the level of cybersecurity corresponds to the country’s economic development level. The developed countries, respectively, have potent capabilities for creating conditions for the cyber defense of various objects. Developing countries, the least developed, have problems in the field of cybersecurity caused by the lack of highly qualified specialists in this area, insufficient investment, a weak level of legal support in this area, etc.

In terms of the integral level of combating financial fraud, 28 countries received a rating of “very good” (see Fig. 2.7): Australia, Austria, Belgium, Canada, Ireland, the Netherlands, Norway, Great Britain, Sweden, Czech Republic, etc. Countries such as Croatia, Germany, Hungary, Italy, Malaysia, Malta, and Singapore have a “good” level of countering money laundering. Botswana, Bulgaria, China, Costa Rica, Greece, Luxembourg, Seychelles, Switzerland, the United States, and Uruguay received a “satisfactory” rating. Nine countries received the “bad” level, and 22 countries – “very bad”. They include Bolivia, Brazil, India, Ukraine, Russian Federation, Mexico, South Africa, Thailand, Indonesia, etc. Thus, some countries with a high level of crime and terrorism, armed conflicts, low economic development are quite attractive for money laundering

and terrorist financing. Therefore, the system of countering such activities is relatively weak and not developed. Countries with a high level of financial secrecy create favorable conditions for money laundering. Today, they are Switzerland, Luxembourg, and the United States.

To determine the level of convergence of cybersecurity and anti-fraud systems, we find the arithmetic mean of two integral indices. The calculation results are presented as a map of the distribution of countries by the level of convergence of cybersecurity and anti-fraud systems (see Fig. 2.8).

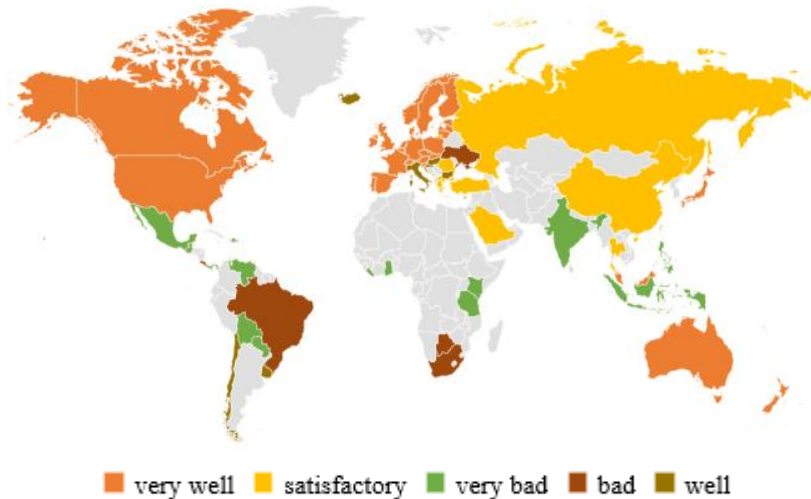


Figure 2.8. Map of the distribution of countries by the level of convergence of cybersecurity and AML systems

Subject to the convergence of the cybersecurity and anti-fraud system for countries with a low level of resistance, their potential capabilities will be enhanced due to the cybersecurity system. Thus, comparing the results presented in Figures 2.6-2.8, it is possible to see that countries such as Bahrain, Botswana, Brazil, Brunei, Bulgaria, Chile, Costa Rica, Iceland, Israel, Luxembourg, Malta, Montenegro, North Macedonia,

Romania, the Russian Federation, Saudi Arabia, Seychelles, Singapore, Switzerland, Thailand, Turkey, Ukraine, the United States, and Uruguay will get a positive effect from the convergence process.

The proposed methodology for the integral assessment of the convergence of the financial monitoring system and cybersecurity system allows developing scenarios by ranking countries using the qualitative assessment scale proposed by Harrington-Mencher. However, the integral representation does not conclude the system's efficiency for ensuring the convergence of the financial monitoring system and cybersecurity system. Thus, it is necessary to carry out a structural analysis of its components, which will allow assessing both the current state of the components of the integral indicator of convergence of the financial monitoring system and cybersecurity system and determine reserves for its improvement. Thus, it is necessary to analyze the efficiency of the system for ensuring the convergence of the financial monitoring system and the cybersecurity system and provide recommendations to improve it.

The study considers indicators that characterize the level of development of cybersecurity in the country and countering money laundering and the financing of terrorism. The Harrington-Mencher approach allowed generating two integral indicators. Assessment of the level of cybersecurity revealed that developed countries have a high level of cyber defense. The lowest ratings were given to countries that are least developed or developing and have a low level of development. According to the integral assessment of the level of counteraction to money laundering, it is established that countries with a high level of crime, terrorism, low quality of public administration, military conflicts, and a high level of financial secrecy have significant problems in this area. This contributes to the possibility of

money laundering and reduces the ability of the system to counteract such activity.

2.3. DEA-analysis of the effect of financial monitoring and cybersecurity systems integration

Depending on the purpose of the analysis, different approaches are used in the scientific literature and practice. The following are considered traditional: the classical Du Pont Return on Equity model, the activity-based profitability analysis by M. Meyer and W. Marshall, Management of Results by R. Kaplan and D. Norton, the analysis method based on the analysis of cash flows.

The main disadvantages of these methods are that their use is advisable for analyzing the efficiency of economic activity and involves calculating various coefficients to draw a conclusion. In the case of assessing the effectiveness of the system for ensuring the convergence of the financial monitoring system and cybersecurity system, it is advisable to use mathematical methods that allow assessing the parameters relative to the values that are best in the group of analyzed objects. That is why the DEA-method (Data Envelopment Analysis), proposed by A. Charnes, W. W. Cooper, and E. Rhodes in 1978, was used for the study (Charnes et al., 1978). This tool does not depend on the purpose of the analysis. It is used in many industries to assess the efficiency of complex systems by solving an optimization task of linear programming. Its purpose is to determine the efficiency of a system based on the ratio of its outputs and inputs. However, it is necessary to consider the maximum resource output at a given input level or the minimum resource level at a given output level.

We selected input data (in subsection 2.2) based on the canonical analysis and calculation of the integral indicator of convergence of the financial monitoring system and

cybersecurity system, namely: Global Cybersecurity Index; National Cybersecurity Index; Networked Readiness Index; Digital Development Level; Political Stability Index; Government Efficiency Index; Ease of Doing Business; Crime Index; Global Terrorism Index; Financial Secrecy Index. These indicators formed a database of input data for 76 countries for 2018. The integral index of convergence of the financial monitoring system and cybersecurity system proposed in subsection 2.2 will serve as an initial parameter, an indicator of the generalized efficiency level.

Since the DEA method is effective for data with similar characteristics, it is advisable to form clusters of countries. Sorting was carried out according to the integral index of convergence of the financial monitoring system and cybersecurity system, and seven groups of countries were identified.

Thus, cluster 0 includes 12 countries: Finland, Australia, Austria, Denmark, Canada, Ireland, Sweden, New Zealand, Norway, Estonia, Belgium, and Portugal. Cluster 1 includes Spain, Lithuania, Slovenia, Latvia, the Netherlands, Japan, Great Britain, France, Cyprus, Czech Republic, Germany, and Slovakia. Cluster 2 includes Poland, Malaysia, Singapore, Switzerland, the USA, Luxembourg, Hungary, Croatia, Mauritania, Italy, Iceland, and Uruguay. Cluster 3 includes Chile, Malta, Israel, Bulgaria, Greece, Saudi Arabia, Russia, Montenegro, Brunei, North Macedonia, Bahrain, and China. Cluster 4 includes Turkey, Thailand, Romania, Costa Rica, South Africa, Seychelles, Ukraine, Brazil, Botswana, Mexico, Indonesia, Panama. Cluster 5 includes Trinidad and Tobago, Barbados, Philippines, India, Dominican Republic, Ghana, Dominica, Paraguay, Kenya, Grenada, Vanuatu, Venezuela. Cluster 6: Bolivia, Guatemala, Tanzania, Liberia.

The DEA method will be used to determine the efficiency of convergence of the financial monitoring system and

cybersecurity system, taking into account the country's potential. Efficiency will be achieved when the level of countering threats for a specific country cannot be increased while leaving the country's level of development and security at the same level. This is also possible if a decrease in the country's level of development and security leads to changes in the level of countering cyber threats. Based on the above, it is possible to create an initial DEA model (Charnes et al., 1978), which will be used to assess the efficiency of the country's information security level using the formula (2.7):

$$\max \theta_s = \frac{\sum_{p=1}^z u_{ps} y_{ps}}{\sum_{i=1}^m v_{is} x_{is}} \quad (2.7)$$

$$\left\{ \begin{array}{l} \frac{\sum_{p=1}^z u_{ps} y_{pj}}{\sum_{i=1}^m v_{is} x_{ij}} \leq 1, \\ s, j = \overline{1, n}, \\ u_p, v_i \geq 0, \\ y_p, x_i \geq 0. \end{array} \right.$$

where θ – the level of efficiency of convergence of the financial monitoring system and cybersecurity system for a particular country, defined as the coefficient between the weighted sum of outputs and inputs;

u_p – output weights that maximize the performance of the unit being evaluated θ ;

v_p – input weights that maximize the performance of the unit being evaluated θ ;

y_p – p -th characteristic of conditional outputs, i.e., values of the index of convergence of financial monitoring and cybersecurity systems for each country;

x_i – i -th characteristic of conditional inputs, i.e., values of indicators of the financial monitoring and cybersecurity systems.

Constraints (2.7) state that the output-to-input ratio cannot exceed 1 for each θ . Therefore, the specified fractional problem should be converted to a linear one, significantly simplifying its further use. Thus, there are two types of DEA models – CCR (Charnes A., Cooper W. and Rhodes E.), which was proposed by Charnes A., Cooper W. and Rhodes E. in 1978 (Charnes et al., 1978), and BCC (Banker R., Charnes A. and Cooper W.), which was developed based on the CCR model in 1984 by Banker R., Charnes A. and Cooper W. (Banker et al., 1984). Each of these models (2.8) – (2.11) is focused on input (resources) and output (resulting indicators):

$$\begin{cases} \max_{u,v} \theta_s = \sum_{p=1}^z u_{ps} y_{ps} \\ \sum_{i=1}^m v_{is} x_{is} = 1 \\ \sum_{p=1}^z u_{ps} y_{pj} - \sum_{i=1}^m v_{is} x_{ij} \leq 0 \\ u_p, v_i \geq \gamma \end{cases} \quad (2.8)$$

$$\begin{cases} \max_{u,v,k} \theta_s = \sum_{p=1}^z u_{ps} y_{ps} + k_s \\ \sum_{i=1}^m v_{is} x_{is} = 1 \\ \sum_{p=1}^z u_{ps} y_{pj} + k_s \leq \sum_{i=1}^m v_{is} x_{ij} \\ u_p, v_i \geq \gamma \\ k_s - \text{unconstrained} \end{cases} \quad (2.9)$$

$$\begin{aligned}
\min_{\alpha, \beta, k} \theta_s &= \sum_{i=1}^m \beta_i x_{is} - k_s \\
\left\{ \begin{array}{l} \sum_{p=1}^z \alpha_p y_{ps} = 1 \\ \sum_{i=1}^m \beta_i x_{ij} - k_s \geq \sum_{p=1}^z \alpha_p y_{pj} \\ \alpha_p, \beta_i \geq \gamma \\ k_s - \text{unconstrained} \end{array} \right. & \quad (2.10)
\end{aligned}$$

$$\begin{aligned}
\min_{\alpha, \beta} \theta_s &= \sum_{i=1}^m \beta_i x_{is} \\
\left\{ \begin{array}{l} \sum_{p=1}^z \alpha_p y_{ps} = 1 \\ \sum_{i=1}^m \beta_i x_{ij} - \sum_{p=1}^z \alpha_p y_{pj} \geq 0 \\ \alpha_p, \beta_i \geq \gamma \end{array} \right. & \quad (2.11)
\end{aligned}$$

where γ – a small positive real number that eliminates the possibility of variables acquiring a zero value.

The CCR (2.8) and BCC (2.9) models are Input-oriented models, i.e., they aim to assess the efficiency of the distribution of indicators that characterize financial monitoring and cybersecurity systems, thus helping to identify structural inefficiency of the specified indexes. The CCR (2.10) and BCC (2.11) models are Output-oriented, i.e., they allow evaluating the efficiency of convergence of the country's financial monitoring and cybersecurity systems by determining the maximum values of the convergence index of the financial monitoring and

cybersecurity systems provided that the values of indicators are set that characterize financial monitoring and cybersecurity systems.

DEA analysis was performed in the Frontier Analyst analytical package, allowing calculations based on CCR and BCC models (Banxia Software, 2021). Since the demo version was used, 12 representatives were selected for the study in each cluster of countries, for which Data Envelopment Analysis was conducted. The minimum value of the weights was established based on the results of the canonical analysis in the STATISTICA analytical platform, which allowed determining the proportion of their values in the total population. Thus, for the Global Cybersecurity Index, a weight was determined to be 0.3133, the Networked Readiness Index – 0.2644, the National Cybersecurity Index – 0.0213, the Digital Development Level – 0.5578, the Political Stability Index – 0.2691; the Government Efficiency Index – 0.7808; the Ease of Doing Business – 0.3417; the Crime Index – 0.0501; the Global Terrorism Index – 0.0093; the Financial Secrecy Index – 0.0915. The maximum value for the weights has been set at 100%, so the corresponding values are listed in proportion.

The CCR model is more restrictive than the BCC model. This is due to the fact that it is based on the consistency of returns to scale, and also allows for the scaling of inefficient sample units. The BCC model is based on a variable return on the scale and evaluates technical efficiency. Such a change in the input parameters can lead to a disproportionate output change, making it possible to evaluate most objects as efficient. Therefore, we use only the BCC model to determine synergistic effects.

We analyze the structural efficiency of the input indicators for the countries from cluster 1, obtained as a result of the analysis according to the Input-oriented CCR-model (Figure 2.8). The obtained values of all indicators are negative, i.e., ensuring the current level of convergence of the financial

monitoring and cybersecurity systems of the countries in cluster 1 occurs with the achievement of efficiency in each area – financial monitoring and cybersecurity. It can be seen that there is potential to ensure the level of convergence (8.51%). For these countries, the largest reserve is formed precisely according to the Global Terrorism Index, which indicates that there are no favorable conditions for money laundering and the financing of terrorism for these countries.

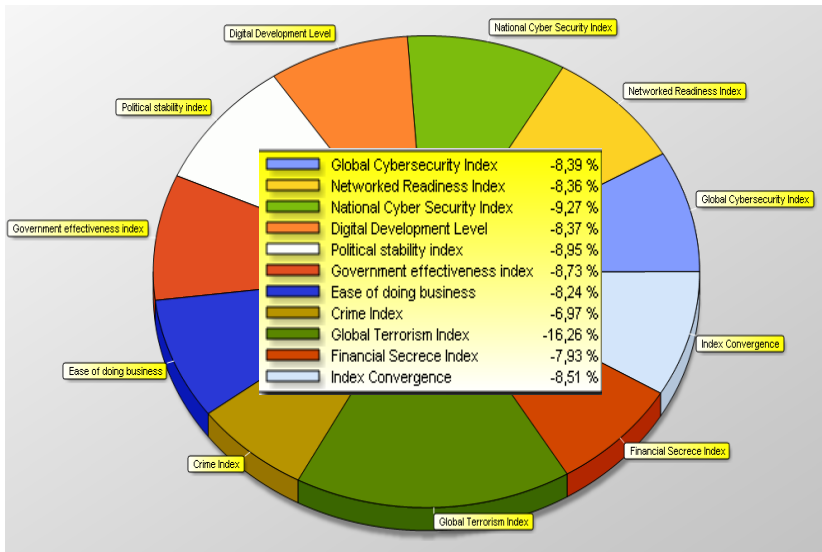


Figure 2.8. Efficiency results for the components of the convergence of the financial monitoring system and cybersecurity system of the countries in cluster 1 (according to the Input-oriented CCR-model)

We will analyze the potential for improving the convergence efficiency of the financial monitoring and cybersecurity systems in cluster 1, provided that the integral convergence index of the financial monitoring and cybersecurity systems is maximized. The results of the Output-oriented CCR-model are shown in

Figure 2.9. It shows that maximum growth of the convergence index for the financial monitoring and cybersecurity systems is possible by 6.6%. This can be achieved at the expense of potential reserves in the following indicators: the National Cybersecurity Index (-4.18%), the Crime Index (-36.48%). Thus, the countries from cluster 0 have, on the one hand, a high potential for cybersecurity development, sufficient to ensure an increase in the level of convergence. On the other hand, a low crime rate creates prerequisites for forming an effective financial monitoring system.

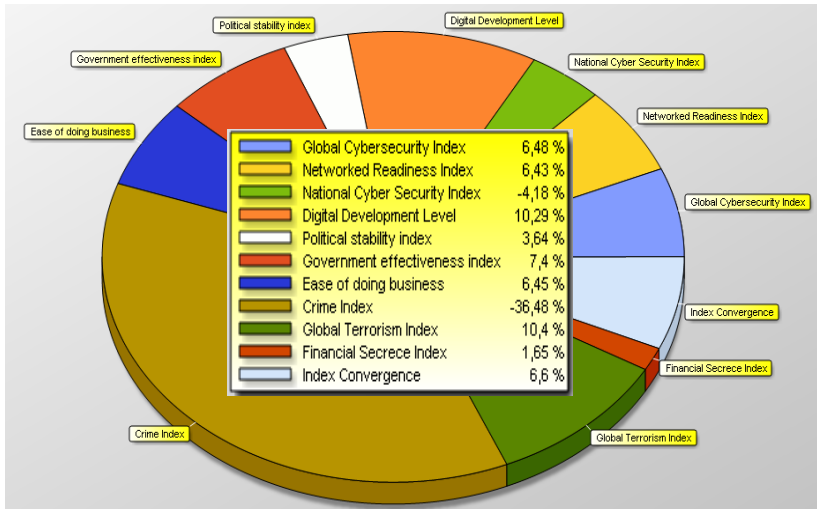


Figure 2.9. Efficiency results for the components of the convergence of the financial monitoring system and cybersecurity system of the countries in cluster 0 (according to the Output-oriented CCR model)

We analyze the structural efficiency of input indicators for the countries in cluster 1 (Figure 2.10). The obtained values of all indicators are positive, which indicates that it is impossible to achieve the level of convergence of the financial monitoring system and cybersecurity system due to the current state of their

functioning. Although the countries of this cluster have developed economies, there are problems at the national level that outweigh the implementation of the specified convergence.

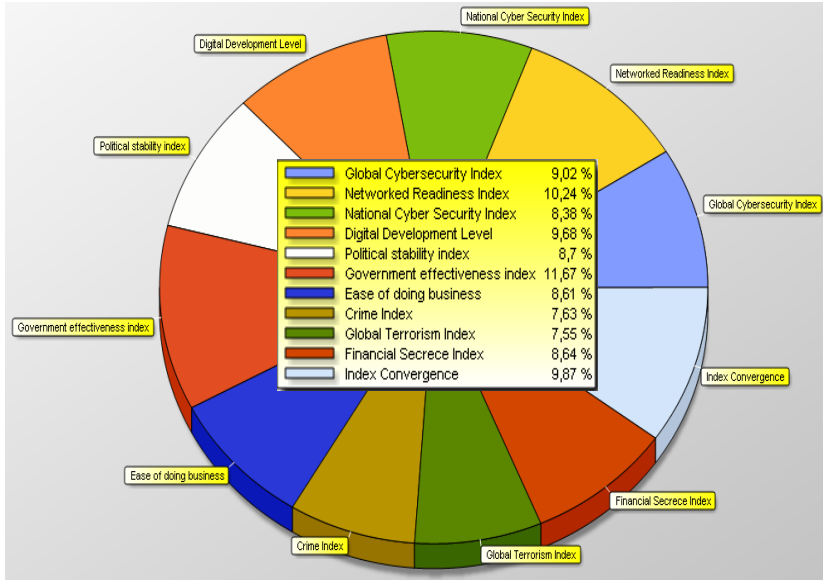


Figure 2.10. Efficiency results based on the convergence components of the financial monitoring and cybersecurity systems of countries in cluster 1 (using the Input-oriented CCR model)

The most significant improvement is required by the Government Efficiency Index, which needs to be increased by 11.67%, and the Networked Readiness Index (10.24%). To ensure the current level of convergence of the systems of countries in cluster 1, it is necessary to increase the efficiency of the functioning of all relevant areas that characterize the cybersecurity and anti-fraud system in the country.

We analyze the structural efficiency of the initial indicators for countries in cluster 1 (Figure 2.11).

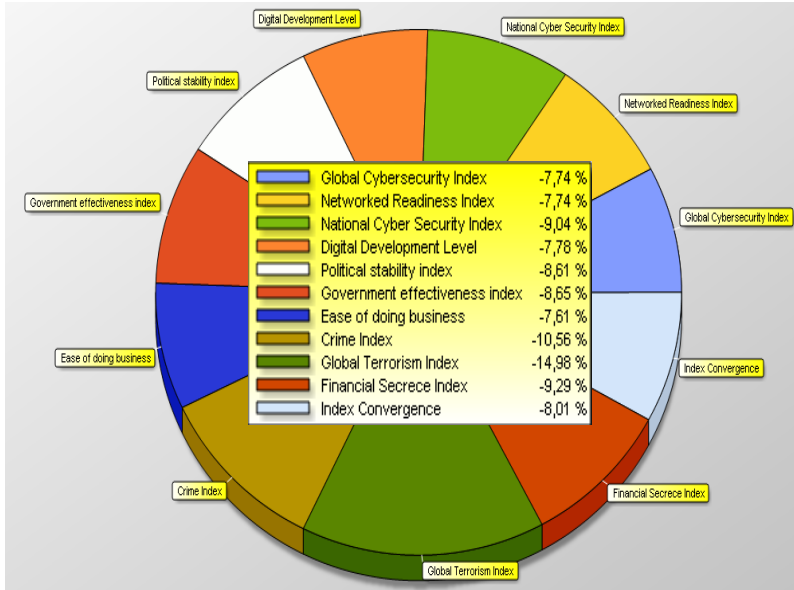


Figure 2.11. Efficiency results for the components of the convergence of the financial monitoring and cybersecurity systems of countries in cluster 1 (according to the Output-oriented CCR-model)

Analysis of the potential for improving the efficiency of convergence of financial monitoring and cybersecurity systems for cluster 1, provided that the integral convergence index is maximized, shows that it may maximally increase by 8.01%. This can be achieved through potential reserves in terms of indicators: the Global Cybersecurity Index (-7.74%), the Networked Readiness Index (-7.74%), the Digital Development Level (-7.78%), and the National Cybersecurity Index (-9.04%). Thus, countries in cluster 1 have significant cybersecurity potential, sufficient to ensure an increase in the convergence of systems. As for the anti-fraud system, these countries also have significant potential in this area, namely: the Political Stability Index (-8.61%); the Government Efficiency Index (-8.65%); the

Ease of Doing Business (-7.61%); the Crime Index (-10.56%); the Global Terrorism Index (-14.98%); the Financial Secrecy Index (-9.29%).

Countries in cluster 1 cannot reach the current level of convergence, but the existing potential can provide a maximum level that is lower than the current one.

We analyze the structural efficiency of input indicators for countries in cluster 2 (Figure 2.12).

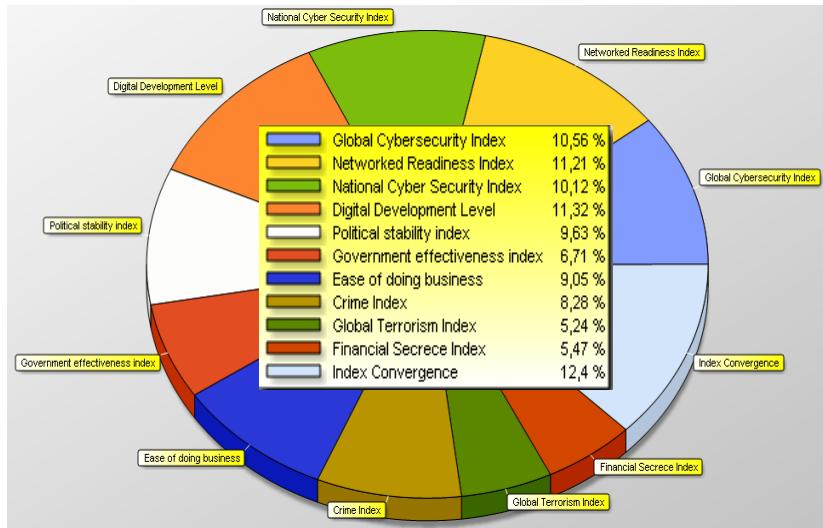


Figure 2.12. Efficiency results for the components of the convergence of the financial monitoring system and cybersecurity system for countries in cluster 2 (according to the Input-oriented CCR-model)

The obtained values of all indicators are positive, indicating that the countries of this cluster cannot reach the current level of convergence of the financial monitoring system and cybersecurity system, which requires growth by 12.4%. The most significant improvement is required by cybersecurity indices, which need to be increased by more than 10% each. The

results show that it is necessary to pay attention to cybersecurity to ensure an effective integration process. For example, this cluster includes the United States, which today ranks first among countries attacked by other countries. Moreover, this country is also a leader in carrying out cyber attacks on other countries. Therefore, the problem related to cyber defense is relevant for the countries of this cluster.

We analyze the structural efficiency of the initial indicators for countries in cluster 2 (Figure 2.13).

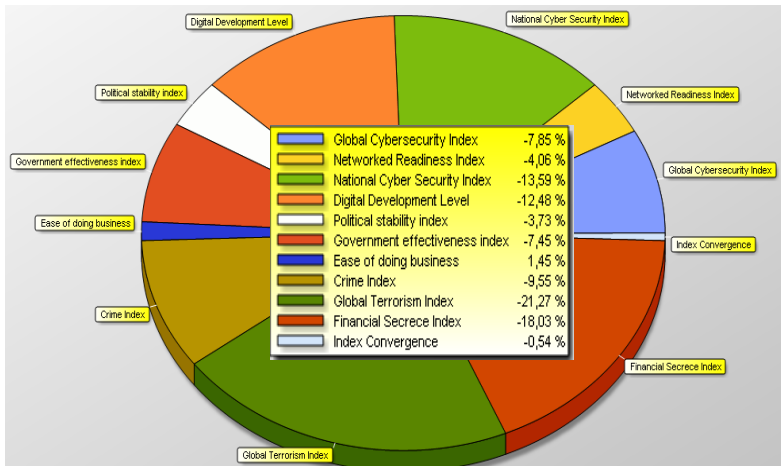


Figure 2.13. Efficiency results for the components of the convergence of the financial monitoring system and cybersecurity system for countries in cluster 2 (according to the Output-oriented CCR-model)

Analysis of the potential for improving the efficiency of convergence of financial monitoring and cybersecurity systems of cluster 2, provided that the integral convergence index is maximized, shows that it can maximally increase only by 0.54%. This can be achieved at the expense of potential reserves in the following indicators: the Global Cybersecurity Index (-7.85%), the Networked Readiness Index (-4.06%), the Digital

Development Level (-12.48%), and the National Cybersecurity Index (-13.59%). In other words, the countries of this cluster have a cybersecurity system potential sufficient to increase the level of system convergence slightly. These countries have the potential of a system for countering financial crimes, namely: the Political Stability Index (-3.73%); the Government Efficiency Index (-7.45%); the Crime Index (-9.55%); the Global Terrorism Index (-21.27%); the Financial Secrecy Index (-18.03%).

Thus, countries in cluster 2 cannot reach the current level of convergence. Still, the achievement of the maximum efficiency level is rather insignificant since there is an imbalance in financial monitoring and cybersecurity systems.

We analyze the structural efficiency of input indicators for countries in cluster 3 (Figure 2.14).

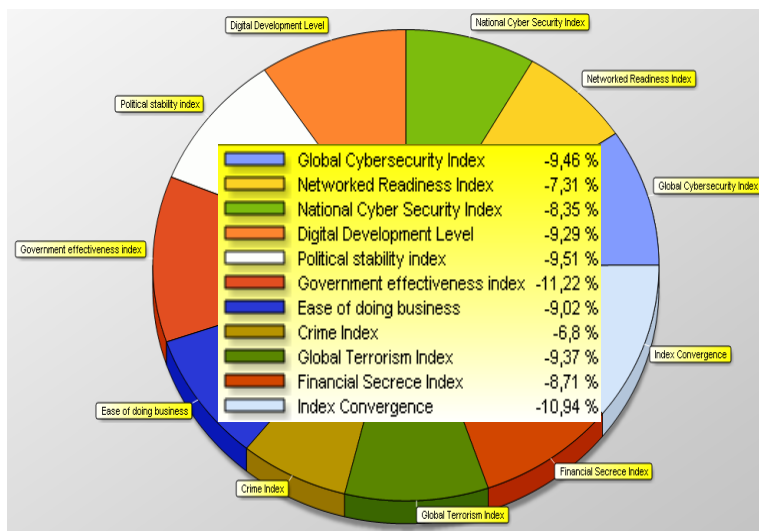


Figure 2.14. Efficiency results for the components of the convergence of the financial monitoring system and cybersecurity system for countries in cluster 3 (according to the Input-oriented CCR-model)

The obtained values of all indicators are negative, indicating the provision of the current level of convergence of the financial monitoring and cybersecurity system and its excess by 10.94%. At the same time, there is an achievement of efficiency in all indicators that characterize the financial monitoring and cybersecurity system. The highest value is typical for the Government Efficiency Index, increasing by 11.22%. In other words, the government's policy of these countries is so effective that opportunities are created to counteract money laundering. However, since the level of convergence of the countries from this cluster is lower than for countries in cluster 2, the result obtained only indicates that the countries have reached a certain level of convergence, which corresponds to the level of their economic development.

We analyze the structural efficiency of the initial indicators for countries in cluster 3 (Figure 2.15).

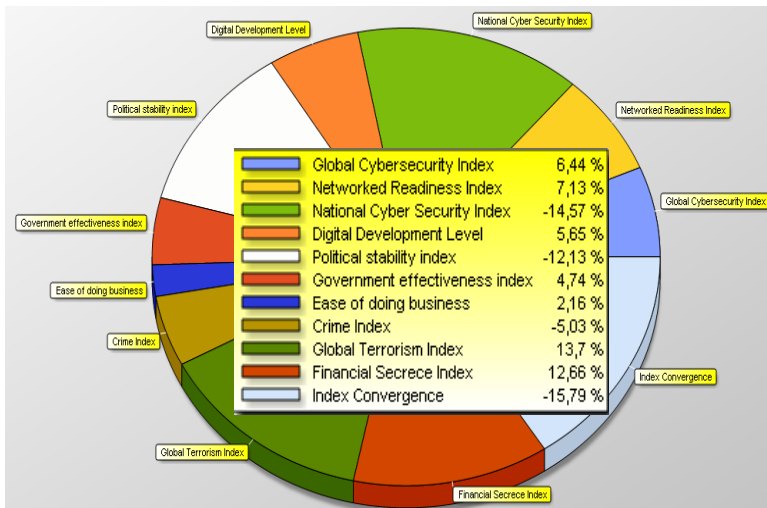


Figure 2.15. Efficiency results for the components of the convergence of the financial monitoring system and cybersecurity system for countries in cluster 3 (according to the Output-oriented CCR-model)

The results of the Output-oriented CCR-model (Fig. 4.8) show that the maximum increase in the convergence index of the financial monitoring system and cybersecurity system is possible by 15.79%. This can be achieved at the expense of reserves for the following indicators: the National Cybersecurity Index (-14.57%), the Political Stability Index (-12.13%), and the Crime Index (-5.03%). All other factors need to be improved accordingly to ensure the maximum level of system convergence. Since the actual level of convergence is achieved and its excess is observed, countries in cluster 3 have significant potential for an effective level of integration of the two systems.

We analyze the structural efficiency of input indicators for the countries in cluster 4 (Figure 2.16).

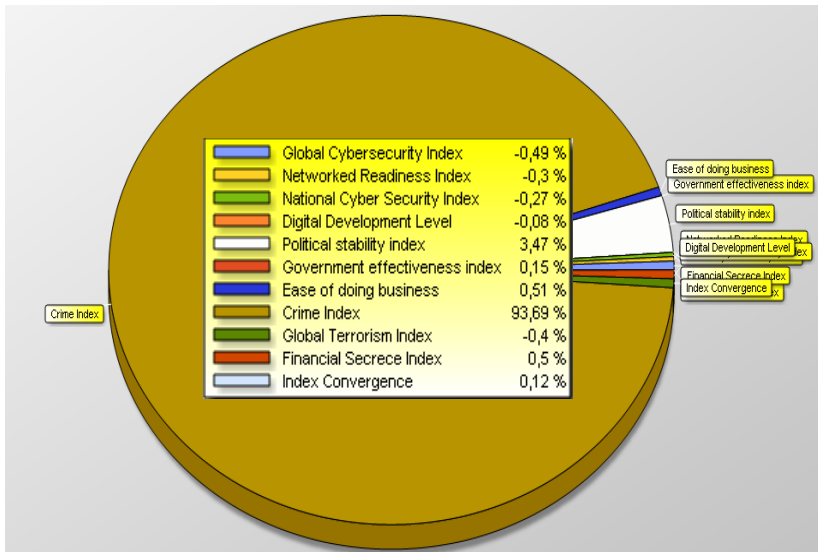


Figure 2.16. Efficiency results for the components of the convergence of the financial monitoring system and cybersecurity system for countries in cluster 4 (according to the Input-oriented CCR-model)

The resulting integral level indicates that its actual value

cannot be ensured by 0.12%. This is due to the high crime rate in these countries (93.69%). At the same time, the indicators that characterize the financial monitoring system are positive, i.e., these countries are characterized by favorable conditions for money laundering and financing of terrorism. However, the cybersecurity system has a small reserve of 1% for each security indicator, which indicates the possibility of supporting the financial monitoring system at the expense of the cybersecurity system.

We analyze the structural efficiency of output indicators for the countries in cluster 2 (Figure 2.17).

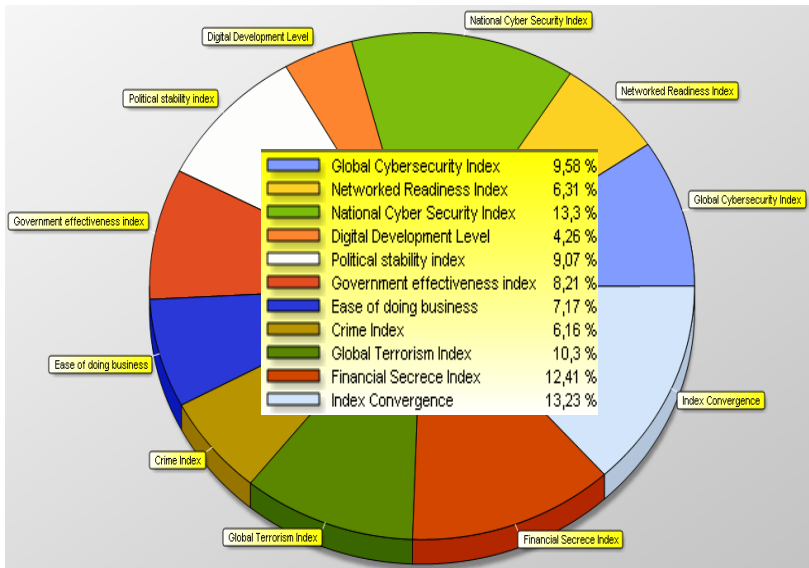


Figure 2.17. Efficiency results for the components of the convergence of the financial monitoring system and cybersecurity system for countries in cluster 4 (according to the Output-oriented CCR-model)

Results of the Output-oriented CCR-model show that only a maximum decrease in the convergence index of the financial

monitoring and cybersecurity systems by 13.23% is possible. Indicators do not have growth reserves because the values obtained are positive. This situation can only indicate that the countries of this cluster have severe problems with the organization of a system for countering financial cyber fraud and providing cyber protection. Therefore, integrating these systems will not contribute to obtaining a synergistic effect.

This cluster includes Ukraine. Indicators of its efficiency are shown in Figures 2.18-2.19.

Ukraine is a representative of cluster 4. The efficiency of the convergence of the financial monitoring and cybersecurity system is ensured at 100.0% in relation to other countries in the cluster (Figure 2.18). All indicators are either close to 0 or positive, which indicates that there are no reserves for increasing the level of integration for Ukraine. However, such an indicator as the Political Stability Index is critical – 99%. In other words, it requires significant improvement to ensure the efficiency of the information security system at the current level. This situation is caused by the political power crisis and a military conflict in the country. Since the impact of this indicator is quite significant, the primary task for ensuring the efficiency of system convergence should be to resolve this situation.

As for the maximum level that Ukraine can reach, it is possible to see on the slide that Ukraine has reached the maximum level of convergence at this stage. It is impossible to improve this value at the expense of the Global Cybersecurity Level (12.8%) and the Political Stability Index (86.3%) (Figure 2.19). This is quite logical since the risks currently existing in the country have a significant impact on the global environment. Accordingly, this situation requires the development of special cybersecurity measures and the improvement of the political situation in the country.

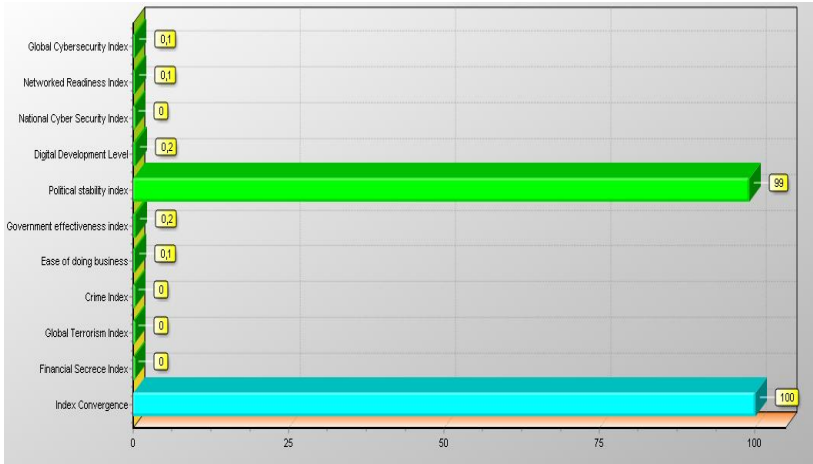


Figure 2.18. Efficiency results for the components of the convergence of the financial monitoring and cybersecurity system for Ukraine (according to the Input-oriented CCR-model)

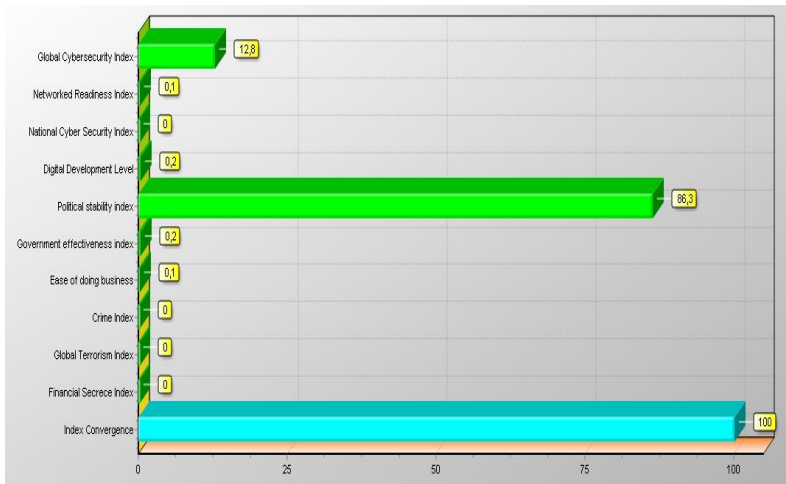


Figure 2.19. Efficiency results for the components of the convergence of the financial monitoring and cybersecurity system for Ukraine (according to the Output-oriented CCR-model)

Analysis of the structural efficiency of input indicators for the countries in cluster 5 (Figure 2.20) showed that these countries provide the current level of convergence of the financial monitoring and cybersecurity systems and exceed it by 4.7%.

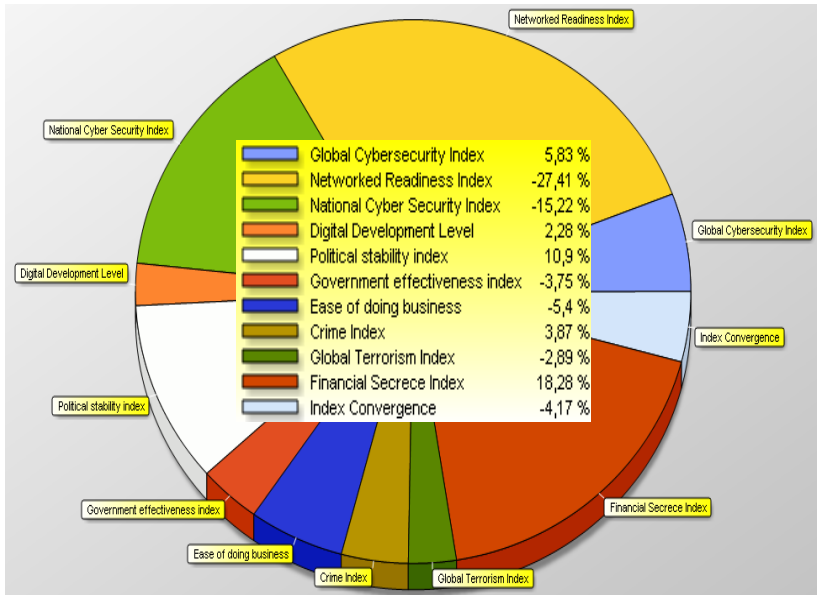


Figure 2.20. Efficiency results for the components of the convergence of the financial monitoring system and cybersecurity system for countries in cluster 5 (according to the Input-oriented CCR-model)

Efficiency is achieved by such indicators as the Networked Readiness Index (-27.41%), the National Cybersecurity Index (-15.22%), the Government Efficiency Index (-3.75%); the Ease of Doing Business (-5.4%); and the Global Terrorism Index (-2.89%). Thus, the countries in this cluster can develop a national cybersecurity system and introduce modern Information Technologies, which is necessary to ensure an appropriate level of system convergence. Some conditions are favorable for doing

business. The level of convergence in the countries in this cluster is lower than the countries in previous clusters. The result obtained indicates that only small positive steps necessary for the convergence of systems.

We analyze the structural efficiency of the initial indicators for the countries in cluster 5 (Figure 2.21).

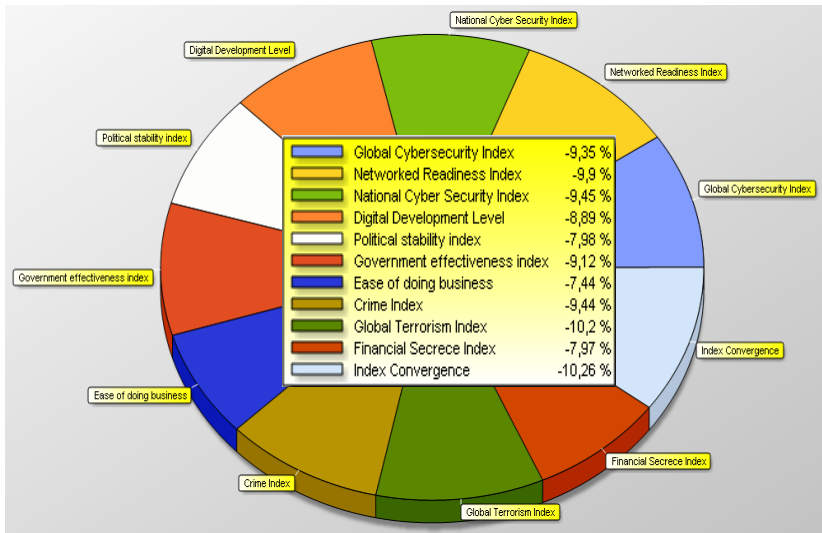


Figure 2.21. Efficiency results for the components of the convergence of the financial monitoring system and cybersecurity system for countries in cluster 5 (according to the Output-oriented CCR-model)

The results of the Output-oriented CCR-model (Fig. 2.21) show that the maximum increase in the convergence index of the financial monitoring system and cybersecurity system is possible by 10.26%. This can be achieved at the expense of reserves for all indicators. Since the current level of convergence is provided and observed to exceed it, the countries in cluster 5 also have the potential for effective integration of the two systems.

Cluster 6 was formed by only four countries with the lowest level of system convergence. Analysis of the structural efficiency of their input indicators (Figure 2.22) showed that these countries provide the current level of convergence of the financial monitoring and cybersecurity systems.

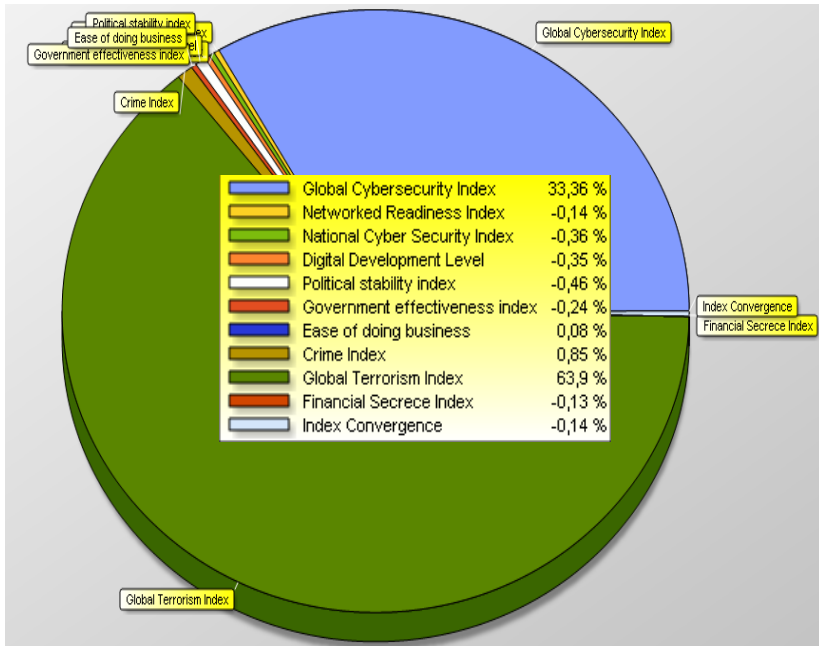


Figure 2.22. Efficiency results for the components of the convergence of the financial monitoring system and cybersecurity system for countries in cluster 6 (according to the Input-oriented CCR-model)

The efficiency is achieved by such indicators as the Networked Readiness Index (-0.14%), the National Cybersecurity Index (-0.36%), the Digital Development Level (-0.35%), the Government Efficiency Index (-0.24%), and the Financial Secrecy Index (-0.13%). In other words, the countries in this cluster can succeed in development, which will be

achieved through systematic integration of financial monitoring and cybersecurity systems. However, the significant problem associated with terrorism and ensuring a global level of cybersecurity signals the need for clear measures at the state level to address these issues or reduce their impact.

We analyze the structural efficiency of the initial indicators for the countries in cluster 6 (Figure 2.23).

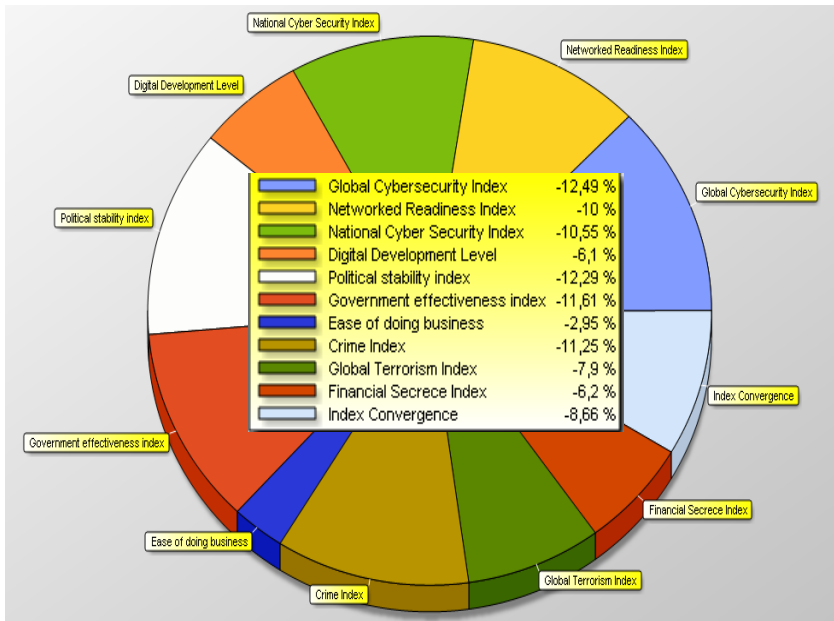


Figure 2.23. Efficiency results for the components of the convergence of the financial monitoring system and cybersecurity system for countries in cluster 6 (according to the Output-oriented CCR-model)

The results of the Output-oriented CCR-model show that the maximum increase in the convergence index of the financial monitoring system and cybersecurity system is possible by 8.66%. This can be achieved at the expense of reserves for all indicators. In other words, there are opportunities for the

countries in this cluster to develop by increasing the efficiency of convergence of systems for countering financial crimes and cyber fraud.

Improving the efficiency of the national security system in terms of convergence of financial monitoring and cybersecurity systems is very relevant, which is associated with the growing level of informatization, digitalization, and computerization of society.

Current trends in the growth of cyber fraud and money laundering require new methods and technologies to combat this phenomenon. This is possible only through the systematic interaction of software, technical, informational, organizational, legal, and technological measures, i.e., the convergence of the system for cybersecurity and countering financial fraud. This process is quite complex, requiring a balanced approach to its implementation. Therefore, the preliminary efficiency of the process of potential convergence of these two systems is necessary to improve the fight against fraud at the global level.

A certain overall level of convergence of the cybersecurity and AML system allowed concluding that this process will positively affect 32% of the countries in the studied set. Thus, we can say that integration processes are favorable for strengthening the capabilities of countries in the fight against financial and cyber fraud. It is planned to assess the potential impact of these processes for certain groups of countries in the future.

The use of Data Envelopment Analysis in this study allowed determining the efficiency of such processes. The CCR model made it possible to analyze the structural efficiency of indicators that characterize the level of development of cybersecurity and AML system. This model also allowed estimating the maximum level of its growth with the available resource potential of the country. The CCR model is more restrictive than the BCC model in determining the efficiency, contributing to a more critical

assessment of the existing reserves of countries needed to ensure integration processes. That is why it was used to analyze all clusters of countries.

2.4. Key algorithms of financial monitoring and cybersecurity systems of financial institutions

According to experts, among the industries that are most affected by cybercriminals, the banking sector ranks first, the energy and mining sector – second, and the telecommunications sector – third. Thus, in 2017, 51.7% of banks suffered the most damage from phishing attacks compared to e-commerce and payment systems representing the financial sector (ElevenPaths, 2017).

Therefore, for banks, one of the more critical and urgent issues is the problem associated with identifying and preventing fraudulent, illegal actions with its financial resources. When bank customers are most often targeted, fraud decreases confidence in financial institutions and the search for alternative ways to keep savings. Improved fraudulent practices and increased frequency of cyber attacks lead to an increase in the losses of banks and their customers. Banking security systems often do not keep pace with the rapid modernization of fraudulent methods and tools. Accordingly, the level of counteraction to threats is inferior to growing threats.

According to the statistics of the Ukrainian Interbank Payment Systems Member Association (2017), the amount of damage to citizens as a result of the actions of fraudsters with payment cards in 2017 reached UAH 670 million, which is significantly higher than the losses in previous years – UAH 339.13 million (2016), UAH 181.00 million (2015), UAH 90.00 million (2014). The average amount of losses from one fraud using social engineering methods has also increased. Thus, in

2017, it amounted to UAH 2,543.00 against UAH 1,403.00 in 2016 and UAH 834.00 in 2015.

The fight against fraud is a global problem. For this purpose, special units are being created, which are trying to regulate at the legislative level. The fight against fraud is influenced by: the development of new methods of fraud; an increase in the volume of information, the processing of which requires new methods, for example, Data Mining; limitation in information systems that do not allow them to be timely adapted to effectively counter threats new in form and level of novelty; problems related to data management at the physical and organizational levels; banking risks; psychology of the relationship “client – fraudster – bank”, which allows the client in cases of communication with a fraudster to provide confidential information.

One of the main areas of the fight against fraud, specified in the Resolution of the National Bank of Ukraine No. 95 On Approval of the Regulation on the Organization of Measures to Ensure Information Security in the Banking System of Ukraine dated September 28, 2017, is the introduction by banks of the main technical systems: detection of attacks; monitoring of incident management events; network access control; e-mail protection; preventing denial of service attacks; anti-virus protection; two-factor authentication (Verkhovna Rada of Ukraine, 2017). There are no explanations regarding their creation, implementation, financing, etc. Thus, the banks have been given a task, and its implementation is already the owners' prerogative, while there is a shortage of cybersecurity specialists, which complicates the task.

The solution to such a complex problem should be approached systematically. The key to its solution should be the development and comprehensive improvement of automated information technologies and systems combined with mathematical methods. Thus, in the field of integration of automated and mathematical methods for the banking sector,

much has been done by the US company SAS Institute operating in business intelligence, which results in software developments for the banking sector (SAS, 2021).

The work done in this area by Kaspersky Lab company should be highlighted. It has been developing software solutions for anti-virus protection and Internet security for many years. It carries out statistical studies of the kinds, methods, types of fraud for various sectors of the economy (Unuchek et al., 2017).

There is a need for convergence of systems considering the growth of the number and varieties of information and cyber threats to ensure an effective information security system of any economic entity. Thus, a possible area is the integration of the system of financial monitoring and cybersecurity, which can be carried out at the algorithmic, software, hardware, information, and organizational levels of the functioning of the information system of a banking institution. Only a systemic combination of cybersecurity and financial monitoring will create a reliable protection system that will identify the consequences and prevent threats. Therefore, it is essential to understand the nature and structure of information security processes, especially those related to verification measures for identifying violations of integrity, data confidentiality, or the consequences of cyber fraud and cyber threats.

We propose developing a three-level system for preventing financial cyber threats, which will be implemented for banking institutions and cover the organizational, information, and algorithmic levels. The activities of each level will be aimed at identifying signs of cyber threats at the stage preceding the implementation of external and internal threats. The conceptual model of this system is shown in Figure 2.24.

The concept of the model is that operations occurring in the bank's front office (directly at the bank, using software and mobile applications) are checked for signs of cyber threats. Therefore, such a system should have a monitoring module built

on the principles of applying the Data Mining methods, where two levels will be implemented – informational (creating a knowledge database with statistics of fraud) and algorithmic (building a database of rules (criteria) for tracing features of fraud) (Figure 2.24).

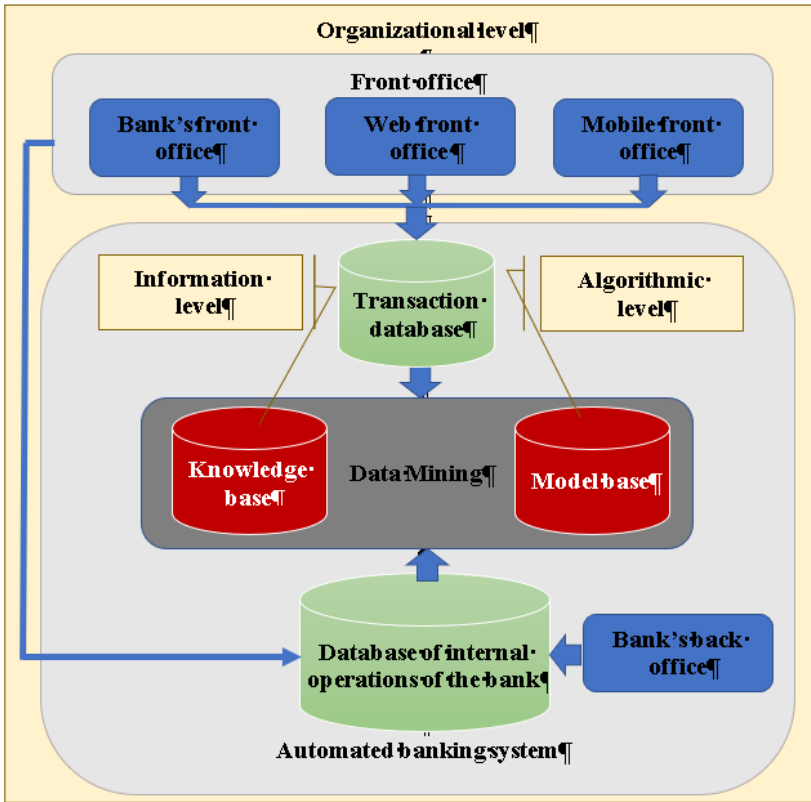


Figure 2.24. Conceptual model of a three-level system for preventing financial cyber threats

Its main purpose is to identify potential financial cyber threats regardless of the nature of the initiator (external – the bank’s client and its operations “Database of transactions”, or internal

– the bank’s personnel and its operations “Database of internal bank operations”). Operations are checked for compliance with certain criteria that determine whether the operation has signs of cyber fraud, which are formed in the knowledge base and rules, taking the accumulated statistical data into account. These verification processes occur based on the organizational level measures at which the business processes of information security are optimized, making it possible to identify weaknesses in the information security system. Based on the outlined tasks of the three levels, we will develop specific proposals for their implementation.

To ensure the organizational level of a three-level system for preventing financial cyber threats, we will apply a methodology for modeling business processes, which allows building a visual model of any process and simulating its implementation in practice. As a result, this approach will help identify weaknesses and optimize with different options in mind.

The methodology provides for the construction and optimization of information security processes of a banking institution, which will be modeled based on the possible integration of the anti-money laundering system (primary financial monitoring) and the information security system (prevention of cyber fraud from external and internal sources).

Thus, at *the first step*, a process model is built based on the BPMN 2.0 notation, a business modeling standard that considers the process-by-process approach. Thus, any activity of the company is considered not in terms of the functions with which it is associated but in terms of the participants and their actions that they carry out over a certain period. This allows seeing who performs, what they do, what they act on, for what period, and what they are guided by. Accordingly, in the process of building the model, it is necessary to define:

–participants in the process or its performers, acting as the company’s resources since the costs associated with the

process will depend on their number. It can be employees of different departments with different positions who make decisions, draw up documents, issue funds, enter data into the system, perform control, etc. They also include suppliers, customers, banking institutions, and others, i.e., external participants in a business process. Separately, we can distinguish automated information systems and their modules, which can also be performers if activities are automated. Several different participants can be involved in a single business process;

- operations, i.e., specific actions of performers that the participant performs as part of the business process. In practice, they relate to a specific object. They are carried out by the person responsible for a specific position and are also carried out following the institution’s instructions. For example, the actions of a bank employee to conclude a loan contract with a client: to find out the purpose of obtaining a loan by the client; verify the presence of a client in the database; enter customer data if it is not in the database; check customer data if it is in the database; correct data; form a contract; agree on the terms with the client; print and sign the contract; transfer it to the client, etc.;
- events that represent actions that occur to initialize a specific process operation. Performers do not directly perform them because they can occur automatically or manifest as a specific signal to start or end an operation. For example, the beginning and end of a business process are the main events of any process; the receipt of a message from the warehouse system about the posting of materials, which triggers the payment to the supplier, is also an event; cancellation of an operation as a result of its erroneous execution by a participant – this is an event that will interrupt the process, etc.;
- control flows that allow generating logic for transitions from one operation to another. This happens if there are alternative

options for participants' actions if a certain condition is applied, formed under the regulatory basis of the economic agent (instructions, standards, laws, regulations, etc.). In practice, management flows are quite challenging to define. This is due to the fact that the simulation process must provide for various options for actions, and due to the frequent condition of their transitions, it is difficult to formalize. Therefore, some companies prefer functional modeling based solely on job descriptions, where the functional responsibilities of personnel are clearly defined and other documents related to the functional structure. However, this approach does not allow selecting actions that can be performed within the same function;

–data, i.e., the entire basis of regulatory documents or information contained in a database or data warehouse, is used to ensure the execution of specific operations, process events, or control flows, or are their direct result. As a rule, they include accounting documents, regulations, instructions, standards, laws, arrays, databases, data warehouses, etc.

Special software is used to implement the model. Its initial construction, which reflects the real process occurring in practice, is called the “AS IS” model.

The model parameters are set at the *second stage*: time to perform operations, cost of resources, and probabilities for control flows. As a rule, this information is taken based on the available data corresponding to this business process. The time is set based on measuring its actual values spent by participants in performing operations. The cost is fixed based on the tariff grid of participants or cost indicators that symbolize the costs incurred for implementing a particular operation. The probability is also set based on statistical data or personal assessment of the participant in the process.

It is advisable to accumulate time and probability statistics for control flows to improve simulation efficiency. This will

$p_i^- (\overline{1, n})$ – probability of a negative (alternative) case for control threads when branching occurs in the model;

n – the number of branches in the model, which are indicated as gateways;

$\lceil \]$ – rounding up the number of operations to the nearest integer.

In the case of simulating the main business processes of the information security system, it is recommended to determine the efficiency factor according to the formula (2.13), reflecting the quality of its work:

$$KR = \frac{NO_{out}}{N_0}, \quad (2.13)$$

where KR – the coefficient of effectiveness of individual modules of the information security system. If $KR = 1$, then it is possible that operations that have received the status of threatening, fraudulent, or subject to financial monitoring have not been detected. Either such cases did not occur, or the system skips all operations because it has inefficient verification settings. If $KR = 0$, then all operations have the status of threatening. In practice, if this situation occurs, we can say that the system is inefficient since it does not skip all operations. The limit values of this indicator indicate the inefficiency of the information security system. If $0 < KR < 1$, some operations were blocked by the system due to the presence of signs of threats in them.

Systems that banks use for financial monitoring can block operations that, upon further verification, do not show signs of money laundering. This can only be explained by the fact that non-transparent verification criteria are used, so the system automatically classifies such transactions as suspicious. Using the index (2.13) will allow accumulating statistics on the system's performance and adjust the verification criteria in case of erroneous selection of operations.

The “Resource analysis” simulation results provide information about the workload of each type of resource involved and their cost. This allows for forming an idea of the financial costs of implementing this process. Suppose several participants (resources) are involved. In that case, it is possible to determine the corresponding costs for each of them separately and compare the cost indicators when choosing alternatives, allowing ways to save money.

At *the fourth stage*, the business process is optimized by making changes and adjustments to the model that will consider the weaknesses identified as a result of the simulation in the previous step. In other words, a “TO BE” model is built that will display the desired process elements. Next, the simulation setup process (second stage) and the simulation itself (third stage) are performed. The results obtained are compared with the “AS IS” model results. This applies to time data and resource costs. The resulting model will be considered suitable for practical use if the indicator values have improved. If the indicators have not changed for the better after optimization, then we perform the optimization again. This will continue until the simulation results are suitable for practical application.

The resulting business process models are implemented in the activities of a bank or other economic agent. In other words, the adjustments made are made to those operations and participants that were optimized in the model.

We use this technique to build models of business processes, which are most critical today for the information security system of banks: the process of customer identification and verification; the process of checking transactions for signs of cyber fraud; automated financial monitoring; checking the actions of insiders for signs of cyber fraud. Bizagi Modeler software was used for simulation. Before analyzing the results obtained, we note the approaches used to build the models.

First, a banking institution is viewed as a complex system, the

components of which are the internal environment: personnel, bank management, its owners, automated banking system (ABS); and the external environment: customers, cybercriminals, connected persons, software, and hardware devices. In other words, a bank is a system of interrelated entities and objects of the internal and external environment. The structure of a system of any nature includes elements of different levels of reliability that can intrude at a particular moment under certain conditions, which can lead to a disruption in its functioning and a violation of the confidentiality, integrity, and value of information. Each of these elements can become a source of threats to information security, potential fraud, or an initiator, or an accomplice, or be indirectly involved.

Secondly, various studies in banking fraud mainly consider the external environment as the initiator of fraud or violation of information security, which is not entirely correct. 80% of the total volume of incidents is related to the bank's personnel. Therefore, intrusion capabilities must also consider the internal aspects of the threat.

Third, when defining the banking system, we will use the principle of professional pessimism, which guides auditors and does not exclude abuse at any bank workplace, the likelihood of unauthorized persons invading to commit fraud or harm. Thus, the source of an incident can be any. It may be implemented anywhere and using any tools and methods. Accordingly, the system should consider negative changes and respond to them.

Fourth, we consider the information security system as a system integrated with the automated banking information system and the system for countering money laundering.

We simulate those processes that are directly involved in the banking security system. Figure 2.25 shows the business model of the customer identification and verification process, which is suitable for remote operations. It is already the result of "TO BE".

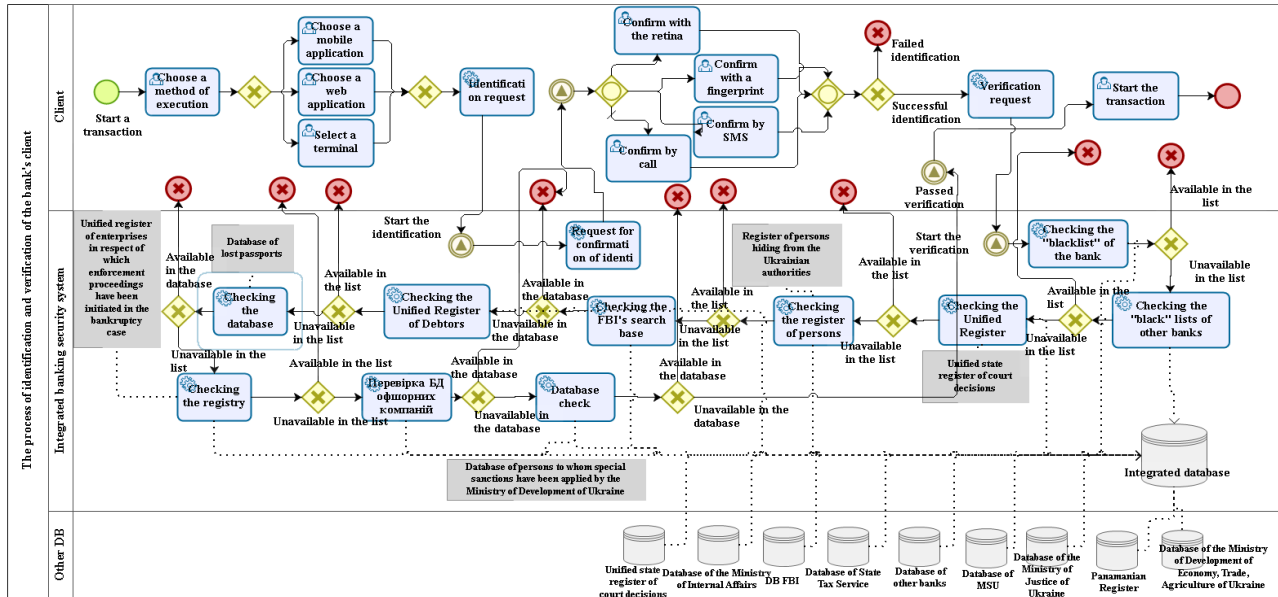


Figure 2.25. The business model of the process identification and verification of the client in the integrated banking security system

Since, in practice, customers are identified, verification is carried out only for individual operations, the construction of the “AS IS” model will be inappropriate since it will not consider many parameters. The comparison will show the inefficiency of the “AS IS” model due to its more complex structure. This problem will also apply to other proposed models. Therefore, analysis and comparison will be carried out for a fully automated process where part of operations is performed by a person, which is typical of many Ukrainian banks.

The model specifies two stages that the client must go through. At the first stage, the client is identified when logging into the system through a mobile application, web banking, or a terminal. This is done by executing a request to confirm the client’s identity by using a fingerprint, retina, or confirmation via SMS or phone call. Currently, only the last two types of confirmation are used in Ukraine. If a fraudster tries to log in using someone else’s data, the identification will not be completed, and the operation will be blocked.

After successful confirmation, the second stage begins – verification, i.e., the client is verified for the presence in (Figure 2.25): the black-list of the bank, where it is a client, and in the black-lists of other banks; the register of court decisions on the client; registers of persons hiding from the Ukrainian authorities; the FBI wanted base; Unified register of debtors; database of lost passports; database of offshore companies; The Unified State Register of Enterprises in respect of which a bankruptcy case has been initiated; based on the data of persons to whom special sanctions have been applied by the Ministry of Economic Development of Ukraine. If the client successfully passes verification, the system permits to perform the operation. Otherwise, the system blocks the client and notifies the relevant security authorities.

The simulation results for this business process are shown in Figure A. 1 in Appendix A. The following was set as the

simulation conditions: the number of operations – 1,000; the probability of rejection of the operation in case of failure to pass the check – 1% for each node (a desirable indicator); execution time of operations in the integrated banking security system – 1 s (this is the maximum time to complete one request in any system) (Hlynnykov, 2021); for identification operations, the time was set based on our measurements of the maximum time in the process of using mobile banking. As a result, it was found that the average time for identification and verification of a client, subject to the implementation of this scheme in practice, will be equal to 69.75 s. The number of operations after verification is 903 (formula 2.12). The performance factor is 0.903 (formula 2.13). In other words, if 1% of operations are identified as fraudulent according to each of the verification criteria, the system will identify 90.3% of operations that have passed monitoring after verification and identification.

After identification and verification, it is proposed to verify operations in accordance with their amounts. If the transaction amount exceeds UAH 400,000, the bank is obliged to monitor it according to the criteria for money laundering (Verkhovna Rada of Ukraine, 2021). Otherwise, it is recommended to check for signs of fraud. This is relevant in the growing number of victims of social engineering. Thus, in Q4 2019, this type of crime combined with malicious software was used in 54%. For individuals, social engineering accounted for 67%, for individuals – 62%. Moreover, for various companies, its share is significant: for state-owned companies – 66%, industrial companies – 88%, financial organizations-94%, IT companies – 50%, trade – 36% (Positive Technologies, 2020).

In practice, institutions are required to carry out monitoring, but the verification process is organized by banks independently. Therefore, most of them do it manually. According to the Resolution of the National Bank of Ukraine No. 65 of May 19, 2020 On Approval of the Regulations on the Implementation of

Financial Monitoring by Banks, banks must organize and automate the relevant processes by June 30, 2021 (Verkhovna Rada of Ukraine, 2020).

Scientists from different countries offer their approaches to the organization of automated monitoring. Thus, Chen et al. (2018) investigated machine learning techniques as a means of combating money laundering. Gao et al. (2009) developed a multi-agent system using intelligent agent technology, which can be integrated into the bank's business processes to identify operations associated with money laundering. The work by Umadevi & Divya (2012) deals with the development of an information model based on the analysis of the flow of transactions, allowing for the clustering of banking operations in terms of the probability of money laundering.

An interesting approach was presented in their work by Caldera et al. (2016), who proposed a payment system with augmented automated functionality for combating money laundering, which was patented by them. Kolhatkar et al. (2014) presented and patented a multi-channel anti-money laundering system for payment cards that monitor operations in real-time. In the work by Dionysios (2010), the modern direction of implementation of modern anti-money laundering systems based on risk identification approaches is considered. The study by Coelho et al. (2019) presents a new area "Suptech", an advanced data collection and analysis tool based on artificial intelligence and machine learning, used against money laundering. Yong (2016) highlights aspects of the technical implementation of AML information systems, especially planning their implementation, design, analysis of the current and future state, some technical and practical solutions.

Despite the significant contribution of foreign scientists to solving the problem of combating money laundering, domestic science lags behind in the creation, development, improvement of information systems and monitoring technologies that are

used to identify criminal proceeds in the process of their laundering. Therefore, the solution to this issue is very relevant for the economy and scientific community of Ukraine. The practical experience of domestic banks offers a business model of the process of primary financial monitoring of the bank, which is carried out in the conditions of automated information processing (Figure 2.26).

The proposed model (Figure 2.26) demonstrates the implementation of automated monitoring for 13 indicators. Suppose the operation does not pass at least one of the verification stages. The system blocks and enters a risk record into the database associated with implementing this transaction. The data is sent to the State Financial Monitoring Service. If the transaction passes all the verification stages, a decision is made on customer service and acceptance of this operation.

The implementation of the automated monitoring system will relieve front office workers from checking potential operations related to money laundering. Its functioning will also improve the efficiency of the bank's staff during financial monitoring. First, it will allow online transaction verification on an ongoing basis. Second, the employee's influence on the verification process and concealment or distortion of its results will no longer be possible. This will happen because the system provides for the use of business rule logic, which will automatically select those operations that do not meet the specified conditions. The system administrator is responsible for configuring them, and other bank employees will not have sufficient rights to influence the verification process purposefully. Third, the proposed system allows checking large volumes of operations for their participation in money laundering. For example, since mandatory monitoring applies to operations above UAH 400,000, operations with lower amounts that may have criminal sources and participate in laundering schemes are ignored.

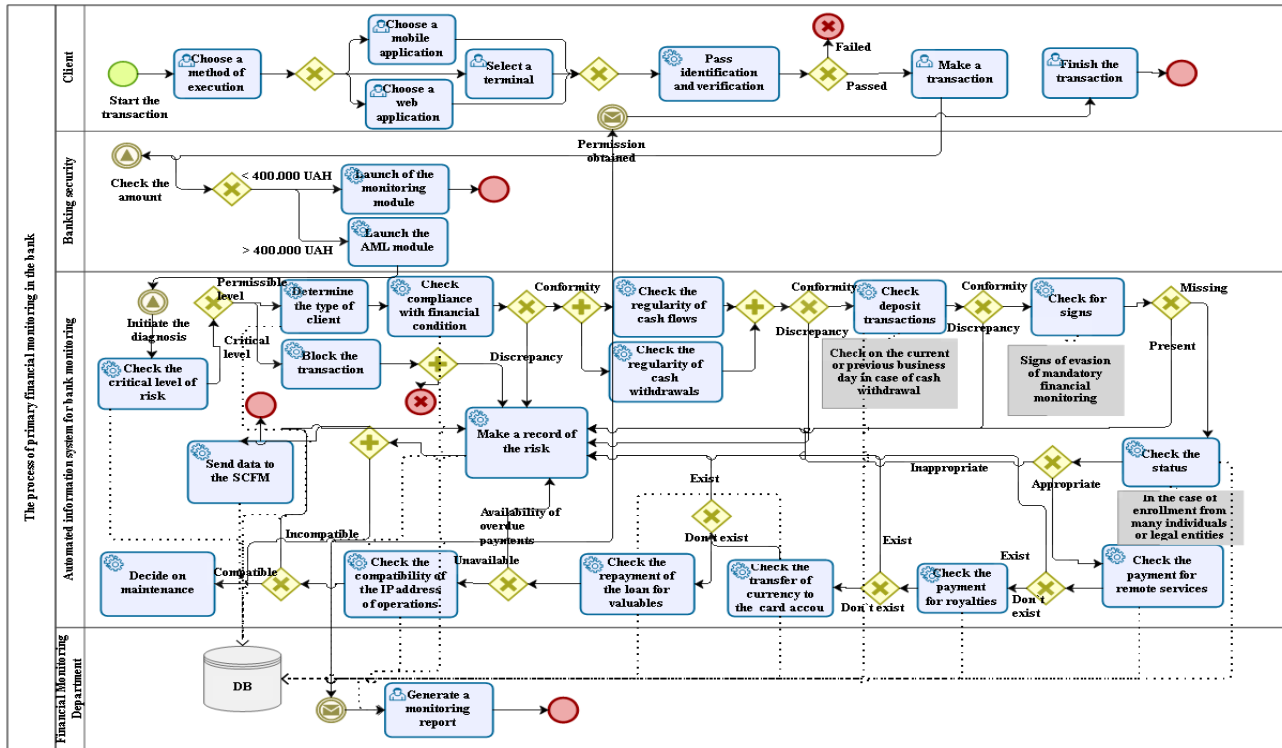


Figure 2.26. The business model of the process of automated financial monitoring of a bank

The use of an automated system will facilitate the verification of the entire volume of transactions, regardless of their amount. Fourthly, the advantage of the proposed solution is the flexibility of debugging the system in the event of changes in legislation, NBU regulations, bank instructions for checking such operations.

Two important statements are taken into account when performing simulations:

1) we take into account that the execution time of operations by an automated system and a specialist is the same, which corresponds to the principle of cost comparability, which must be observed in the case of determining efficiency and comparing costs;

2) we simulate the results based on automated and manual data processing since the proposed business processes already have optimization elements, i.e., the processes implemented in practice are already outdated and are predicted to improve based on compliance with legislation.

The results of the simulation for this process are shown in Figure A. 2 in Appendix A. The simulation conditions were as follows: the number of operations – 1,000; the probability of rejection of the operation in case of failure to pass the verification – 1% for each node (a desirable indicator); execution time for one request in the automated financial monitoring system – 1 s; the time was set only for verification operations, to reveal only the amount that will be spent on monitoring. As a result, it was found that the average time to verify one transaction for signs of financial monitoring is 41.37 seconds, i.e., 11.54 hours will be spent per 1,000 operations. Since the simulation does not consider the servers' capacity, this figure can be overestimated. In practice, such verification by an experienced specialist takes 20 minutes. In other words, a person will need to spend 333.33 hours checking 1,000 operations: $((20 \text{ min.} * 1,000 \text{ trans.}) / 60 \text{ min.})$. In terms of time alone, the effectiveness of the implemented proposed process will be as follows: the automated system will check operations 28.88 times

faster per 1,000 operations.

The number of operations after verification is 878, calculated according to the formula (2.12), the efficiency factor is 0.878 (according to the formula (2.13)). Thus, provided that 1% of operations have signs of money laundering, the system will positively identify 87.8% of operations for each of the verification criteria, which is a high result.

Let's carry out a simulation on resources. For this purpose, we set the monitoring specialist and an automated information system for financial monitoring (AML-module). Let's determine their cost estimates, namely the cost of man-hours and machine-hours. For calculations, we use data reflecting the actual costs of Asian banks incurred for the AML system (AML – Anti-Money Laundering), which, according to the principles of work in this area, are similar to Ukrainian ones. The information is contained in the LexisNexis report and covers the period from September 2015 to January 2016 (LexisNexis, 2021). The calculations are shown in Table 2.1:

Table 2.1 – Calculations of the cost of man-hours and machine-hours

Indicator	Actual value taken from the report (LexisNexis, 2021)	Calculated value
Number of companies surveyed	210	X
Number of banks surveyed	50%	105
AML expenses for all banks, USD	1,500,000,000	X
Average expenses per bank, USD	X	14,285,714.29
Expenses for software and hardware (external and internal), USD	19%	2,714,285.71
Cost of personnel involved in AML, USD	81%	11,571,428.57
Operating time of the AML system per year, subject to 24-hour operation, hour	X	8,760
Cost of a machine-hour, USD	X	309.85
The cost of man-hour, US dollars	X	1,320.94

The calculations in Table 2.1 show the cost of a machine-hour if the entire complex of software and hardware is involved and the cost of a man-hour if the entire staff is involved. Since the value of cost indicators is a commercial secret for banks, it is only possible to use a conditional definition of costs. But even these calculations can give an idea of the effectiveness. Using the obtained values of the cost of a machine-hour and a man-hour, we will carry out a simulation “Resource Analysis”, the result of which is shown in Figure 2.27.

The results shown in Figure 2.27 show that the cost per 1,000 transactions verified by financial monitoring specialists is 4.26 times higher than the cost per 1,000 transactions verified by the AML module. It can be concluded that when implementing the proposed business process of financial monitoring, its effectiveness will be higher for the automated version than for the manual one. For final calculations, it is important to have information about the costs of purchasing and implementing such a system and information about its effectiveness.

Resource	Utilization	Total fixed cost	Total unit cost	Total cost
Financial monitoring specialist	100,00 %	0	14 885,53	14 885,53
AML-system	0,00 %	0	0	0
Total		0	14 885,53	14 885,53

Resource	Utilization	Total fixed cost	Total unit cost	Total cost
Financial monitoring specialist	0,00 %	0	0	0
AML-system	100,00 %	0	3 491,67	3 491,67
Total		0	3 491,67	3 491,67

Figure 2.27. Results of resource simulation for the business process of automated financial monitoring of the bank

Before building a business process model for verifying transactions for signs of fraud, creating an information model for detecting signs of fraud for operations initiated by the external environment is necessary, reflecting the functioning of information flows in an automated environment. The model (Figure 2.28) is constructed in the DFD (data flow diagrams) notation, which is one of the tools for structural modeling and design of information systems, using the All Fusion Process Modeller software (CA, 2021).

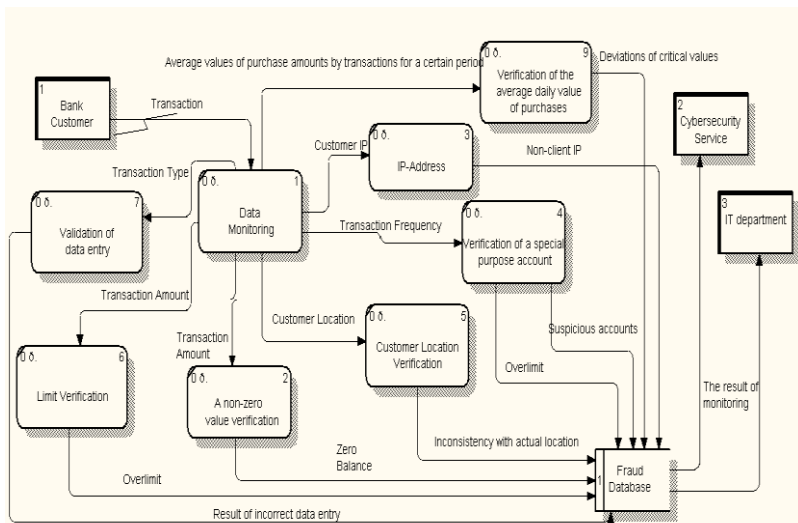


Figure 2.28. Information model for detecting signs of customer fraud

The model shown in Figure 2.28 displays information flows that will be used in the transaction verification (monitoring) module to detect signs of fraud and prevent them. This is done by checking a bank transaction (“Transaction”), which is carried out by the client (the “Bank Customer” entity), using the “Data Monitoring” functions. The following are verified:

–transaction amounts (“Transaction Amount”) for account

zeroing (“a non-zero value verification”). A fraudster often withdraws all funds from the account during a fraudulent operation, which is most likely not typical for the account holder. As a result, the information is obtained that the account has “Zero Balance”;

- “Transaction Amount” for exceeding the established “Limit Verification”. In the process of fraud, operations may exceed the “Overlimit” set by the bank or client, which will signal an attempt to make an illegal operation;
- “Customer Location Verification”, since the operation can be performed from any country or city and may not correspond to the actual geolocation of the client;
- “Verification of a special purpose account”. The account may be on the “Suspicious accounts”, or it may exceed the transaction amount limits (“Overlimit”) if the target account is opened with another bank;
- Client’s “IP address”. If an operation is attempted from an IP address that does not belong to the client (“non-client IP”);
- correctness of the entered data (“Validation of data entry”) depending on the type of transaction (“Transaction type”). The results of incorrect attempts (“Result of incorrect data entry”) may signal a possible hacking of the client’s account;
- exceeding the average daily value of purchases (“Verification of the average daily value of purchases”). At the input, the average daily values of funds spent are analyzed, and if they are critically exceeded, the system can signal the possibility of fraud.

Information about possible violations, scams, and hacks is sent to the fraud database and processed. The “Results of Monitoring” are transmitted to the bank’s “IT Department” and “Cybersecurity Service”.

In accordance with the proposed information model (Figure 2.28), a business model has been developed for the process of verifying transactions for signs of cyber fraud in BPMN 2.0 notation (Figure 2.29).

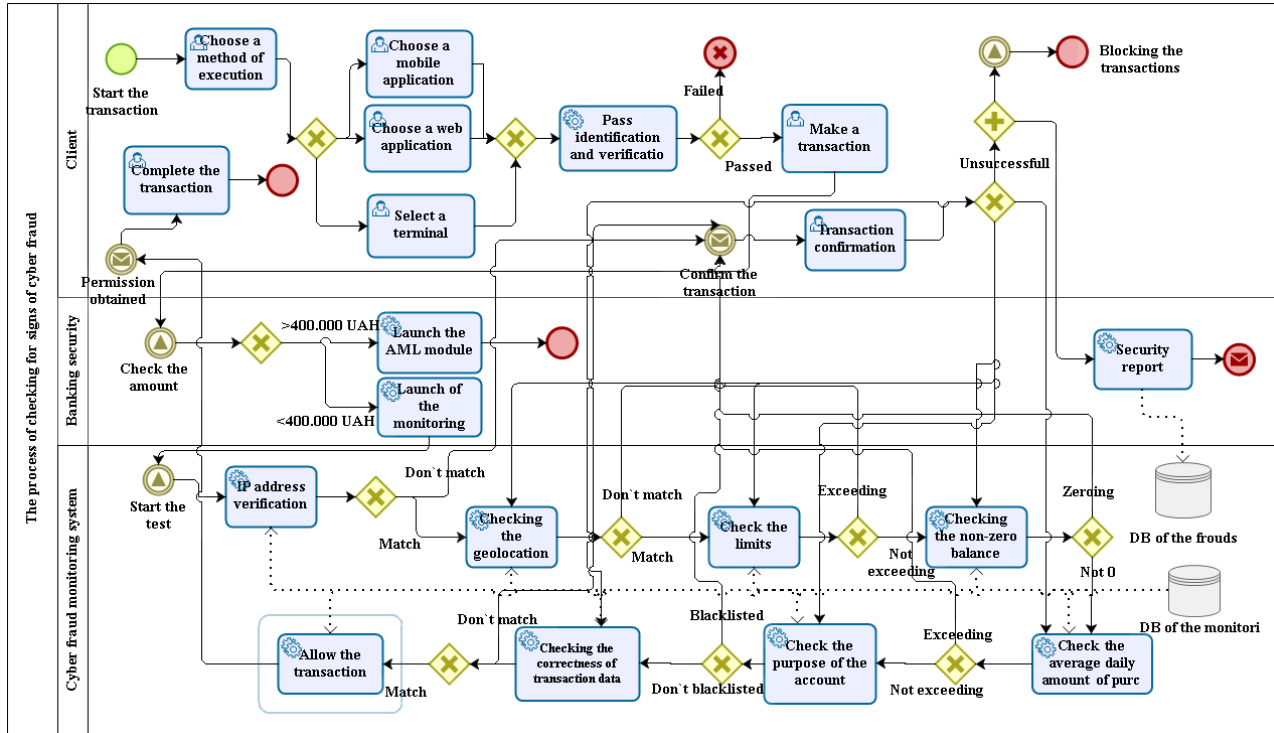


Figure 2.29. The business model of the process for verifying transactions for signs of cyber fraud

The process will be as follows (Figure 2.29): a bank customer or potential fraudster enters the system either using a website, a mobile device, or a terminal; if he or she successfully passed identification and verification, then the system, depending on the amount of the transaction, will check either for signs of money laundering or fraud. The system verifies the operations for signs of fraud using the monitoring module according to the criteria shown in the Figure 0. If the verification result shows no signs of potential fraud, then the system allows the operation and the client completes it; if the verification result shows signs of fraud, the system requests to confirm the operation by SMS or call, or in any other way; the client performs additional authentication; if the operation was initiated by the client, then it will be successfully completed; if the client turns out to be a fraudster, i.e., the client will not be able to pass additional authentication, it will be blocked and informed by the security system.

Time and resource cost simulations were performed for this process (figure A. 3 in Appendix A). Simulation conditions: number of operations – 1,000; probability of operation rejection in case of failure to pass verification – 1% for each node (desired indicator); for a node that corresponds to additional authentication after the system has detected a potential threat, the probability was distributed proportionally; time to complete one request in an automated system – 1 s. It was found that the average time to verify one transaction for signs of cyber fraud is 9.86 seconds, i.e., 2.71 hours will be spent on 1,000 operations.

It turned out that 7 operations did not pass verification and re-identification. Since only 976 operations out of 1,000 were subject to verification for signs of cyber fraud, the performance indicator was 99.28%. This value may indicate high system efficiency. In practice, this result can be achieved by effectively configuring monitoring parameters, which require constant verification by the bank's internal audit department.

Let's simulate the process based on resources (Figure 2.30).

Resource	Utilization	Total fixed cost	Total unit cost	Total cost
Analyst	99,97 %	0	8,1	8,1
Monitoring system	0,00 %	0	0	0
	Total	0	8,1	8,1

Resource	Utilization	Total fixed cost	Total unit cost	Total cost
Analyst	0,00 %	0	0	0
Monitoring system	99,99 %	0	3,27	3,27
	Total	0	3,27	3,27

Figure 2.30. The results of simulation by resources for the business process of verifying transactions for signs of cyber fraud

For this purpose, we determine the cost of man-hours and machine-hours. The Deloitte report notes that in 2020, banks spent 0.6% of all expenses on information security, which accounted for approximately 9.4% of the IT budget, or USD 2,688 per 1 person per year (Bernard & Nicholson, 2021). Based on the fact that in 2020 there were 251 working days, and taking into account the 8-hour working day, we determine that the cost of 1 machine-hour will be equal to USD 1.34: $\text{USD } 2,688 / (251 \text{ days} * 8 \text{ hours})$. To compare this process with manual processing, we determine that the salary of a bank analyst in Ukraine is equal to UAH 17,500 per month (Work.ua, 2020). Based on the fact that in 2020 there were 251 working days, and taking into account the 8-hour working day, we determine that the cost of 1 machine-hour will be equal to USD 1.34: $\text{USD } 2,688 / (251 \text{ days} * 8 \text{ hours})$.

The results of the resource simulation are shown in Figure 2.30, where you can see that if an automated system and an analyst perform almost 100% of transactions, the resource costs

for the first option are 2.48 times less. In other words, it is economically feasible to carry out verification using an automated module (USD 3.27 per 1,000 operations) compared to performing an audit by a specialist (USD 8.1 per 1,000 operations).

As for internal fraud cases, an information model for detecting fraud was also developed if the fraudster is bank staff, i.e., insiders (Figure 2.31).

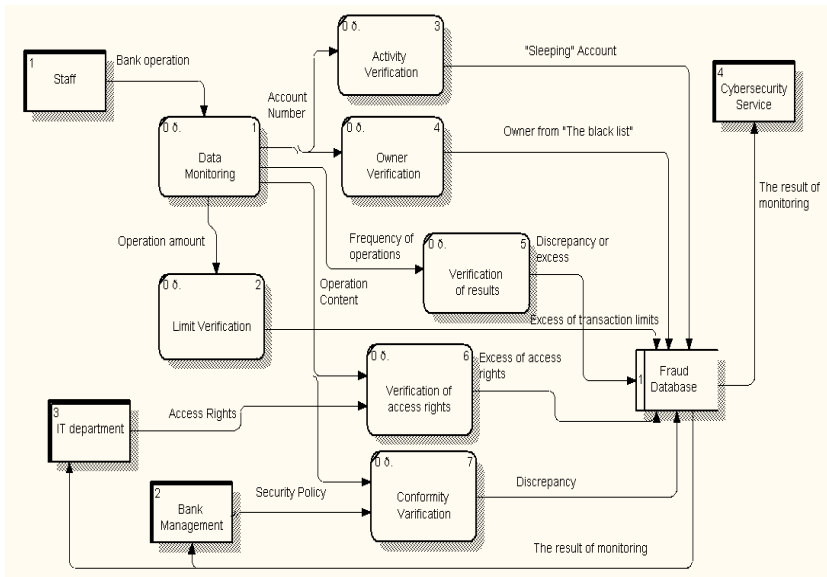


Figure 2.31. Information model for detecting signs of fraud of bank personnel

The model shown in Figure 2.31 reflects the information flows that circulate during the process of verifying by the monitoring module (“Data Monitoring”) of operations (“Bank operation”) carried out by the bank's personnel (“Staff”) for signs of fraud. The following are verified:

- account activity (“Activity Verification”) in the case when the staff uses “Sleeping Account” for own purposes;

- account holders (“Owner Verification”), if the owner is present on the “Black List” or is a foreigner, deceased, etc.;
- limits on operations carried out in accordance with the requirements of the National Bank of Ukraine, the bank’s policy, job descriptions, etc. (“Limit Verification”), resulting in excess of transaction limits);
- the activity of bank employees (“Frequency of operations”) for compliance with banking standards that the employee may exceed or under-comply with (“Discrepancy or excess”);
- operations of employees for compliance with their proper access rights (“Verification of access rights”). This may be the case when employees exceed their rights (“Excess of access rights”) and, for example, perform operations that do not correspond to their functional responsibilities and job descriptions;
- employee operations for compliance with the bank’s security policy (“Conformity Verification”). These may include copying the database, using non-corporate mail, viewing customer accounts, especially VIP clients, etc.

The results are accumulated in a fraud database, processed, and sent to the bank’s “Cybersecurity Service”, “IT Department”, and “Bank Management”.

In accordance with the proposed information model (Figure 2.31), a scheme of the operation process by personnel is developed, taking into account its verification for signs of fraud in the BPMN 2.0 notation (Figure 2.32).

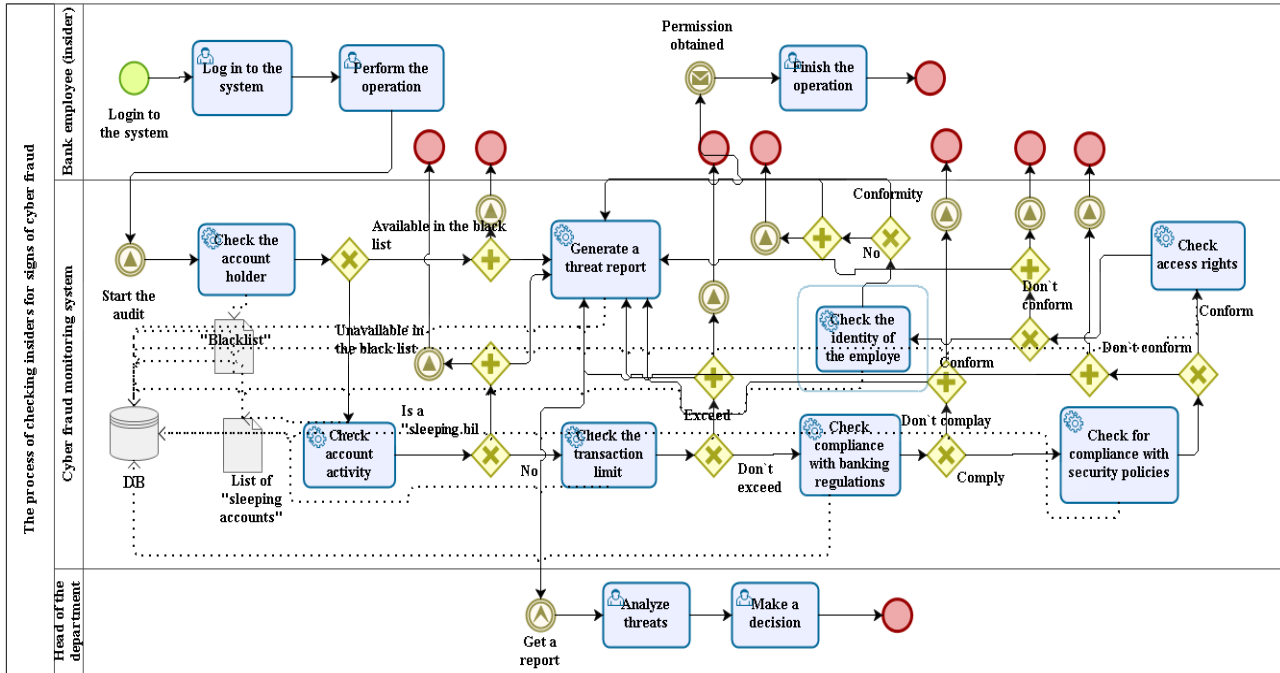


Figure 2.32. The business model of the process for verifying insiders' actions for signs of cyber fraud

The process will be as follows:

- 1) a bank employee who may be a potential fraudster logs in to the banking system and performs a banking operation;
- 2) the cyber fraud monitoring system verifies the operation for cybercrime using the specified verification criteria, namely: access rights, operations for compliance with security policies, employee identity, compliance with bank regulations, sleeping accounts, account activities, and operation limits;
- 3) if the operation meets all the criteria and does not contain signs of fraud on the part of the staff, then the system allows its implementation and the employee can complete it;
- 4) if the system detects signs of fraud, it notifies the head of the relevant department where the operation was performed, who analyzes the information and makes decisions about the potential sign of cybercrime.

Simulations of time and resources were performed for this process (figure A. 4 in Appendix A). According to the following conditions: the number of operations – 1,000; probability of operation rejection in case of failure to pass verification – 1% for each node (desired indicator); time to complete one request in an automated system – 1 s. It was found that the average time to verify 1 transaction for signs of cyber fraud on the part of insiders is 6.86 seconds, i.e., 1.90 hours will be spent on 1,000 operations. 65 operations with signs of fraud were identified, respectively, the system's performance indicator is 93.5%.

The results of the resource simulation (Figure 2.33) show that the efficiency of automated detection of signs of cyber threats is 2.79 times less expensive.

Resource	Utilization	Total fixed cost	Total unit cost	Total cost
Analyst	100,00 %	0	7,12	7,12
Monitoring system	0,00 %	0	0	0
	Total	0	7,12	7,12

Resource	Utilization	Total fixed cost	Total unit cost	Total cost
Analyst	0,00 %	0	0	0
Monitoring system	100,00 %	0	2,55	2,55
	Total	0	2,55	2,55

Figure 2.33. Results of resource simulations for the business process of verifying insiders' actions for signs of cyber fraud

The proposed methodology for optimizing business processes represents the organizational level of key algorithms for integrating financial monitoring and cybersecurity systems. Its implementation will make it possible to form prerequisites for detecting transactions that may result in fraud committed by an external criminal or insider and money laundering. Implementing the developed models in practice will cover a wide range of operations, regardless of their belonging to the external or internal environment. The proposed algorithms will identify weaknesses in information security and serve as a prerequisite for the convergence of cybersecurity and financial monitoring systems within a single integrated banking automated system. This will facilitate the implementation of system monitoring to verify bank transactions for signs of cyber and financial crimes. In the end, implementing the proposed approach to optimizing business processes will increase the efficiency and management systems due to the timely adoption of a timely decision.

CONCLUSIONS

Dynamic digitalization of the economy makes banking and non-banking financial institutions more vulnerable to cybercrime. Financial institutions accumulate a significant amount of information from their customer. In case of the information security breach, confidential data may be used for illegal activities or sold on dark web sites, which may lead to the loss of business reputation of both financial institutions and their customers.

Cybercrimes in the financial sector of the economy have reached an unprecedented scale, which is caused by the action of the following potential factors: an increase in the proportion of banking processes that are transferred to the management of third parties, including abroad; the use of cloud technologies for storing and transferring data; increased use of robotics or algorithms for automated trading and application development; increased use of virtual and digital currencies.

The safe and efficient functioning of the financial market infrastructure is essential for maintaining and promoting financial stability, increasing public confidence in financial institutions. The study showed that the level of cyber vulnerability of EU citizens is on average 11%, which makes it possible to assert that the population of European countries is aware of threats in the virtual space, ways of protecting against cybercrime. However, the level of cyber vulnerability of consumers of financial services in the context of the EU countries is not uniform. Namely, citizens of countries such as Denmark, the Netherlands, and Sweden have the lowest risk of becoming victims of cyber fraud. Countries with high values of the calculated level of cyber vulnerability of consumers of financial services (18%) include Spain, Italy, Romania.

Financial market participants need confidence in data security, the ability to minimize cyber risks and defend against cyber threats. Increasing financial damage from cyberattacks, combined

with the growing volume of information data stored in the network infrastructure necessitate the development of new tools to ensure information security. To combat cybercrime, a combination of traditional and non-traditional strategies and tactics using digital information technology. To make managerial decisions in the field of cybersecurity, the development of tools is gaining ground, which involves the accumulation of large amounts of information and the use of modern approaches in the field of artificial intelligence.

For Ukraine and the world as a whole the issues of anti-money laundering, countering terrorist financing, proliferation of weapons of mass destruction will be acute for a long time. At the same time, the problem of cybersecurity is no less relevant, when there is a need to ensure the confidentiality, security, integrity, accessibility and authenticity of information resources. Research of these two directions involves generalization, structuring of theoretical achievements of world and domestic literature in terms of defining the basic concepts, goals, objectives, directions and models of research issues, as well as developing the authors' own conclusions on these aspects. The main emphasis of the study is that both sets of measures, both financial monitoring and cybersecurity, are becoming one of the main tasks of the world community, leadership, government agencies, and society. Overall, the proposed convergence of financial monitoring and cybersecurity systems can be taken as a basis, adapted and adapted to address a wide range of issues such as economic and financial security, the fight against money laundering and other financial market issues.

REFERENCES

1. Payments Industry Intelligence (2019). Removing roadblocks. The new road of fintech. FinTech disruptors 2019. URL: <https://www.paymentscardsandmobile.com/research/fintech-disruptors-2019-report/>
2. Albeshr S., Nobanee H. (2020). Blockchain Applications in Banking Industry: A Mini-Review. SSRN Electronic Journal. URL: <http://dx.doi.org/10.2139/ssrn.3539152>.
3. Risman A., Mulyana B., Silvatika B. A., Sulaeman A. S. (2021). The effect of digital finance on financial stability. *Management Science Letters*. 2021. P. 1979–1984. URL: <https://doi.org/10.5267/j.msl.2021.3.012>
4. Frame, W. Scott and White, Lawrence J. and White, Lawrence J. (2014) Technological Change, Financial Innovation, and Diffusion in Banking (January 2014). NYU Working Paper No. 2451/33549, Available at SSRN: <https://ssrn.com/abstract=2380060>
5. Lyeonov S., Bilan Yu., Rubanov P., Grenčíková A. (2019). Countries Financial Development and Digital Readiness as Determinants of Financial Sector Innovativeness. Proceedings of the 34rd International Business Information Management Association Conference, IBIMA 2019: Vision 2025: Education Excellence and Management of Innovations through Sustainable Economic Competitive Advantage, 13–14 November 2019. Madrid, 2019. P. 13604–13619
6. Wirdiyanti R. (2018). Digital Banking Technology Adoption and Bank Efficiency: The Indonesian Case. *Ojk*, (December). P. 1–34.
7. Carbó-Valverde S., Cuadros-Solas P. J., Rodríguez-Fernández F. (2020). The Effect of Banks' IT Investments on the Digitalization of their Customers. *Global Policy*. 11(S1). P. 9–17. URL: <https://doi.org/10.1111/1758-5899.12749>
8. Bazarbash M. (2019). FinTech in Financial Inclusion: Machine Learning Applications in Assessing Credit Risk. IMF

Working Papers. 19(109). URL:
<https://doi.org/10.5089/9781498314428.001>

9. Huang Y., Zhang L., Li Z., Qiu H., Sun T., Wang X. (2020). Fintech Credit Risk Assessment for SMEs. IMF Working Papers. 220(193). URL: <https://doi.org/10.5089/9781513557618.001>

10. Martínez-Sánchez J.F., Cruz-García S., Venegas-Martínez F. (2020). Money laundering control in Mexico: A risk management approach through regression trees (data mining). Journal of Money Laundering Control. 2020. 23(2), P. 427-439, URL: <https://www.emerald.com/insight/content/doi/10.1108/JMLC%2D10%2D2019%2D0083/full/html>

11. PWC 2017 – Risk in review study. (2017). URL: <https://www.oxfordeconomics.com/my-oxford/projects/364357>

12. Marsh&McLennan companies (2019) Artificial intelligence applications in financial services.. URL: <https://www.oliverwyman.com/content/dam/oliverwyman/v2/publications/2019/dec/ai-app-in-fs.pdf>

13. European Commission (2020). Europa-2020. A European strategy for smart, sustainable and inclusive growth. URL: <http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%2020%20007%20-%20Europe%202020%20-%20EN%20version.pdf>

14. Association of Certified Fraud Examiners (2019). Study: AI for fraud detection to triple by 2021. URL: <https://www.acfe.com/press-release.aspx?id=4295006598>

15. Rubanov P.M. (2019). Market structure of FinTech innovations. Scientific Bulletin of Polissya. № 2 (18). P. 184-189.

16. Semenog A.Yu., Tsyruk S.C. (2018). The Tendencies in the Development of Fintech Services in Both the Global and

the National Financial Services Markets. *Economics*. № 10. P. 327-334.

17. World Bank Group and the University of Cambridge (2020). The Global Covid-19 FinTech Regulatory Rapid Assessment Report. URL: <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-report-fintech-regulatory-rapid-assessment.pdf>

18. KPMG (2020). Pulse of Fintech H2.2020. URL: <https://assets.kpmg/content/dam/kpmg/xx/pdf/2021/02/pulse-of-fintech-h2-2020.pdf>

19. Andreou, P. C., & Anyfantaki, S. (2021). Financial literacy and its influence on internet banking behavior. *European Management Journal*, 39(5). <https://doi.org/10.1016/j.emj.2020.12.001>

20. Nuha, M., Mahmud, S., & Sattar, A. (2021). A Case Study and Fraud Rate Prediction in e-Banking Systems Using Machine Learning and Data Mining. *Advances in Intelligent Systems and Computing*, 1248. https://doi.org/10.1007/978-981-15-7394-1_6

21. IBM (2021). X-Force Threat Intelligence Index 2021. IBM Security. Available at: <https://www.ibm.com/downloads/cas/M1X3B7QG>

22. F-Secure (2019) Cyber Threat Landscape for the Finance Sector. Available at: <https://www.f-secure.com/content/dam/f-secure/en/business/common/collaterals/f-secure-cyber-threat-landscape-finance-sector.pdf>

23. Federal Bureau of Investigation (2020). Internet Crime Report. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

24. Nish A., Naumann S., Muir J. (2020). Enduring Cyber Threats and Emerging Challenges to the Financial Sector. Carnegie Endowment for International Peace. Available at:

<https://carnegieendowment.org/2020/11/18/enduring-cyber-threats-and-emerging-challenges-to-financial-sector-pub-83239>

25. Insights (2018). The Top Threat Actors Targeting Financial Services Organizations.. Available at: <https://insights.com/blog/the-top-threat-actors-targeting-financial-services-organizations>

26. OECD Policy Responses to Coronavirus (COVID-19) (2020) Dealing with digital security risk during the Coronavirus (COVID-19) crisis. Version 3 April 2020. Available at <https://www.oecd.org/coronavirus/policy-responses/dealing-with-digital-security-risk-during-the-coronavirus-covid-19-crisis-c9d3fe8e/>

27. Securitymagazine (2019). Business Losses to Cybercrime Data Breaches to Exceed \$5 Trillion by 2024. Available at <https://www.securitymagazine.com/articles/90806-business-losses-to-cybercrime-data-breaches-to-exceed-5-trillion-by-2024>

28. European Commission. Strategic plan 2020-2024 – Informatics. Avai

lable at https://ec.europa.eu/info/publications/strategic-plans-2020-2024-informatics_en

30. Deloitte (2018). Centre for regulatory strategy EMEA : Cyber risk and regulation in Europe A new paradigm for banks. Available at https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu_deloitte-cyber-risk-regulation-europe.pdf

31. OECD Policy Responses to Coronavirus (COVID-19) (2020). Dealing with digital security risk during the Coronavirus (COVID-19) crisis. Version 3 April 2020. Available at <https://www.oecd.org/coronavirus/policy-responses/dealing-with-digital-security-risk-during-the-coronavirus-covid-19-crisis-c9d3fe8e/>

32. Savchuk, T. O., Pryimak, N. V., Slyusarenko, N. V., Smolarz, A., Smailova, S., & Amirgaliyev, Y. (2020). Improved

method of searching the associative rules while developing the software. *International Journal of Electronics and Telecommunications*, 66(3), 425-430. doi:10.24425-ijet.2020.131895/715.

33. Horban, H., Kandyba, I., Dvoretzkyi, M., & Boiko, A. (2021). Principles of searching for a variety of types of associative rules in OLAP-cubes. *CEUR Workshop Proceedings*, 2845, 181-192.

34. GSM Association (2020). The Mobile Economy 2020. Available at: https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf

35. Global Social Network Users 2020. Available at: <https://www.emarketer.com/content/global-social-network-users-2020>.

36. Comparitech (2020) Which countries have the worst (and best) cybersecurity? Comparitech. Available at: <https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/>

37. European Commission (2020a). Europeans' attitudes towards cyber security. Special Eurobarometer 499.. Available at: <https://europa.eu/eurobarometer/surveys/detail/2249>

38. European Commission (2020b). Shaping Europe's digital future Digital Economy and Society Index. URL: <https://digital-agenda-data.eu/datasets/desi/visualizations>

39. National Bank of Ukraine (2021). On the approval of the Regulation on monitoring the compliance by banks with the requirements of the legislation on information security, cyber protection, and electronic trust services Resolution of the NBU No. 4 dated January 16, 2021. URL: https://bank.gov.ua/admin_uploads/law/16012021_4.pdf

40. Bank for International Settlement (2016). Guidance on cyber resilience for financial market infrastructures, CPMI-IOSCO, 2016. URL: <https://www.bis.org/cpmi/publ/d146.pdf>

41. European Central Bank (2018). Cyber resilience oversight expectations for financial market infrastructures, ECB, 2018). URL: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

42. Bank for International Settlement (2018). Cyber-resilience: Range of practices. Basel Committee on Banking Supervision. URL: <https://www.bis.org/bcb/publ/d454.pdf>

43. European Commission (2020). Europeans' attitudes towards cyber security (cybercrime). URL: <https://europa.eu/eurobarometer/surveys/detail/2249>

44. Achim, M. V., Borlea, S. N., & Văidean, V. L. (2021). Does technology matter for combating economic and financial crime? A panel data study. *Technological and Economic Development of Economy*, 27(1), 223-261. doi:10.3846/tede.2021.13977.

45. Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review*, 40 doi:10.1016/j.cosrev.2021.100402.

46. Bendre, M., Das, M., Wang, F., & Yang, H. (2021). GPR: Global personalized restaurant recommender system leveraging billions of financial transactions. Paper presented at the *WSDM 2021 - Proceedings of the 14th ACM International Conference on Web Search and Data Mining*, 914-917. doi:10.1145/3437963.3441709 Retrieved from www.scopus.com

47. De Campos Souza, P. V., & Torres, L. C. B. (2021). Extreme wavelet fast learning machine for evaluation of the default profile on financial transactions. *Computational Economics*, 57(4), 1263-1285. doi:10.1007/s10614-020-10018-0.

48. El-Bannany, M., Dehghan, A. H., & Khedr, A. M. (2021). Prediction of financial statement fraud using machine learning techniques in UAE. Paper presented at the *18th IEEE International Multi-Conference on Systems, Signals and Devices, SSD* 2021, 649-654. doi:10.1109/SSD52085.2021.9429297 Retrieved from www.scopus.com.
49. Feng, N., Zhao, H., & Singh, P. K. (2022). Modeling in mechanical engineering cad technology. *Computer-Aided Design and Applications*, 19(S2), 1-14. doi:10.14733/cadaps.2022.S2.1-14.
50. Gabudeanu, L., Brici, I., Mare, C., Mihai, I. C., & Scheau, M. C. (2021). Privacy intrusiveness in financial-banking fraud detection. *Risks*, 9(6) doi:10.3390/risks9060104.
51. Houben, R., & Snyers, A. (2021). Cryptoassets and financial crime: A european union perspective. *The routledge handbook of FinTech* (pp. 163-189) Retrieved from www.scopus.com.
52. Huang, S., Zuo, W., Vrabie, D., & Xu, R. (2021). Modelica-based system modeling for studying control-related faults in chiller plants and boiler plants serving large office buildings. *Journal of Building Engineering*, 44 doi:10.1016/j.jobe.2021.102654.
53. Keshavarzian, M., & Tabatabaienasab, Z. (2021). Application of bootstrap panel granger causality test in determining the relationship between renewable and non-renewable energy consumption and economic growth: A case study of OPEC countries. *Technology and Economics of Smart Grids and Sustainable Energy*, 6(1) doi:10.1007/s40866-021-00106-x.
54. Leonov, S., Yarovenko, H., Boiko, A., & Dotsenko, T. (2019). Information system for monitoring banking transactions related to money laundering. Paper presented at the *CEUR*

Workshop Proceedings, , 2422 297-307. Retrieved from www.scopus.com.

55. Moreno-Fernández, M. M., Blanco, F., & Matute, H. (2021). The tendency to stop collecting information is linked to illusions of causality. *Scientific Reports*, *11*(1) doi:10.1038/s41598-021-82075-w.

56. Núñez-Ochoa, M. A., Chiprés-Tinajero, G. A., González-Domínguez, N. P., & Medina-Ceja, L. (2021). Causal relationship of CA3 back-projection to the dentate gyrus and its role in CA1 fast ripple generation. *BMC Neuroscience*, *22*(1) doi:10.1186/s12868-021-00641-4.

57. Pyrik, J. (2021). The financial transactions and reports analysis centre of canada (FINTRAC). *Top secret canada: Understanding the canadian intelligence and national security community* (pp. 106-123) Retrieved from www.scopus.com.

58. Vasilyeva, T., Kuzmenko, O., Kuryłowicz, M., & Letunovska, N. (2021). Neural network modeling of the economic and social development trajectory transformation due to quarantine restrictions during covid-19. *Economics and Sociology*, *14*(2), 313-330. doi:10.14254/2071-789X.2021/14-2/17.

59. Venkatraman, S., & Reddy, P. G. (2021). Cashlessness and scalable multi-pay practices: Capturing the everyday financial transactions in local contexts. *Telecommunications Policy*, *45*(5) doi:10.1016/j.telpol.2021.102113.

60. Wang, Z. (2021). Abnormal financial transaction detection via AI technology. *International Journal of Distributed Systems and Technologies*, *12*(2), 24-34. doi:10.4018/IJDST.2021040103.

61. Wei, Y., Yazdi, M. D., Di, Q., Requia, W. J., Dominici, F., Zanobetti, A., & Schwartz, J. (2021). Emulating causal dose-response relations between air pollutants and mortality in the medicare population. *Environmental Health: A Global Access Science Source*, *20*(1) doi:10.1186/s12940-021-00742-x.

62. Wu, H., Yu, Q., Ma, L., Zhang, L., Chen, Y., Guo, P., & Xu, P. (2021). Health economics modeling of antiretroviral interventions amongst HIV serodiscordant couples. *Scientific Reports*, 11(1) doi:10.1038/s41598-021-93443-x.
63. Wu, T., Gao, X., An, S., & Liu, S. (2021). Time-varying pattern causality inference in global stock markets. *International Review of Financial Analysis*, 77 doi:10.1016/j.irfa.2021.101806.
64. Babenko K.E. (2019). Osoblyvosti pobudovy prychnynno-naslidkovoii modeli ekonomichnoho rozvytku rehioniv [Features of building a causal model of economic development of regions]. *Problems of System Approach in Economics*. No. 6(74). P.77-82.
65. Voronov V. T. Sudovo-medychna otsinka prychnynno-naslidkovykh zviazkiv mizh utvorenniam travmy ta nespriyatlyvymy naslidkamy [Forensic assessment of causal relationships between trauma and adverse effects]: Dissertation for a degree of Doctor of Medical Sciences: 14.01.25 – Sudova medytsyna / V. T. Voronov ; Kharkiv National Medical University. Vinnytsia, 2018. 359 p.
66. Chynyska I. I. Determinanty metodolohichnoho zabezpechennia stratehichnykh napriamiv rozvytku finansovoho rynku u konteksti aktualnykh potreb suchasnosti [Determinants of methodological support of strategic directions of financial market development in the context of current needs]. *Investments: Practice and Experience*. 2018. No. 6. Pp. 18–21.
67. Banker, R.D., Charnes, A., & Cooper, W.W. (1984). Some Models for Estimating Technical and Scale Inefficiencies in Data Envelopment Analysis. *Management Science*, 30(9), 1031-1142. doi: 10.1287/mnsc.30.9.1078.
68. Banxia Software (2021). *Frontier Analyst*. Retrieved September 30, 2021 from <https://banxia.com/frontier/resources/demodownload/>.

69. Bernard, J., & Nicholson, M. (2021). *Reshaping the cybersecurity landscape. How digitization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions*. Retrieved September 30, 2021 from <https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html>.

70. CA (2021). *AllFusion® Process Modeler Data Flow Diagramming. Design Guide r7.2*. Retrieved September 30, 2021 from <https://supportcontent.ca.com/cadocs/0/e002761e.pdf>.

71. Caldera, J., Hain, J., & Sherlock, K. (2016). Enhanced automated anti-fraud and anti-money-laundering payment system: patent US20160071108A1. United States. Filed 04.09.2015, pub. date 10.03.2016. Retrieved September 30, 2021 from <https://patentimages.storage.googleapis.com/a7/34/0c/64cca0829ed4ea/US20160071108A1.pdf>.

72. Charnes, A., Cooper, W.W., & Rhodes, E. (1978). Measuring the efficiency of decision making units. *European Journal of Operational Research*, 2, 429-444.

73. Chen, Z., Van Khoa, L.D., Teoh, E.N., Nazir, A., Karuppiyah, E.K., & Lam, K.S. (2018). Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. *Knowledge and Information Systems*, 57(2), 245–285. doi: 10.1007/s10115-017-1144-z.

74. Coelho, R., De Simoni, M., & Prenio, J. (2019). Suptech applications for anti-money laundering. *FSI Insights on policy implementation*, 18, 1-18. Retrieved September 30, 2021 from <https://www.bis.org/fsi/publ/insights18.pdf>.

75. Dionysios, S. Demetis (2010). *Technology and Anti-Money Laundering: A Systems Theory and Risk-Based Approach*. Edward Elgar Publishing, Incorporated.

76. Dong, F., Li, Y., Qin, C., & Sun, J. (2021). How industrial convergence affects regional green development efficiency: A spatial conditional process analysis. *Journal of Environmental Management*, 300. doi: 10.1016/j.jenvman.2021.113738.

77. ElevenPaths (2017). *Trend Report «Financial Cyber Threats Q1 2017»*. Retrieved September 30, 2021 from https://www.elevenpaths.com/wp-content/uploads/2017/04/Financial_Threats_Q1-2017_EN.pdf.

78. Gao, S., Xu, D., Wang, H., & Green, P. (2009). Knowledge-based anti-money laundering: a software agent bank application. *Journal of Knowledge Management*, 13(2), 63-75. doi: 10.1108/13673270910942709.

79. Gimenez-Aguilar, M., de Fuentes, J. M., Gonzalez-Manzano, L., & Arroyo, D. (2021). Achieving cybersecurity in blockchain-based systems: A survey. *Future Generation Computer Systems*, 124, 91-118. doi: 10.1016/j.future.2021.05.007.

80. Guilbeault, D., Baronchelli, A., & Centola, D. (2021). Experimental evidence for scale-induced category convergence across populations. *Nature Communications*, 12(1). doi: 10.1038/s41467-020-20037-y.

81. Halafyan, A.A. (2007) *STATISTICA 6. Statisticheskii analiz dannyih* / [*STATISTICA 6. Statistical data analysis*]. Moscow : LLC «Binom-Press» [in Russian].

82. Han, C.H., & Han, C. (2021). Semi-quantitative cybersecurity risk assessment by blockade and defense level analysis. *Process Safety and Environmental Protection*, 155, 306-316. doi: 10.1016/j.psep.2021.09.028.

83. Hlynykov, N. (2021). *Optymyzatsyia nahruzky sozdavaemoi saitom na vyrtualnom khostynhe* / [*Optimization of the load created by the site on shared hosting*]. Retrieved September 30, 2021 from <https://my.activecloud.com/ru/index.php?/Knowledgebase/Arti>

cle/View/317/36/optimizcija-ngruzki-sozdvmojj-sjtom-n-virtulnom-khostinge [in Russian].

84. Hrabchuk, O., & Suprunova, I. (2020). Finansovy monitorynh yak umova zabezpechennia derzhavnoi bezpeky krainy: poniattia, skladovi, etapy rozvytku | [Financial monitoring as a condition for ensuring the countries national security: concepts, components, stages of development]. *Aspects of public administration*, 8(4), 75–83. doi: 10.15421/152082.

85. Ibrahim, A. E. A., Elamer, A. A., & Ezat, A. N. (2021). The convergence of big data and accounting: Innovative research opportunities. *Technological Forecasting and Social Change*, 173. doi: 10.1016/j.techfore.2021.121171.

86. Kolhatkar, J., Fatnani, S., Yao, Yi., & Matsumoto, K. (2014) Multi-channel data driven, real-time anti-money laundering system for electronic payment cards: patent US8751399B2. United States. Filed 15.07.2012, pub. date 10.06.2014. Retrieved September 30, 2021 from <https://patentimages.storage.googleapis.com/20/52/22/4f12c57929b368/US8751399.pdf>.

87. Kuzmenko, O.V., Yarovenko, H.M., & Radko, V.V. (2021). Poperednii analiz protsesu konverhentsii system kiberbezpeky ta finansovoho monitorynhu krain | [Preliminary analysis of the convergence process of cyber security systems and financial monitoring of countries]. *Economy and society*, 32. doi: 10.32782/2524-0072/2021-32-37 [in Ukrainian].

88. LexisNexis (2021). *Uncover the True Cost of Anti-Money Laundering & KYC Compliance*. Retrieved September 30, 2021 from <https://www.lexisnexis.com/risk/intl/en/resources/research/true-cost-of-aml-compliance-apac-survey-report.pdf>.

89. Madeira, P. M., Vale, M., & Mora-Aliseda, J. (2021). Smart specialisation strategies and regional convergence: Spanish extremadura after a period of divergence. *Economies*, 9(4). doi: 10.3390/economies9040138.

90. Mokhor, V., Honchar, S., & Onyskova, A. (2021). Cybersecurity risk assessment of information systems of critical infrastructure objects. Paper presented at the *2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 - Proceedings*, 19-22. doi: 10.1109/PICST51311.2020.9467957.

91. Morse, J.C. (2019). Blacklists, market enforcement, and the global regime to combat terrorist financing. *International Organization*, 73(3), 511-545.

92. Pershyn, V.G. (2019). Rol finansovoho monitorynhu v mezhakh protydiv lehalizatsii dokhodiv, oderzhanykh zlochynnym shliakhom | [The role of financial monitoring in counteracting the legalization of proceeds from crime]. *Bulletin of Luhansk State University of Internal Affairs named after E.O. Didorenko*, 4(88), 250-257. doi: 10.33766/2524-0323.88.250-257 [in Ukrainian].

93. Positive Technologies (2020). *Aktualnye kyberuhrozby: IV kvartal 2019 hoda* | [Topical Cyber Threats: Q4 2019]. Retrieved September 30, 2021 from <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q4/#id7> [in Russian].

94. Radygin, V.Y., Kupriyanov, D.Y., Bessonov, R.A., Ivanov, M.N., & Oслиakova, I.V. (2021). Application of text mining technologies in Russian language for solving the problems of primary financial monitoring. Paper presented at the *Procedia Computer Science*, 190, 678-683. doi: 10.1016/j.procs.2021.06.078.

95. Repetto, M., Striccoli, D., Piro, G., Carrega, A., Boggia, G., & Bolla, R. (2021). An autonomous cybersecurity framework for next-generation digital service chains. *Journal of Network and Systems Management*, 29(4). doi: 10.1007/s10922-021-09607-7.

96. Rysin, V.V., & Stepanova, A.V. (2020) Instrumenty protydyi finansuvanniu teroryzmu z vykorystanniam finansovykh ustanov | [Anti-terrorist financing tools using financial institutions]. *Economy and state*, 6, 80–86. doi: 10.32702/2306-6806.2020.6.80 [in Ukrainian].

97. SAS (2021). *SAS Fraud Management*. Retrieved September 30, 2021 from https://www.sas.com/en_us/software/fraud-management.html.

98. Shackelford, S., Dockery, R., Prabhakar, B., & Raymond, A. (2021). Cybersecurity in crisis. *Business Horizons*, 64(6), 725-727. doi: 10.1016/j.bushor.2021.07.003.

99. Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers and Security*, 109. doi: 10.1016/j.cose.2021.102387.

100. Ukrainian Interbank Payment Systems Member Association (2017). *Statistika platezhnogo moshennichestva — itogi 2017-go goda (INFOGRAFIKA) | [Payment fraud statistics - results of 2017 (INFOGRAPHICS)]*. Retrieved September 30, 2021 from <https://ema.com.ua/cyberfraud-ema-statistics-results-2017/>.

101. Umadevi, P., & Divya, E. (2012). Money laundering detection using TFA system. In *the International Conference on Software Engineering and Mobile Application Modelling and Development (ICSEMA 2012)*. Chennai, India. 1-8. doi: 10.1049/ic.2012.0150.

102. Unuchek, R., Sinitsyn, F., Parinov D., & Liskin, A. (2017). *IT threat evolution Q3 2017*. Retrieved September 30, 2021 from <https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/>.

103. Verkhovna Rada of Ukraine (2017). *Postanova NBU № 95 «Pro zatverdzhennia Polozhennia pro orhanizatsiiu zakhodiv iz zabezpechennia informatsiinoi bezpeky v bankivskii systemi Ukrainy» vid 28.09.2017.* | [Resolution of the NBU № 95 On

Approval of the Regulations on the Organization of Measures to Ensure Information Security in the Banking System of Ukraine, as amended and supplemented on September 28, 2017.]. Retrieved September 30, 2021 from <http://zakon3.rada.gov.ua/laws/show/v0095500-17> [in Ukrainian].

104. Verkhovna Rada of Ukraine (2020). *Postanova NBU №65 «Pro zatverdzhennia Polozhennia pro zdiisnennia bankamy finansovoho monitorynhu» vid 19.05.2020* | [Resolution of the National Bank of Ukraine No. 65 On Approval of the Regulations on the Implementation of Financial Monitoring by Banks, as amended and supplemented on May 19, 2020]. Retrieved September 30, 2021 from <https://zakon.rada.gov.ua/laws/show/v0065500-20#Text>.

105. Verkhovna Rada of Ukraine (2021). *Zakon Ukrainy «Pro zapobihannia ta protydiuu lehalizatsii (vidmyvanniu) dokhodiv, oderzhanykh zlochynnym shliakhom, finansuvanniu teroryzmu ta finansuvanniu rozpovsiudzhennia zbroi masovoho znyshchennia», zi zminamy ta dopovnennia vid 08.10.2021.* | [Law of Ukraine On Prevention and Counteraction to Money Laundering, Terrorism Financing and Financing the Proliferation of Weapons of Mass Destruction, as amended and supplemented on October 8, 2021.] Retrieved October 08, 2021 from <https://zakon.rada.gov.ua/laws/show/361-20#Text> [in Ukrainian].

106. Work.ua (2020). *Srednyaya zarplata po kategorii «Finansyi, bank» v Ukraine* | [Average salary in the category "Finance, Banking" in Ukraine]. Retrieved September 30, 2021 from <https://www.work.ua/ru/salary-banking-finance/> [in Russian].

107. Yarovenko, H. (2020). Evaluating the threat to national information security. *Problems and Perspectives in Management*, 18(3), 195–210. doi: 10.21511/ppm.18(3).2020.17.

108. Yarovenko, H. (2021). Information Security as a Driver of National Economic Development. (*Doctoral dissertation*). Retrieved September 30, 2021 from SumDU Repository: <https://essuir.sumdu.edu.ua/handle/123456789/83664> [in Ukrainian].

109. Yashina, N. I., Kashina, O. I., Pronchatova-Rubtsova, N. N., Yashin, S. N., & Kuznetsov, V. P. (2021). Financial monitoring of financial stability and digitalization in federal districts. In book "*Smart Technologies" for Society, State and Economy*", 1045-1051. doi: 10.1007/978-3-030-59126-7_115.

110. Yong, Li (2016). *Implementation of Anti-Money Laundering Information Systems*. AuthorHouse.

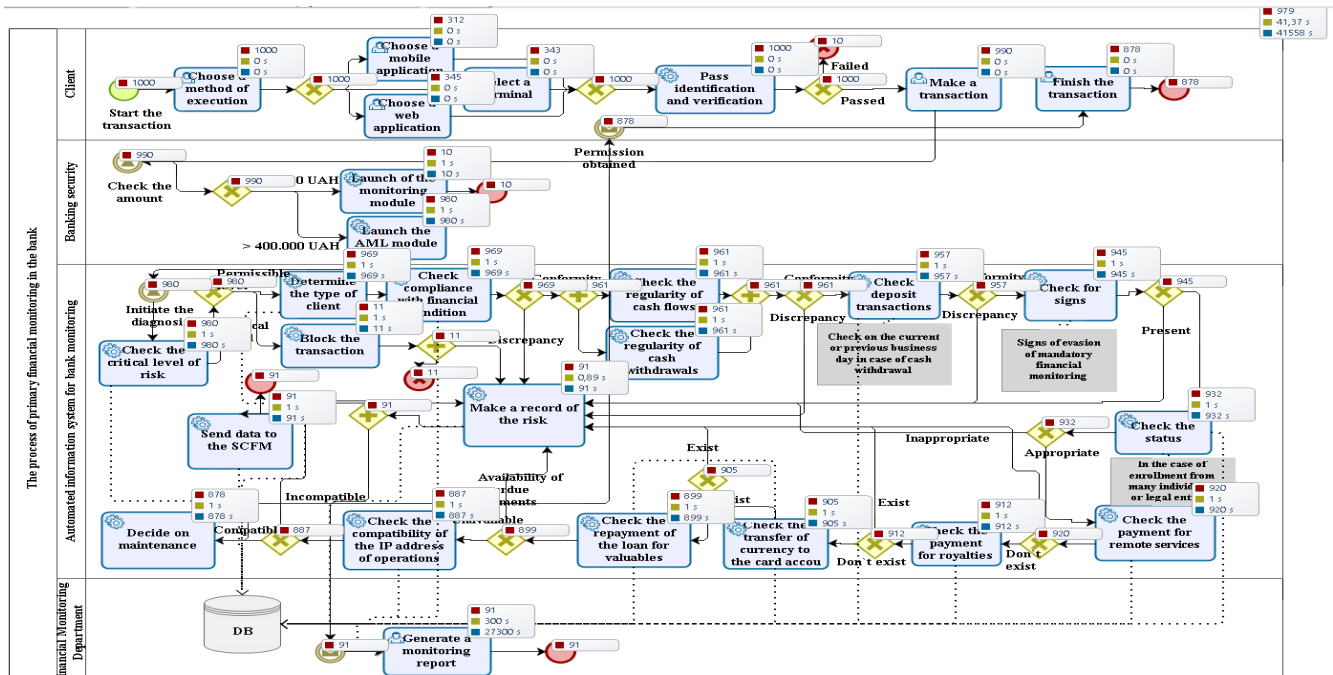


Figure A.2. Time simulation results for the business model of the automated financial monitoring process

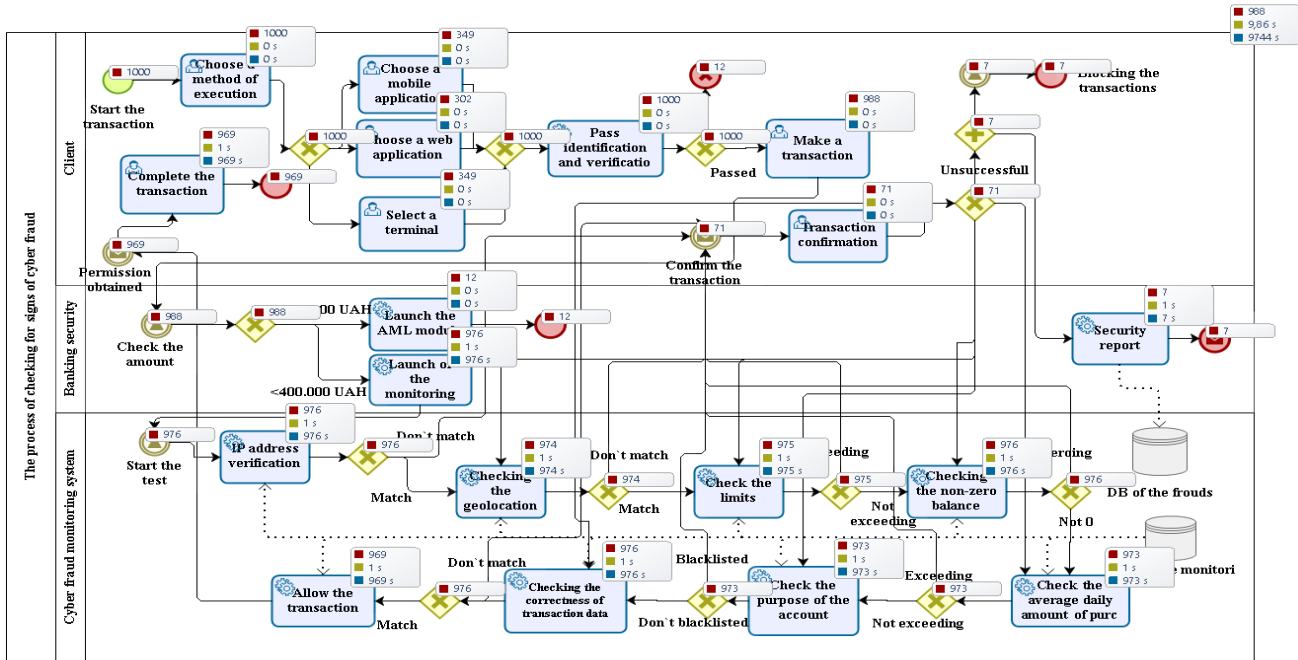


Figure A.3. Simulation of the business process of checking transactions for signs of external cyber fraud

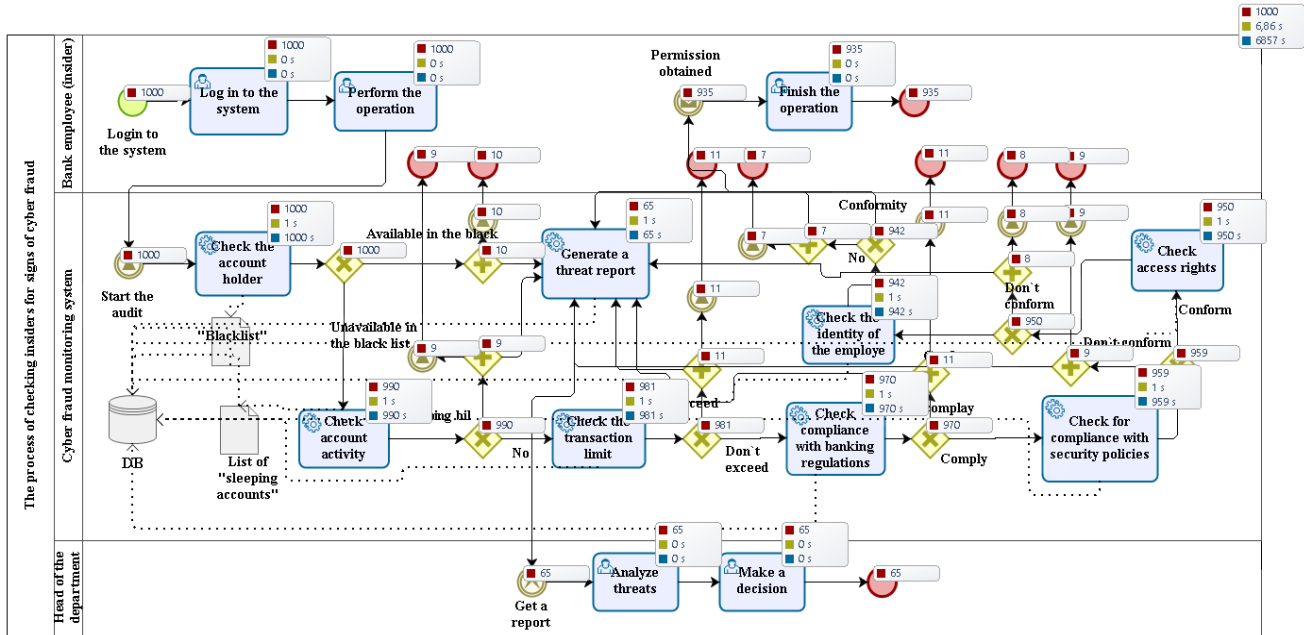


Figure A.4. Simulation of the business process of checking transactions for signs of cyber fraud by insiders

Tackling Illicit Financial Flows and Cyberattacks for Enhancing National Security

Authors

© Prof. Dr. Olha Kuzmenko
Sumy State University, Ukraine

Dr. Hanna Yarovenko
Sumy State University, Ukraine

PhD Victoria Bozhenko
Sumy State University, Ukraine

Reviewers

Prof. Dr. Ludmila Malyarets
Simon Kuznets Kharkiv National University of Economics,
Ukraine

PhD. Bholu Khan
Yobe State University, Gujba Road, Damaturu, Nigeria

Dr. Anton Boyko
Sumy State University, Ukraine

The scientific monograph was performed within the framework of the research theme «Data Mining for Countering Cyber Fraud and Money Laundering in the Context of Digitalization of the Financial Sector of the Ukrainian Economy» (0121U100467), «National security through the convergence of financial monitoring and cybersecurity systems: intelligent modeling of financial market regulation mechanisms» (0121U109559), which are financed by the State budget of Ukraine.

Author is responsible for content and language qualities of the text. The publication is protected by copyright. Any reproduction of this work is possible only with the agreement of the copyright holder. All rights reserved.

1st Edition

Range 189 pg (13.72 Signatures)

© Centre of Sociological Research, Szczecin 2021

ISBN 978-83-963452-7-1


Suggested citation:

Kuzmenko, O., Yarovenko, H., Bozhenko, V. (2021). Tackling Illicit Financial Flows and Cyberattacks for Enhancing National Security, Szczecin: Centre of Sociological Research, 189 p. ISBN 978-83-963452-7-1

ISBN 978-83-963452-7-1



9 788396 345271



THE SCIENTIFIC MONOGRAPH WAS PERFORMED WITHIN THE FRAMEWORK OF THE RESEARCH THEME «DATA MINING FOR COUNTERING CYBER FRAUD AND MONEY LAUNDERING IN THE CONTEXT OF DIGITALIZATION OF THE FINANCIAL SECTOR OF THE UKRAINIAN ECONOMY» (O121U100467), «NATIONAL SECURITY THROUGH THE CONVERGENCE OF FINANCIAL MONITORING AND CYBERSECURITY SYSTEMS: INTELLIGENT MODELING OF FINANCIAL MARKET REGULATION MECHANISMS» (O121U109559), WHICH ARE FINANCED BY THE STATE BUDGET OF UKRAINE.

FIRST EDITION, 2020
PUBLISHING HOUSE: CENTRE OF SOCIOLOGICAL RESEARCH
[HTTP://WWW.CSR-PUB.EU](http://www.csr-pub.eu)
SZCZECIN, POLAND 2020
ALL RIGHTS RESERVED.