This paper reports a study aimed at determining the features of using information protection systems at financial institutions in order to improve the level of financial security. It has been proven that under the conditions of digitization of the business environment, information provision is the basis of financial security at both the macro and micro levels. Information has become a strategic resource that needs protection due to the spread of cybercrime. The level of efficiency of information provision and the level of financial security of Ukraine was determined, and the relationship between them was confirmed. Attention is focused on the need to improve these indicators. It has been proven that an effective information protection system enables economic entities to resist dangers and threats. It was substantiated that the intensification of the processes of digitalization of economic activity had created prerequisites for the growth of risks and threats to the integral, uninterrupted, protected circulation of information resources of financial institutions, which leads to huge financial losses. This requires improvement of existing information protection systems. A topology of information protection systems has been presented. An algorithm for building effective information protection systems of financial institutions was proposed, which includes system vulnerability assessment, system assessment for compliance with security standards, penetration testing, and application assessment. Its application would allow financial market entities to promptly respond to real and potential threats, increase the level of information security, and ensure financial stability. The results of the study could also be used by state and local authorities to devise the principles of financial security management at the macro level under the conditions of the digital economy

Keywords: information security, information protection, financial market entities, financial security, digitalization

UDC 336:658+004
DOI: 10.15587/1729-4061.2023.288175

DETERMINING THE PATTERNS OF USING INFORMATION PROTECTION SYSTEMS AT FINANCIAL INSTITUTIONS IN ORDER TO IMPROVE THE LEVEL OF FINANCIAL SECURITY

Svitlana Onyshchenko
Doctor of Economic Sciences, Professor*
Yevhen Zhyvylo
PhD, Associate Professor
Department of Computer and Information Technologies and Systems**
Anna Cherviak
PhD*
Stanislav Bilko
Corresponding author
Postgraduate Student*
*Department of Finance, Banking and Taxation**
**National University «Yuri Kondratyuk Poltava Polytechnic»
Pershotravnevyi ave., 24, Poltava, Ukraine, 36011
E-mail: s.bilko.86@gmail.com

Received date 19.07.2023
Accepted date 21.09.2023
Published date 30.10.2023

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

1. Introduction

Under the conditions of strengthening the processes of Ukraine's integration into the European economic space, the growth of competition in the foreign and domestic markets, ensuring the financial sustainability, stability, and security of business entities directly depends on the level of management efficiency and the ability to adapt to an unstable business environment. At the same time, the digitalization of the economy, characterized by the intensification of the use of modern information technologies in all sectors, has led to a decrease in the effectiveness of traditional methods of justifying management decisions. Business entities are faced with the need to process large information arrays, which is impossible without the use of a set of specialized software and technical tools, as well as instructions and regulations regarding the collection, storage, and transmission of information. Given the above, the implementation of information protection systems as the basis for the safe functioning of entities in the digital economy is an urgent problem.

The information technology leap in the development of the world economy is characterized by the appearance of new risks and threats to the security of financial institutions, which are the basis of the functioning of the economy, and the state as a whole. The increase in the scale and frequency of cyber-attacks leads to huge financial losses. Financial security is an important priority of economic entities since its sufficient level creates favorable conditions for effective implementation of activities and development. In this aspect, the issue of implementing information protection systems as the basis of financial security of financial institutions becomes particularly relevant. Building a modern and effective financial security system should be based on accurate, timely, and reliable information. In the future, its functioning requires the use, processing, interpretation, and analysis of a large amount of information, and, of course, its protection. After all, under the conditions of intensification of informatization processes and progressive development of the IT industry, one of the most urgent problems is the issue of increasing the security of information resources of finan-

cial institutions against cyber incidents, that is, ensuring information security.

Ensuring information security of financial institutions involves timely detection of channels of information loss, prompt response to threats, and creation of conditions for maximum compensation of losses [1]. In this aspect, the implementation of information protection systems as the basis of information security and the basis of operational decision-making in the field of financial security management of financial institutions under the conditions of dynamic external and internal environment becomes of primary importance.

The relevance of the issue of implementing information protection systems is confirmed by the active research of scientists. Noting the role and significance of existing scientific research, it is quite obvious that under modern conditions the need to increase the protection of the interests of financial institutions against the improper use of internal information, commercial secrets, is undeniable. In connection with the above, consideration of the peculiarities of the use of information protection systems in terms of increasing the level of financial security of financial institutions is relevant.

2. Literature review and problem statement

Study [2] reports the analysis of financial security of enterprises and its management. The authors systematized external and internal threats to financial security, in particular, the crisis of the monetary and financial and credit systems was highlighted; economic instability; imperfect state economic policy; management errors, etc. However, the risks and threats that are associated with the development of the digital economy and require increased protection of information, which is the basis of management decision-making, remain overlooked. As a result, noting the presence of information support in the financial security management system, the authors do not attach great importance to the influence of this component on the level of financial security of the business entity. In other words, information security is mentioned but not analyzed in depth in the cited paper. The value of information and its protection for the financial security of economic entities is growing under conditions of digitalization.

In work [3], the digitalization of the economy is revealed as the main challenge to the security of the financial system. The need to take into account the challenges associated with digital transformation is a crucial condition for ensuring the financial security and socio-economic stability of the state. The article substantiates that ignoring the negative impact of fundamentally new threats (cybercrime in the financial system, disinformation) on the functioning of financial market entities makes it impossible to ensure financial security. According to the authors, the low level of information protection against digital threats may be a consequence of technological unreadiness for the introduction of innovations and digital technologies. Based on this, the cited work carried out a comparative analysis of the level of implementation of innovations and digital technologies in Ukraine and other countries of the world. Since the analysis is based only on the Networked Readiness Index for the years 2013–2020, these results do not necessarily accurately reflect the overall level of digitization of countries and are not relevant for the present time.

A thorough analysis of the impact of the digital economy on economic processes at the macro and micro levels and ensuring financial security is carried out in work [4]. The mechanism of the influence of the development of high-tech companies on financial security at the macro and micro levels in the plane of changes in capital costs and changes in the phases of the economic cycle was revealed. The conclusions drawn by the authors are useful for understanding the driving influence of digitalization and the cause-and-effect relationships between the level of implementation of the latest information technologies and the state of financial security of the business entity. At the same time, the study does not take into account potential benefits from the use of information protection systems alongside the implementation of information technologies.

Study [5] presents a model of effective cybersecurity management, which is based on such key components as a cybersecurity strategy, standardized processes, compliance, top management oversight, and resources. However, the model does not take into account such an important tool as testing the protection system. The intrusion detection system as a basis for the protection of information resources of economic entities is detailed in work [6]. An overview of existing intrusion detection systems is structured and presented. Attention in the research is focused on the protection of information from DdoS attacks. Other types of cyberthreats and dangers remained outside the attention of the authors.

The USA is one of the world leaders in the implementation of information technologies. This requires the implementation of an effective information security policy and the improvement of countermeasures against information threats. A study of the US government's policy on information security management [7] allowed the author to argue that the dominant concept of information security is aimed at managing uncertainty through risk management. Interdependencies and the associated difficulties of breaking ties create a kind of uncertain governance – a regime of insecurity. It is emphasized that digitalization of economic processes makes it posible to reduce costs, but at the same time requires increased security in computer networks. Since the cited article deals only with the theoretical foundations and policy of information security, the issue of evaluating the effectiveness of information security at the macro level remains unresolved.

As in [7], legislative initiatives of cyber security policy were analyzed in [8]. The article provides a retrospective analysis of the legal support for increasing cyber security resilience of the United Nations (UN) and the European Union (EU). The author identifies five factors that explain the slow development of the global cyber security management system, which underlies the complex relationship between cyber security and international law. These include the high speed of digitization; fragmentary jurisdiction and the legal problem of attribution; the regulatory role in cyberspace of the state or the private sector; inadequacy of existing norms of international law; the phenomenon of "cybermania". The result of the study is a statement about the need to expand public-private partnership in the direction of creating effective information protection systems, but there is no specification of measures in this direction.

In work [9], increasing the protection of information of economic entities is seen through the formation of an information security culture (ISP) among employees. The research model developed involves ensuring employee compliance with information security policies by facilitating factors such as supportive organizational culture, end-user

involvement, and compliance management. The results of the research are not completely accurate since the effectiveness of the model is confirmed only by a field survey.

In the context of the development of the global digital ecosystem, scientists consider the issue of increasing the level of economic and financial security of business entities by outlining strategic tools for managing the security system and improving information protection processes at the enterprise [10]. Based on the use of methods of economic statistics (statistical observation, dynamic and structural analysis), the hypothesis about the relationship between informatization and economic security of trade enterprises was confirmed. The proposal to supplement the already existing methodology for assessing the economic security of a trading enterprise with indicators that reflect the impact of digital technologies is substantiated. However, the study is based on the analysis of actors in the field of trade and does not take into account other industries.

In work [11], an authentic approach to managing the financial and economic security of the enterprise is proposed that outlines two blocks of organizational and methodical support for this process: organizational and methodical. These blocks are based on the information protection system as an integral element of the secure activity of the business entity under modern conditions. At the same time, there are no proposals for improving the protection of information resources in the study.

Taking into account the practical value of the results of the above works, there remain many unresolved issues related to a comprehensive approach to ensuring the financial security of financial market entities under the conditions of the digital economy. Therefore, there are reasons to believe that the implementation of effective information protection systems will allow financial institutions to make timely adjustments and increase the protection of data against risks and threats. The problem of using information protection systems as the basis of financial security of subjects under the conditions of digitalization is extremely important. This necessitates further research.

3. The aim and objectives of the study

The purpose of this study is to determine the peculiarities of the use of information protection systems at financial institutions as a basis for increasing the level of their financial security under the conditions of the digital economy. This will allow for a prompt response to real and potential threats, in order to increase the level of information security of financial market entities and ensure their financial stability.

To achieve the goal, the following tasks were set:

– to justify the relationship between the level of information provision and financial security;

– to implement the topology of information security and cyber security systems of financial market entities;

– to determine the algorithm for building effective information protection systems at financial institutions as a basis for financial security.

4. The study materials and methods

Under the conditions of the aggravation of global crisis phenomena in all aspects of social life, financial security is one of the priorities of state policy since the availability of favorable conditions for economic recovery and growth depends on the adequacy of its level. At the same time, the rapid development of computer technologies and the global nature of mass communication systems testify to the growing role of the information component in ensuring both financial and national security as a whole [12]. It can be argued that information has become a strategic resource, the security of which depends on the security of the economic interests of citizens, businesses, and the country.

Taking into account the above, the object of our study is information protection systems at financial institutions. It is assumed that the level of security of economic data of financial market subjects depends on their ability to ensure financial security.

In order to substantiate this hypothesis, using economic-statistical, graphical methods and correlation-regression analysis, the relationship between the level of information security and financial security at the macro level has been proven. In this aspect, the level of financial security of Ukraine was determined taking into account the structural components determined on the basis of the Methodological recommendations for calculating the level of economic security of Ukraine [13]. The structural components of financial security are banking security, security of the non-banking financial sector, debt security, budget security, currency security, monetary security. These components directly affect the level of financial security and are the basis for determining the direction of neutralization of threats in the financial sector. Using the indicator method and retrospective analysis, the absolute values of the indicators of the components of financial security for the years 2013–2021 were calculated.

The next stage, in the process of diagnosing the financial security of the state as a complex phenomenon, was the aggregation of indicators into one integral assessment.

Information support at the macro level is proposed to be evaluated through the level of effectiveness of the state information policy. Based on the method of critical analysis, it was determined that the integral indicator of information policy efficiency can be based on global indices. These include the Press Freedom Index, the Social Progress Index, the e-Government Development Index (EGDI), and the Global Innovation Index. The specified indices contain indicators that characterize the level of effectiveness of information policy. Calculation of the level of effectiveness of information policy through retrospective analysis was based on the application of methods of quantization (reducing qualitative indicators to a quantitative form), smoothing, normalization, and the method of principal components (determining the weighting coefficients of the components of information policy). Conclusions regarding the existence of a relationship between information provision and financial security were drawn within the framework of probability theory based on correlation-regression analysis tools and using a graphic method.

The next stage of the research was the topology of information security and cyber security systems of financial market entities based on such statistical methods as grouping and classification, abstract-logical method, and generalization.

The theoretical and methodological basis of our analysis are modern concepts of financial security of the state, research by scientists in the field of information protection systems and digitalization of the economy, reports and analytical materials by leading analytical centers.

5. Results of research into improving information protection systems at financial institutions in terms of ensuring their financial security

5. 1. Determination of the relationship between the level of information support and financial security

In modern conditions, financial security is a multifaceted category that has an interdisciplinary and convergent nature, which is manifested in a close relationship and interdependence with other components of national security. Ensuring financial security, both at the macro and micro levels, involves establishing an effective management and decision-making process in order to prevent and minimize the negative impact of risks and threats from the external and internal environment [14]. An integral part of making managerial decisions both at the level of enterprises and at the level of the state is to legitimately define the process of accumulating, processing and analyzing a large mass of information. This process is information provision.

Information support is interpreted by economists as a system of qualitative and quantitative indicators that provides subjects of management activity with information and information technologies for the purpose of realizing established goals and objectives [15]. A number of scientists consider it as a type of ensuring management processes, which includes a set of information resources, means, methods and technologies for collecting, processing, and issuing information used in the interests of economic entities [16, 17].

In the context of ensuring financial security, information security is aimed at fulfilling the task of qualitatively meaningful transformation of information for management needs in the security sphere. Functionally overlapping with scientific and managerial activities, information security is focused on providing preventive data protection against potential and real risks and threats.

The effectiveness of information provision at the macro level can be legitimately considered through the effectiveness of the state information policy. It should ensure the protection of the national economic interests of citizens, businesses, and the country in the information space, the development of information stability in society, and counteract possible risks and threats [18]. The state information policy should ensure the security, reliability, and safety of data, access to them, and transfer to public administration entities for decision-making. There is no clearly established methodology that would allow evaluating the effectiveness of information provision at the macro level. At the same time, taking into account the approaches of scientists and indicators that are the basis of a number of world ratings, it is proposed to evaluate the effectiveness of information support based on an integral method. The integral indicator of the effectiveness of information provision in the study is based on such global indices as Press Freedom Index, Social Progress Index, EGDI, Global Innovation Index. These indices include indicators capable of characterizing the level of efficiency of information provision. PFI makes it possible to determine the level of transparency and openness of the country's information environment, the level of freedom of speech. The SPI includes 54 indicators grouped into three areas: provision of opportunities for people, satisfaction of basic human needs, provision of the basics of well-being (including access to information and communications). EGDI includes three sub-indices (online services, telecommunications infrastructure, human capital). This index makes it possible to assess the readiness of the government to use information and communication technologies to provide quality information and public services to the population.

A retrospective analysis of Ukraine's positions in the specified global indices allows us to outline the following trends.

In the PFI 2021 rating, Ukraine lost one position compared to the previous year and took 97th place out of 180. Analysts characterize the situation in Ukraine as "problematic". The Institute of Mass Information (IMI) at RSF counted more than 170 cases of violence against media workers. In comparison, Germany lost 2 positions and took 13th place. In 2020, there were about 65 cases of violence against journalists in Germany. The first positions in the rating belong to Norway, Finland, Sweden, and Denmark [19].

According to the "Press Freedom Index 2022" published in May 2022, Ukraine was in 106th place, having lost 9 positions. The report highlights the spread of chaos (fake news and propaganda) in the unregulated world's online information space. The international human rights organization "Reporters Without Borders" links Ukraine's loss of positions to the military aggression of the Russian Federation, noting such negative factors as dangerous conditions for the media, a high level of censorship in the occupied territories, and mass disinformation.

In 2021, Ukraine took 48th place out of 163 in terms of social development, rising 15 positions compared to the previous year [20]. It should be noted that in 2020, the number of countries included in the states with very high quality of life, high quality of life, and moderately high quality of life decreased from 104 to 71 [21]. This is due to the pandemic, the deterioration of access to primary medical services, and the increase in the burden on health care systems.

According to the "E-Government Survey 2020" research, Ukraine belongs to the group of countries with a high level of development. In 2020, Ukraine took 69th place in the ranking of countries with the most developed electronic governance [22]. The positive dynamics of Ukraine's positions were largely influenced by the creation of the DIYA application. The leaders in the rating are Denmark, South Korea, Estonia, and Finland.

The positions of Ukraine in the specified ratings are given in Table 1.

Table 1

Ukraine's Position in the Rankings Characterizing the Effectiveness of Information Support at the Macro Level in 2013–2021 [19, 20, 22, 23]

Global index	2013	2014	2015	2016	2017	2018	2019	2020	2021
Press Freedom Index	126	127	129	107	102	101	102	96	97
Social Progress Index	–	62	62	63	88	64	80	63	48
EGDI	–	87	–	62	–	82	–	69	–
Global Innovation Index	71	63	64	56	50	43	47	45	49

Taking into account the above, it is legitimate to note that Ukraine has a positive dynamic regarding the growth of the level of efficiency of information provision at the macro level. At the same time, in order to confirm this statement, using quantization and smoothing methods (for those years where official data are not available), certain qualitative indicators of the effectiveness of information provision at the macro level were represented in a quantitative form (Table 2).

The next stage was the normalization of indicators, the results of which are given in Table 3.

The determined integral indicator of the efficiency of information provision of Ukraine (Fig. 1) proves the growth of the level of efficiency of information provision. The built trend line substantiates a stable trend to the next increase (value of approximation reliability R^2=0.811).

The next stage of the research is to establish the relationship between information provision and the level of financial security at the macro level. For this purpose, on the basis of the Methodological recommendations for calculating the level of economic security of Ukraine, the absolute values of the indicators of the components of financial security were calculated and the integral indicators were determined, summarized in Table 4.

The calculation of the level of financial security of Ukraine was carried out taking into account the above structural components and their weighting factors, determined by the Methodological recommendations for calculating the level of economic security of Ukraine. The integral indicator of Ukraine's financial security (Fig. 2) proves its dangerous level and the need to implement operational measures to increase it. In this aspect, an effective system of information support, which makes it posible to resist dangers and threats that can cause financial damage, is one of the main components of the system of ensuring the financial security of the state.

Based on our analytical studies, using the tools of correlation and regression analysis, the relationship between the level of efficiency of information provision and the level of financial security of the state was established. The graphic interpretation of the results is shown in Fig. 3.

Table 2

Indicators of efficiency of information support of Ukraine for 2013–2021, brought to quantitative form by the method of quantization

Global index	2013	2014	2015	2016	2017	2018	2019	2020	2021
Press Freedom Index	0.300	0.294	0.283	0.406	0.433	0.439	0.433	0.467	0.461
Social Progress Index	0.620	0.620	0.620	0.614	0.460	0.607	0.509	0.614	0.706
EGDI	0.466	0.466	0.543	0.620	0.558	0.497	0.537	0.577	0.577
Global Innovation Index	0.564	0.614	0.607	0.656	0.693	0.736	0.712	0.724	0.699

Table 3

Normalized indicators of effectiveness of information policy and information support of Ukraine for 2013–2021

Global index	2013	2014	2015	2016	2017	2018	2019	2020	2021
Press Freedom Index	0.075	0.074	0.071	0.101	0.108	0.110	0.108	0.117	0.115
Social Progress Index	0.155	0.155	0.155	0.153	0.115	0.152	0.127	0.153	0.176
EGDI	0.117	0.117	0.136	0.155	0.140	0.124	0.134	0.144	0.144
Global Innovation Index	0.141	0.153	0.152	0.164	0.173	0.184	0.178	0.181	0.175
Integral index	0.488	0.499	0.514	0.573	0.536	0.570	0.547	0.595	0.610

Table 4

Integral indicators of structural components of financial security of Ukraine for 2013–2021

Integral index	2013	2014	2015	2016	2017	2018	2019	2020	2021
Bank security, %	41.1	29.0	37.1	35.5	43.2	46.1	27.0	48.1	49.2
Security of the non-banking financial market, %	49.0	46.0	36.1	32.4	30.0	33.0	34.9	33.5	34.0
Debt security, %	65.0	37.0	36.6	38.0	39.9	42.4	48.2	42.24	37.51
Budget security, %	56.0	47.0	36.6	38.0	39.9	42.4	48.2	50.0	55.4
Currency security, %	44.0	26.0	36.0	38.8	40.2	42.0	41.0	46.3	48.74
Monetary security, %	59.0	70.0	44.9	54.9	54.5	42.3	36.5	38.0	39.2

Note: calculated by authors according to the methodology [13]

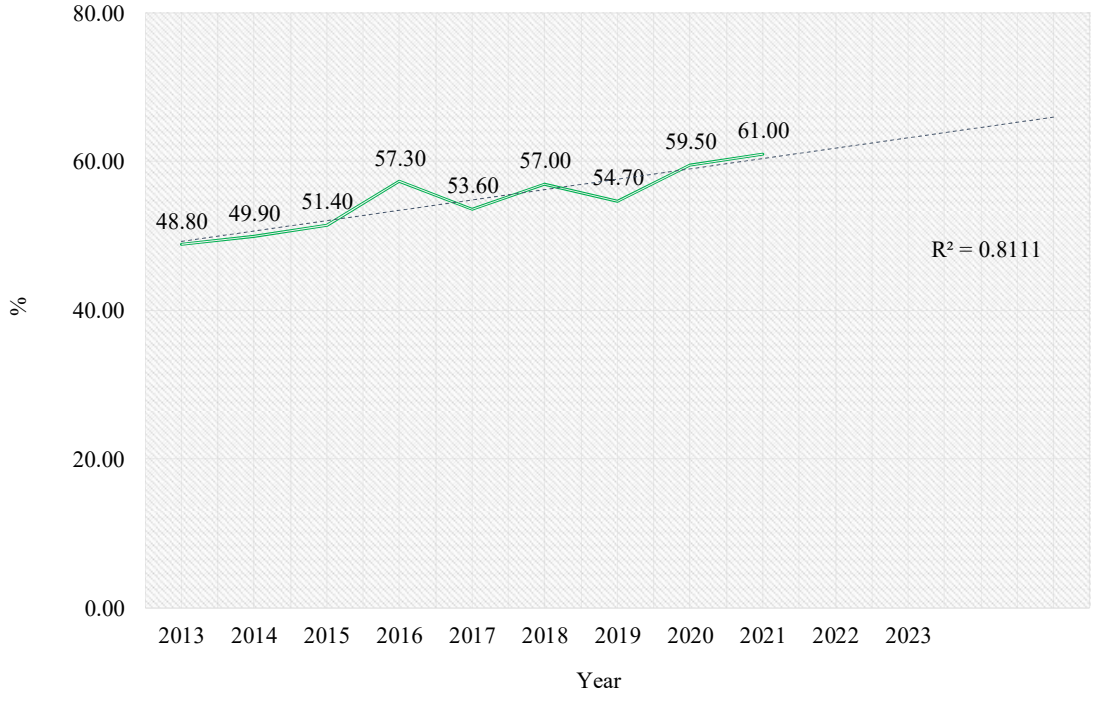

Fig. 1. Integral indicator of the level of efficiency of information support at the macro level in Ukraine

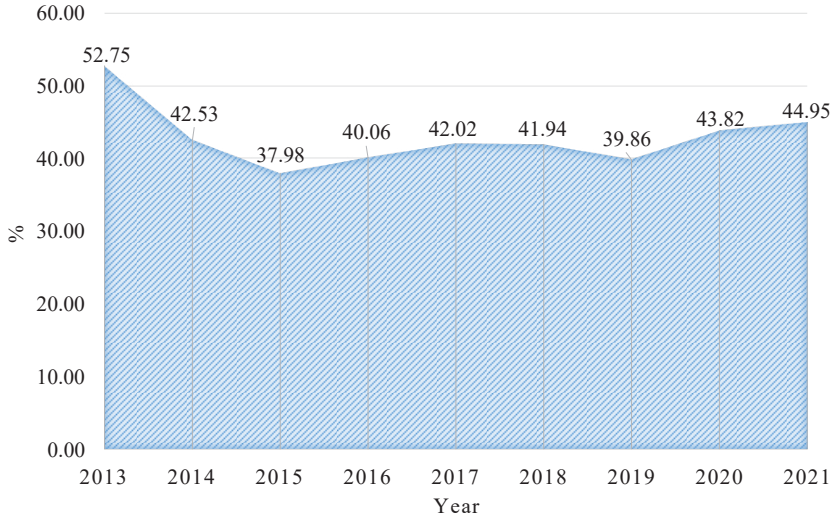

Fig. 2. Dynamics of the level of financial security of Ukraine in 2013–2021

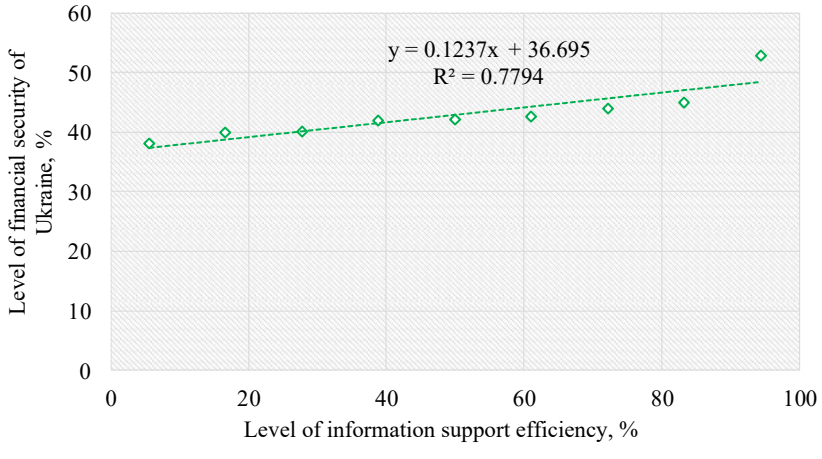

Fig. 3. The relationship between information support and the level of financial security of Ukraine

The value of the correlation coefficient is 0.2165. That is, during the years 2013–2021, there was a direct relationship between the level of financial security of Ukraine and the level of efficiency of information provision. The average bond strength is noted. Thus, the proposed hypothesis regarding the importance of information support in the financial security system of Ukraine is confirmed.

The calculated elasticity coefficient proves that with a 1 % increase in the level of efficiency of information provision, there is an increase in the level of financial security of Ukraine by 0.097 %.

At the micro level, information provision of financial security has its specificity for each economic entity, which is determined by the specifics of risks and threats to the activities of enterprises of various industries, organizational and legal forms, etc. [24]. Information provision of the financial security of economic entities characterizes the level of their access to the necessary information, the efficiency of its storage, use, protection, the possibility of conducting business intelligence, and the ability of the information and analytical system of economic entities to develop [25]. The effectiveness of information provision of financial market entities involves:

– opportunities for timely detection of information loss channels, potential threats and their level of importance, types of information theft subjects, methods of their actions;

– prompt response to real and potential threats;

– provision of compensation for losses;

– prevention of economic and industrial espionage.

The dependence of economic entities on information systems and their services causes an increase in their vulnerability to information threats. The increase in the interaction of public and private networks, the joint use of information resources cause an increase in difficulties in managing access and providing guarantees of services and security of information and communication systems and networks. Digitalization of economic activity creates conditions for the growth of cases of unauthorized use of computer networks and systems, that is, an increase in cybercrime [26].

In the financial industry, threats to information and cyber security changed the paradigm of banking operations several decades ago, as they can disrupt banking functions and cause significant direct and indirect losses [27]. In today's environment, financial services, sensitive data, transactions, customer account information and private personal data are the primary targets for cybercriminals. Therefore, institutions, banking structures, and other persons operating in financial services markets face a rather significant problem of determining the procedure for forming requirements and implementing measures to ensure cyber protection and information security. In this aspect, the issue of implementing effective information protection systems is a priority for financial market entities.

5. 2. Topology of information security and cybersecurity systems of financial market entities

According to the available assessments of IT experts and the analysis of publications and articles from open sources, the topology of the information security and cyber security systems of the entities of the global financial market are kept secret. At the same time, it is known that these systems are used to check the security of their own communication systems, and their construction is quite extensive and not of the same type with defined connections between them and united by a single management.

Under these conditions, the transformation of views on the issue of creating information protection systems in Ukraine takes place under the influence of technological development, changes in the financial security environment, forms, methods, and technologies of using cyber-influence means [28].

The classical topology of information protection systems is based on their functional purpose (Fig. 4). Information protection systems can be aimed at preventing threats, their prevention, recovery, etc.

Fig. 4. Topology of information security systems of economic entities by functional purpose

The Prevention protection system is based on measures of early detection, avoidance, deterrence, prevention of possible (potential) cyber threats or cyber attacks, and termination of preparations for them. The Protection system provides for anticipatory protection against possible cyberattacks (cyber influence) of attackers, in the interests of comprehensive and sustainable provision of own asset management processes in cyberspace. The Mitigation protection system includes measures for direct detection, averting the threat, and reducing possible losses (damages, damages) in the event of an immediate threat of cyber-attacks. Under certaunder conditions, anticipatory (anticipatory) measures of active cyber protection may be carried out within the specified limits. Response provides comprehensive countermeasures and actions to prevent potential threats, including by means of active cyber protection under the conditions of direct cyber attacks with the simultaneous implementation of measures to protect one's own infrastructure from intruders. The Recovery system is aimed at restoring information and other infrastructure that has become the object of cyberattacks by fraudsters, stabilizing the situation and eliminating other negative consequences.

At the same time, the constant transformation and emergence of new modified threats to information and cyber security requires financial market entities to increase efficiency and modernize existing information protection systems.

In today's environment, financial institutions are increasingly exposed to security threats due to the widespread adoption of online financial transactions and services. Therefore, it is important to ensure the integrity and confidentiality of information when performing any operations in a virtual environment.

The analysis of the current information protection systems of financial institutions of Ukraine confirms that the information and cyber security policy is carried out in accordance with the legislation of Ukraine, the normative legal acts of the National Bank of Ukraine, taking into account international standards, in particular:

1. Resolution of the Board of the National Bank of Ukraine dated September 28, 2017, No. 95, document v0095500-17, "On approval of the Regulation on the organization of measures to ensure information security in the banking system of Ukraine".

2. The Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine" (Verkhovna Rada Bulletin, 2017, No. 45, Article 403, with amendments), document 2163-VIII.

3. Law of Ukraine "On Banks and Banking Activity" (News of the Verkhovna Rada of Ukraine, 2001, No. 5, 6, Article 30, with amendments), document 2121-III.

4. National standard of Ukraine on information security DSTU ISO/IEC 27000:2015 "Information technologies. Protection methods. Information security management system. Review and dictionary".

5. National Standard of Ukraine on Information Security DSTU ISO/IEC 27001:2015 "Information Technologies. Protection methods. Information security management systems. Requirements".

6. National Standard of Ukraine on Information Security DSTU ISO/IEC 27002:2015 "Information Technologies. Protection methods. A set of practices regarding information security measures".

7. Internal Statutes.

The above regulatory documents and standards provide requirements for the minimum necessary package for creation, implementation, technical support [29], and improvement of the information security and cyber protection management system. At the same time, more and more organizations are also realizing that traditional information protection systems and manual procedures are no longer sufficient to implement and maintain security policies.

Modern structures of information protection and cyber security systems must meet international standards, standards of the European Union and NATO, provide for the use of a powerful line of tools at both the technological and software levels. They should be based on the use of branched architectures, protection methods that are aimed at anticipating, detecting, and responding to potential cyber threats.

Analysis of information protection systems of financial market entities in Ukraine allows us to single out the leaders in this area: Raiffeisen Bank Aval, Ukrsibbank BNP Paribas Group, Kredobank, and Privatbank. These institutions systematically protect their critical online assets from a wide range of cyber-attacks, implement modern protected online banking programs, proactively react to leaks of confidential customer data. They implement the latest tools to detect and locate malicious, careless, and compromised users, and optimize auditing by complying with a number of international regulations and industry standards.

The information protection systems of these financial institutions are based on information security requirements specified in such international standards as:

1. Payment Card Industry Data Security Standard (PCI-DSS).

2. Sarbanes-Oxley Act (SOX).

3. Monetary Authority of Singapore-Technology Risk Management (MAS-TRM).

4. General Data Protection Regulation (GDPR).

These documents contain requirements for information protection systems (Table 5), compliance with which allows ensuring a high level of information security at financial institutions.

Compliance with systematized requirements will allow financial market entities to ensure the security and confidentiality of customer information, data integrity; protection against unauthorized access to information; implementation of preventive measures against possible risks.

Table 5

Systematization of normatively established requirements for information security [30–33]

Requirement (need)	Regulations governing activities	Capability
Identifying confidential data/assessing risks, security gaps and vulnerabilities	PCI 2	Detection of active database services and regulated data stored in databases, cloud applications
	PCI 6.1	
	MAS 2.0.1	Risk assessment of database vulnerabilities, each asset, data sensitivity, configuration flaws
	MAS 2.0.5	
	SOX 302	Identifying authorized and unauthorized cloud applications that users have access to and assessing the risks of each of them
	SOX 404	
	GDPR Article 25/32/35	
Implementation of security controls	PCI 3	Web Application Firewall (WAF) – Protects public web applications
	PCI 6.6	Virtual patch installation
	PCI 7	Compensatory control that makes it possible to block web application vulnerabilities
	PCI 8.5	Runtime Program Self-Defense (RASP) – neutralizes threats in production
	PCI 11.5	
	MAS 5.1.2	Account Hijacking Protection – Mitigate malicious ATO attacks without affecting legitimate users
	MAS 5.1.7 (c/d/j)	
	MAS 12.1.6	Cloud Application Delivery Service - Protects websites from DDoS attacks
	SOX 302	User Rights Management – helps implement least privilege and business access
	SOX 404 GDPR Article 5/25/32	Data masking – eliminates the use of sensitive data in non-production systems by restricting access
Auditing, monitoring and ensuring access	PCI 10	Database and file activity monitoring collects and records database and file access and activity details
	PCI 12	
	MAS 5.1.2	Notification and blocking of access mode to regulated data in databases and files in order to reduce the risks of data breach
	MAS 5.1.7 (b, e, f, j)	
	SOX 302	Predefined PCI and SOX audit policies provide an automated audit log
	SOX 404	Privileged user access audit, monitoring of all privileged user actions, direct access to the database server
	SOX 409	
	GDPR Article 25/32/33/34/35/44	Basic user data access policies
Reporting	PCI SOQ	Preliminary preparation of reports for PCI, SOX and other regulatory acts
	SOX 302	Elimination of a human resource that is prone to errors and takes a lot of time to prepare reports
	SOX 404	
	SOX 409	Reconciliation of SOX changes shows SOX auditors that database changes can be traced back to approved ticket change requests
	GDPR Article 32/33/34	

5. 3. Development of an algorithm for building effective information protection systems at financial institutions as a basis for financial security

In modern conditions, information protection and cyber security systems of corporations and institutions of the global financial market process and store a rather powerful array of confidential data. This data will include customer transactions, account information and private personal data of payment cards, payment processors, and more [34]. The effectiveness of their operation is complicated by the constant change in the volume, speed, and variety of attacks, which vary from denial of service to malicious theft from the inside. Therefore, there is a need to use non-traditional approaches to the implementation of security measures.

The Kali Linux distribution can rightfully be defined as the most powerful preventive tool for protection against information and cyber risks in the world today. This distribution includes penetration testing, forensics, reverse engineering, and vulnerability assessment. It is the culmination of many years of improvements and the result of a continuous evolution from WHoppiX to WHAX, then to BackTrack, and now to a full-fledged penetration testing distribution. Kali uses many of the features of Debian GNU/Linux and takes into account the valuable advice of members of the dynamic global community of dedicated open-source software.

Taking into account the availability of traditional and non-traditional tools for ensuring information security, the construction of an effective system of information protection at financial institutions should involve a certain phasing (Fig. 5).

Therefore, according to the presented algorithm, it is possible to ensure an effective information protection system only if it is systematically analyzed and evaluated. This process includes system vulnerability assessment, system security compliance assessment, penetration testing, and application assessment.

Vulnerability testing of systems due to its simplicity is often performed on a regular basis in a fairly sophisticated branched architecture as part of demonstrating their level of security or compliance with some security standard. Utilities used to detect live systems in a target environment identify services, scan some ports, and analyze them to gather as much information as possible about the system. The collected information is then checked for known signatures of vulnerabilities. The latter consist of combinations of data fragments that allow recognition of known security problems. Here, as much information as possible is used because the more information there is, the more accurate the identification of the vulnerabil-

ity will be. There are many indicators that are of interest when analyzing system vulnerabilities. Among them, the following can be named: operating system version, patch level, processor architecture, target software version.

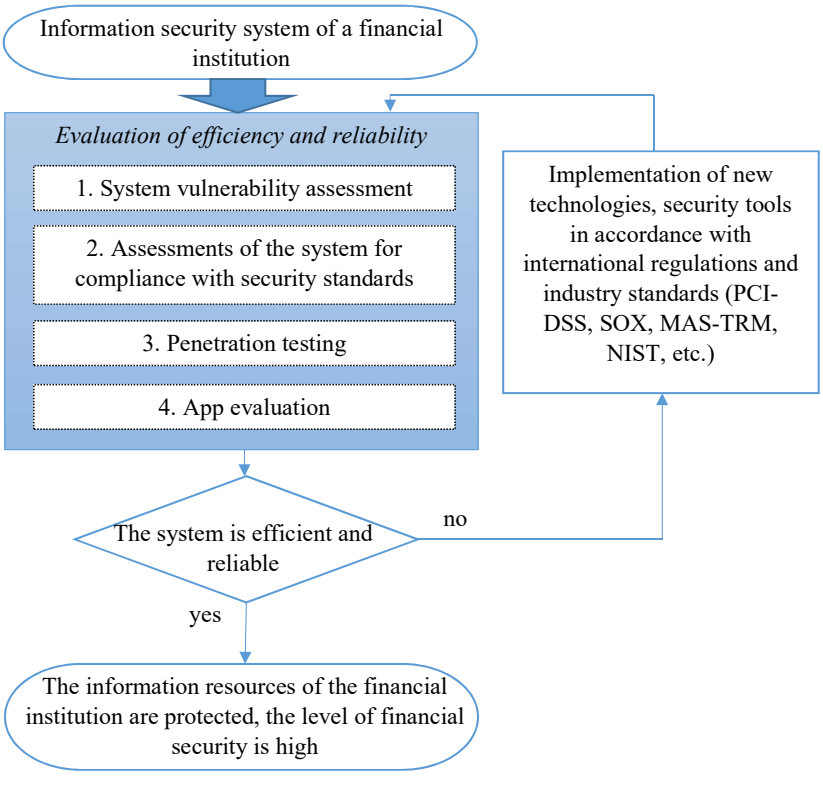

Fig. 5. Algorithm for building an effective information security system at financial institutions

When the scan is complete, detected vulnerabilities are typically associated with standard identifiers such as CVE [35], EDB-ID, or vulnerability classification codes accepted by scan tool vendors. This information, together with CVSS vulnerability assessment information [36], is used to determine the level of risk. All this information, taking into account false positive and false negative reports of vulnerabilities, gives a general idea that must be taken into account when analyzing the scan results.

Since automated tools are used to detect vulnerabilities in signature databases, the slightest deviation from a known signature can change the result and, accordingly, the validity of reports about detected vulnerabilities. At the same time, false positive results indicate something that is not there, and false negative results, on the contrary, hide existing problems. Therefore, the quality and capabilities of automatic vulnerability scanners directly depend on the signatures used by databases.

The next stage is the assessment of systems for compliance with security standards. Such system tests are quite common, as they are based on the analysis of requirements defined by government and industry standards that apply to organizations, such as PCI-DSS, DISA STIG, FedRAMP, FISMA. Many organizations use Kali Linux as a platform specifically for evaluating systems for compliance with security standards.

The third stage of evaluating the effectiveness and reliability of information protection systems involves penetration testing. Traditional penetration tests rarely start with defining the scope of the test. Instead, certain goals are set for them. For example: "simulate the consequences of an internal user being compromised" or "find out what would happen if the organization came under a targeted attack by an external attacker". The key difference of such an analysis is that in the course of its execution, vulnerabilities are not only found and evaluated but also the threats found are used to reveal the worst-case scenarios. Penetration testing does not rely solely on vulnerability scanning tools. Work continues with vulnerability research, exploits, or testing to eliminate false positives, and every effort is made to identify hidden vulnerabilities. Such research often involves exploiting the identified vulnerabilities, assessing the level of access provided by the exploits, and using this increased level of access as a starting point for additional attacks on the target system.

Despite the complexity and multi-facetednes of traditional penetration testing, the course of such research can be streamlined by dividing it into several steps: gathering information, identifying vulnerabilities, exploiting vulnerabilities, penetrating, and extracting data, and preparing reports.

The peculiarity of the fourth stage – evaluation of applications – is the fact that a specific program is subject to study. Such checks are becoming more and more common due to the specifics of the applications used by financial companies. Most of these programs are created directly by businesses and institutions. A number of applications that should be analyzed from a security standpoint include:

1. Web applications. Standard tests quite often make it possible to detect basic problems of web applications.

2. Application and server applications, in particular applications for reading PDF files or video programs that use Internet resources. To date, attackers are constantly improving their means of defeating these applications on the Internet, so assessing their vulnerability is undeniably necessary.

3. Mobile applications. With the increasing popularity of mobile devices, these applications are becoming a constant subject of security research. Such programs develop and change very quickly, so the research methodology in this field has not yet reached sufficient maturity, which leads to the regular, almost weekly, appearance of new procedures.

Application research can be done in different ways. For example, to identify potential threats, it is possible to apply automatic tools designed to test a specific program. Based on the specifics of the applications, such tools try to find unknown weaknesses in them, instead of relying on a set of predefined signatures. Tools for program analysis must take into account the specifics of their tactics. In particular, the Burp Suite web application vulnerability scanner [37] is common. During the study of the application, it finds the fields for entering data, after which it applies various attacks by means of SQL injections while observing the "behavior" of the application, in order to identify attacks that were successful.

There are also more complex application analysis scenarios. Such checks can be performed interactively. When conducting them, they use "black and white box" models.

Black-box research method: the tool (or researcher) interacts with the application without having special knowledge about it or special access to it beyond the capabilities of a typical user. For example, in the case of a web application, a researcher may only have access to functions and features open to a user who is not authorized in the system. Any account will be the same as a normal user can register themselves. This will prevent an attacker from analyzing functionality that is only available to privileged users whose accounts must be created by an administrator.

White-box research method: the tool (or researcher) often has full access to the application's source code, administrator access to the platform it runs on, etc. This ensures that a full and thorough analysis of all the application's capabilities is performed regardless of where it is located functionality under investigation. The disadvantage of such a study is that it is not an imitation of the actual actions of an attacker.

Of course, there are shades of gray between white and black – a combined method. Usually, such an application research algorithm will be conducted depending on the goal. If it is about determining what might happen to an application that is the subject of a targeted external attack, then black-box testing is probably best suited. If the goal is to identify and eliminate as many security problems as possible in a relatively short time, then white box research can be more effective.

In other cases, a hybrid approach can be used. The researcher does not have full access to the source code of the application for the platform on which it runs but the account given to him by the administrator gives access to the maximum possible number of functions of the application.

In the case of successful completion of the specified four assessment stages, the information protection system in a financial institution can be considered reliable and provide a high level of information and financial security of the financial market entity. In the opposite case, it becomes necessary to introduce new technologies, security tools in accordance with international regulations and industry standards (PCI-DSS, SOX, MAS-TRM, NIST, etc.) in order to improve the existing information protection system.

6. Discussion of results of the study on the improvement of information security systems at financial institutions

The relationship between the level of information provision and financial security has been established. Its existence is proven by the tools of correlation-regression analysis (Fig. 3) based on the preliminary determination of the integral indicator of the level of information provision (Fig. 1) and the level of financial security of Ukraine (Fig. 2). Our result correlates with the conclusions of previous scientific works. In particular, paper [10] confirms the hypothesis of the relationship between digitization and the results of business entities in the field of trade. At the same time, the advantage of our research is the presentation of the authentic methodology for determining the effectiveness of information provision at the macro level, which is based on the indicators of global indexes (Tables 1–3). This procedure is based on an integrated approach and involves considering all sectors of the national economy.

A detailed topology of information protection systems at financial institutions is presented (Fig. 4, Table 4), which was not reflected in previous scientific works. Taking into account the achievements of scientists in the field of information protection, systematized models of corporate security solutions of the Secure SaaS template, which are used for the purpose of checking risks [38], it is right to note the speed with which risks and threats are transformed in cyberspace. This requires the introduction of new protection tools against information and cyber risks. This paper describes one of the latest Kali Linux distributions, which is an important addition to existing research in this area.

An algorithm for building effective information protection systems at financial institutions is proposed as a basis for financial security (Fig. 5). This algorithm is based on systematic vulnerability assessment of the system, assessment of system compliance with security standards, penetration testing and application assessment. Application of the developed algorithm by financial institutions is one of the conditions for building an effective information protection system in the digital economy. The result is an important addition to the work of leading foreign specialists [39], aimed at detecting errors in information protection systems, but does not take into account other components of the systems.

Thus, the identified problem of the lack of a comprehensive approach to ensuring the financial security of financial market entities due to the improvement of the effectiveness of information protection was eliminated.

Emphasizing the importance of the current research, the limitation of the proposed approach to the use of information protection systems as the basis of financial security is insufficient access of financial institutions of Ukraine to the latest global information protection tools. The main drawback is the difficulty of taking into account dynamic changes in both economic data protection tools and risks and threats to information and cyber security. In this aspect, the development of Ukraine's cooperation with world leaders in the field of cyber security is important. Therefore, the development of this study involves a thorough analysis of the current information protection systems at financial institutions in the leading countries of the world. This will make it possible to determine those of them whose experience is optimal for implementation by the entities of the financial market in Ukraine.

7. Conclusions

1. It has been established that digitalization of the world economy and the economy of Ukraine creates a number of undeniable opportunities, in particular, ensuring rapid economic growth, raising the standard of living of the population, developing high-tech and innovative industries, etc. At the same time, this creates new risks for business, including threats in the digital space, and requires an appropriate response and a systemic approach from both the state and business entities. Considering that under the conditions of digitization, information has become a strategic resource, information security is rightly defined as the basis of financial sustainability, stability, and security of economic entities and the country as a whole.

In order to substantiate the value of information provision in the financial security system, the study, based on the integral method and correlation-regression analysis, established the relationship between the level of information provision and financial security at the macro level. The obtained results allow us to assert that an effective system of information support allows economic entities and the state

to resist risks and threats and is one of the main conditions for ensuring their financial security.

2. It is substantiated that the effectiveness of information provision involves prompt identification and timely response to risks and threats to economic data; creating conditions for reimbursing damages; avoidance of economic and industrial espionage.

As part of solving the task of ensuring the reliability, confidentiality, and integrity of information resources as the basis of the company's financial security, the topology of information protection systems is given, and the current legal framework is analyzed. It has been established that the modernization of structures and topologies of information protection systems takes place under the influence of technological development, changes in the security environment itself, forms, methods and technologies of using means of cyber influence and new achievements in this regard. These measures are carried out in accordance with international regulations and industry standards (PCI-DSS, SOX, MAS-TRM, NIST, and others).

3. The basis of the development and implementation of management decisions in order to increase the level of financial security is defined as effective information provision, which is the basis of a flexible and adequate response to changes in the environment of the functioning of economic entities. An algorithm for building effective information protection systems of financial institutions is proposed, which includes system vulnerability assessment, system assessment for compliance with security standards, penetration testing and application assessment. Its effectiveness will depend on the ability to adequately detect risks at each of the identified stages.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study and the results reported in this paper.

Funding

The study was conducted without financial support.

Data availability

All data are available in the main text of the manuscript.

References

1. Onyshchenko, S., Brychko, M., Litovtseva, V., Yevsieieva, A. (2022). Trust in the financial sector: a new approach to conceptualizing and measuring. Financial and Credit Activity Problems of Theory and Practice, 1 (42), 206–217. doi: https://doi.org/10.55643/fcaptp.1.42.2022.3735
2. Varnalii, Z., Bondarenko, S. (2023). Financial security of Ukrainian enterprises during the war and post-war period. University Economic Bulletin, 56, 106–113. doi: https://doi.org/10.31470/2306-546x-2023-56-106-113
3. Onyshchenko, V., Yehorycheva, S., Maslii, O., Yurkiv, N. (2021). Impact of Innovation and Digital Technologies on the Financial Security of the State. Proceedings of the 3rd International Conference on Building Innovations, 749–759. doi: https://doi.org/10.1007/978-3-030-85043-2_69
4. Varnalii, Z., Mekhed, A. (2022). Business entities` financial security under digital economy. Financial and Credit Activity Problems of Theory and Practice, 4 (45), 267–275. doi: https://doi.org/10.55643/fcaptp.4.45.2022.3813
5. Yusif, S., Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. Journal of Applied Security Research, 16 (4), 490–513. doi: https://doi.org/10.1080/19361610.2021.1918995
6. Hidouri, A., Hajlaoui, N., Touati, H., Hadded, M., Muhlethaler, P. (2022). A Survey on Security Attacks and Intrusion Detection Mechanisms in Named Data Networking. Computers, 11 (12), 186. doi: https://doi.org/10.3390/computers11120186
7. Slayton, R. (2020). Governing Uncertainty or Uncertain Governance? Information Security and the Challenge of Cutting Ties. Science, Technology, & Human Values, 46 (1), 81–111. doi: https://doi.org/10.1177/0162243919901159
8. Verhelst, A., Wouters, J. (2020). Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives. International Organisations Research Journal, 15 (2), 141–172. doi: https://doi.org/10.17323/1996-7845-2020-02-07
9. Amankwa, E., Loock, M., Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. Information & Computer Security, 26 (4), 420–436. doi: https://doi.org/10.1108/ics-09-2017-0063
10. Zubko, T., Hanechko, I., Trubei, O., Afanasyev, K. (2021). Determining the impact of digitalization on the economic security of trade. Eastern-European Journal of Enterprise Technologies, 6 (13 (114)), 60–71. doi: https://doi.org/10.15587/1729-4061.2021.248230
11. Kondratenko, N. O., Doroshenko, H. O., Ternova, I. A., Babych, S. N., Dorosheko, O. G. (2021). Organizational and methodical provision of the financial and economic security management of the enterprise. Financial and Credit Activity Problems of Theory and Practice, 1 (32), 129–137. doi: https://doi.org/10.18371/fcaptp.v1i32.200301
12. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., Skryl, V. (2023). The Mechanism of Information Security of the National Economy in Cyberspace. Proceedings of the 4th International Conference on Building Innovations, 791–803. doi: https://doi.org/10.1007/978-3-031-17385-1_67
13. Pro zatverdzhennia Metodychnykh rekomendatsiy shchodo rozrakhunku rivnia ekonomichnoi bezpeky Ukrainy: Nakaz Ministerstva ekonomichnoho rozvytku i torhivli Ukrainy vid 29.10.2013 No. 1277. Available at: http://search.ligazakon.ua/l_doc2.nsf/link1/ME131588.html
14. Pronoza, P., Kuzenko, T., Sablina, N. (2022). Implementation of strategic tools in the process of financial security management of industrial enterprises in Ukraine. Eastern-European Journal of Enterprise Technologies, 2 (13 (116)), 15–23. doi: https://doi.org/10.15587/1729-4061.2022.254234

15. Onyshchenko, S., Shchurov, I., Cherviak, A., Kivshyk, O. (2023). Methodical approach to assessing financial and credit institutions' economic security level. Financial and Credit Activity Problems of Theory and Practice, 2 (49), 65–78. doi: https://doi.org/10.55643/fcaptp.2.49.2023.4037
16. Stechyshyn, Y. (2023). The role and place of information and analytical support determination in the economic security system. Scientific Notes of «KROK» University, 1, 110–119. doi: https://doi.org/10.31732/2663-2209-2022-69-110-119
17. Khvalchyk, I. (2020). Summary of information-analytical safety management of enterprise. Economics: Time Realities, 1 (47), 84–90. doi: https://doi.org/10.15276/etr.01.2020.10
18. Onyshchenko, S., Bilko, S., Yanko, A., Sivitska, S. (2023). Business Information Security. Proceedings of the 4th International Conference on Building Innovations, 769–778. doi: https://doi.org/10.1007/978-3-031-17385-1_65
19. World Press Freedom Index 2021. Available at: https://rsf.org/en/index?year=2021
20. 2021 Social Progress Index. Executive Summary. Available at: https://www.socialprogress.org/static/9e62d-6c031f30344f34683259839760d/2021%20Social%20Progress%20Index%20Executive%20Summary-compressed_0.pdf
21. Onyshchenko, S., Skryl, V., Hlushko, A., Maslii, O. (2023). Inclusive Development Index. Proceedings of the 4th International Conference on Building Innovations, 779–790. doi: https://doi.org/10.1007/978-3-031-17385-1_66
22. UN E-Government Survey 2020. Available at: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020
23. Global Innovation Index 2021. Available at: https://www.wipo.int/global_innovation_index/en/2021/
24. Glushko, A. D. (2013). Directions of Efficiency Increase of State Regulatory Policy in Ukraine. World Applied Sciences Journal, 27 (4), 448–453. Available at: https://idosi.org/wasj/wasj27(4)13/6.pdf
25. Onyshchenko, S., Maslii, O., Kivshyk, O., Cherviak, A. (2023). the impact of the insurance market on the financial security of Ukraine. Financial and Credit Activity Problems of Theory and Practice, 1 (48), 268–281. doi: https://doi.org/10.55643/fcaptp.1.48.2023.3976
26. Onyshchenko, V., Onyshchenko, S., Verhal, K., Buriak, A. (2023). The Energy Efficiency of the Digital Economy. Proceedings of the 4th International Conference on Building Innovations, 761–767. doi: https://doi.org/10.1007/978-3-031-17385-1_64
27. Onyshchenko, V., Onyshchenko, S., Maslii, O., Maksymenko, A. (2023). Systematization of Threats to Financial Security of Individual, Society, Business and the State in Terms of the Pandemic. Proceedings of the 4th International Conference on Building Innovations, 749–760. doi: https://doi.org/10.1007/978-3-031-17385-1_63
28. Zhyvylo, Y., Shevchenko, D., Chernonog, O. (2021). Typology of cyber security systems in information and telecommunication systems of military (special) purpose. Modern Information Technologies in the Sphere of Security and Defence, 42 (3), 37–44. doi: https://doi.org/10.33099/2311-7249/2021-42-3-37-44
29. Glushko, A., Marchyshynets, O. (2018). Institutional provision of the state regulatory policy in Ukraine. Journal of Advanced Research in Law and Economics, 9 (3 (33)), 941–948. Available at: https://journals.aserspublishing.eu/jarle/article/view/2536
30. PCI DSS (Payment Card Industry Data Security Standard). Available at: https://platon.ua/faq/pci-dss
31. Information security, Cybersecurity and the IEC 62443 series of standards (2022). Available at: https://ikmj.com/en/information-security-cybersecurity-and-the-iec-62443-series-of-standards/
32. CIS Controls Implementation Guide for SMEs. Available at: https://www.cisecurity.org/wp-content/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf
33. International Organization for Standardization. Available at: https://www.iso.org/home.html
34. Svistun, L., Glushko, A., Shtepenko, K. (2018). Organizational Aspects of Development Projects Implementation at the Real Estate Market in Ukraine. International Journal of Engineering & Technology, 7 (3.2), 447. doi: https://doi.org/10.14419/ijet.v7i3.2.14569
35. CVE. Available at: https://cve.mitre.org/
36. CVSS. Available at: https://www.first.org/cvss/
37. Burp Suite. Available at: https://portswigger.net/burp/
38. Moral-García, S., Moral-Rubio, S., Fernández, E. B., Fernández-Medina, E. (2014). Enterprise security pattern: A model-driven architecture instance. Computer Standards & Interfaces, 36 (4), 748–758. doi: https://doi.org/10.1016/j.csi.2013.12.009
39. Wu, X., Zheng, W., Chen, X., Wang, F., Mu, D. (2020). CVE-assisted large-scale security bug report dataset construction method. Journal of Systems and Software, 160, 110456. doi: https://doi.org/10.1016/j.jss.2019.110456