CZU: 658.15:004.056.5 **https://doi.org/10.59295/sum2(11)2023_05**

INFORMATION COMPONENT OF ENSURING THE ENTERPRISE FINANCIAL SECURITY

Nadiia DAVYDENKO, Alina BURIAK,
The State Tax University, Irpin city, Kyiv region, Ukraine

In modern conditions, the information security of an enterprise is an important component of its financial security, since information is an integral part of the context of enterprise modernization with a view to competing in the market. Neglecting the processes of information risk management may cause the enterprise to lose intangible assets, which will lead to destabilization of financial security at the enterprise and the inability to maintain its own competitiveness in the future.

The aim of the article is to find approaches to prevent information risks, determine the algorithm of actions for diversifying information risks at different levels of information support, and develop a set of measures to protect the information system for the financial security of an enterprise.

The research is based on general scientific methods. In particular, the systematic approach was used to describe the essence of financial security as an economic category; methods of scientific abstraction and synthesis were used to determine the directions of the potential impact of information risks; and generalization was used to draw conclusions. The information base consists of the research papers of Ukrainian and international scholars.

The article studies information support of an enterprise. The measures to prevent information risks in the system of enterprise financial security are considered. The scheme of information support of enterprise financial security has been developed.

Keywords: *enterprise protection system, financial security, information risks.*

COMPONENTA INFORMAȚIONALĂ A ASIGURĂRII SECURITĂȚII FINANCIARE A ÎNTREPRINDERII

În condițiile moderne, securitatea informațională a unei întreprinderi este o componentă importantă a securității financiare a acesteia, deoarece informația este parte integrantă a contextului de modernizare a întreprinderii în vederea concurenței pe piață. Neglijarea proceselor de gestionare a riscurilor informaționale poate duce la pierderea de către întreprindere a activelor intangibile, ceea ce va duce la destabilizarea securității financiare a întreprinderii și la imposibilitatea de a-și menține propria competitivitate în viitor.

Scopul articolului este de a găsi abordări de prevenire a riscurilor informaționale, de a determina algoritmul acțiunilor de diversificare a riscurilor informaționale la diferite niveluri de suport informațional și de a elabora un set de măsuri de protecție a sistemului informațional pentru securitatea financiară a unei întreprinderi.

Cercetarea se bazează pe metode științifice generale. În special, abordarea sistematică a fost utilizată pentru a descrie esența securității financiare ca o categorie economică; metodele de abstractizare și sinteză științifică au fost utilizate pentru a determina direcțiile impactului potențial al riscurilor informaționale, iar generalizarea a fost utilizată pentru a trage concluzii. Baza informațională constă în lucrări de cercetare ale cercetătorilor ucraineni și internaționali.

Articolul studiază suportul informațional al unei întreprinderi. Sunt luate în considerare măsurile de prevenire a riscurilor informaționale în sistemul de securitate financiară a întreprinderii. A fost elaborată schema de susținere informațională a securității financiare a întreprinderii.

Cuvinte-cheie: *sistemul de protecție a întreprinderii, securitate financiară, riscurilor informaționale.*

Introduction

Financial relations are inherent in information, which is their integral part and objective attribute. Modern challenges set us the task of creating a system that would collect financial information in order to improve the financial performance of enterprises in the context of economic instability in Ukraine. It is important to take into account that information security of an enterprise has become a key component of its

financial security in the modern world, as information has become an integral part of the enterprise modernization process and the possibility of competing in the market. Neglect of information risk management can lead to the loss of intangible assets, which in turn can endanger the enterprise's financial stability and make it difficult to restore its competitiveness in the future.

The effectiveness of implementing measures to protect confidential and commercial information directly depends on the development and implementation of an enterprise information security policy, which is an integral part of financial security. The information component of financial security requires a new approach to business, and this topic is not only relevant but also requires additional in-depth research.

Materials and methods

The research is grounded on general scientific methods as a methodological basis. Specifically, the systemic approach is used to highlight the essence of financial security as an economic concept; methods of scientific abstraction and synthesis are used to determine the potential impact of information risks; and generalization is used to draw conclusions. At the same time, the information base is grounded on the research of Ukrainian and foreign scholars.

Results and discussions

The creation of an integrated management system for the information component of an enterprise's financial security is a key aspect of its long-term survival. Given the constant changes in the business environment, leadership must be able to make carefully considered management decisions and develop the skills to respond quickly to changes in themselves and their employees. This system helps an enterprise to adapt to the impact of both external and internal factors, which ensures its sustainability and competitiveness in the long run. Digitalization has transformed the way businesses operate and interact with their environment. This process has put new emphasis on the need to ensure the financial security of enterprises, which is becoming a key aspect for their survival and prosperity. At the same time, digital transformation creates opportunities to develop long-term strategic plans that should be well aligned with the tactics and strategy of the enterprise itself. Such planning takes into account the impact of digital technologies on business processes as well as helps companies maintain a competitive advantage in the changing business world. Therefore, it is no exaggeration to state that one of the most important elements of the entire system of ensuring the enterprise's financial security is information security. To understand the role of the information component, it is advisable to define the concepts of information and financial security.

We are deeply convinced that financial security is a system of strategic and tactical measures as well as instruments of financial support for balanced development by mobilizing financial resources to achieve sustainable expanded reproduction of business entities. The key elements of such a systemic concept are financial support for balanced development for sustainable expanded reproduction of enterprises, which, in turn, includes a mechanism for managing business activities.

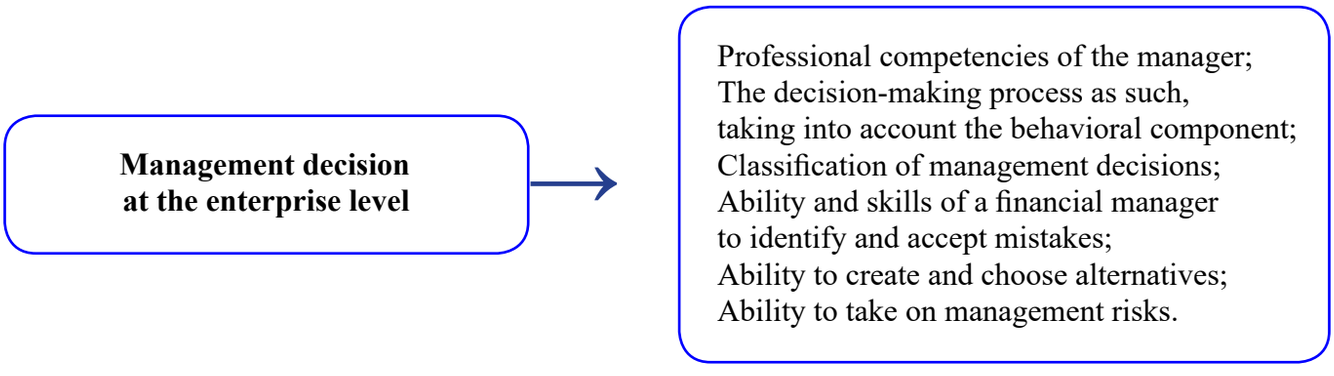
Enterprise information security is a set of measures, strategies and policies aimed at protecting and ensuring the reliability of information that is processed, stored and transmitted during the enterprise's operations. This information may be confidential, commercial, or technical, and its loss, damage, or unauthorized access can lead to serious financial, legal, and reputational problems for the enterprise.

Information security includes various aspects such as protection against computer attacks, cybercrime, protection against internal threats, ensuring compliance with confidentiality and data protection laws, and ensuring that employees are trained and aware of security rules. Information security has become extremely important in the modern world, where business information is one of the most valuable assets of an enterprise and where cyber threats are constantly growing. Information security is becoming a fundamental aspect of an enterprise's management strategy and helps ensure its long-term sustainability and success. It consists of up-to-date financial reports of the business entity and information on the enterprise's competitive position in the market, and should also include quantitative and qualitative values of financial security indicators, the presence of probable risks or threats, the established financial interests of the enterprise and the state of their implementation, a strategic plan for ensuring the financial security of the business entity,

parameters for the use of financial resources and sources of their income. It is on this basis that all studies of the enterprise's performance are conducted.

The field of strategic decisions in the context of information formation and development of an enterprise is quite multifaceted: the choice of activity areas, priorities for resource formation, ensuring effective long-term partnership, developing possible potential, and conducting a constant analysis of the strengths and weaknesses of the enterprise. In this regard, there are two levels of decision-making at the enterprise: individual and organizational [1]. If, in the first case, the financial manager is interested in the direct management process, in the second case, the interest shifts towards creating an appropriate environment around the information component management system (Fig. 1).

Fig. 1. Management decisions in the system of information component of enterprise financial security*.



**author's development*

Improving the effectiveness of an enterprise's financial performance by ensuring the completeness and reliability of financial information requires the implementation of measures that include adapting management structures to the requirements of international standards and reducing financial risks by ensuring the integrity and reliability of financial data.

Many of the risks faced by enterprises arise from a lack of information about potential changes that may occur or are already occurring in the macroeconomic environment. Underestimating these changes and their possible impact on the enterprise can lead to serious problems and even threaten its sustainability and success.

Enterprises should always be aware that macroeconomic conditions can change, and these changes can occur at various levels, including the global market, the national economy, and the regional business environment. Insufficient understanding of these changes and insufficient measures to manage them can create serious challenges for the enterprise.

Therefore, it is important that enterprises pay special attention to monitoring and analyzing macroeconomic trends and be prepared to make timely strategic decisions to adapt to changes. This may include advanced analytics, participation in global information exchange networks, and the development of action plans for various scenarios. Only such awareness and calculation will allow enterprises to reduce the risks associated with the unknown macroeconomic environment and ensure the sustainability of their business in it.

The main areas of a commercial enterprise's activities that are exposed to possible information risks include the following:

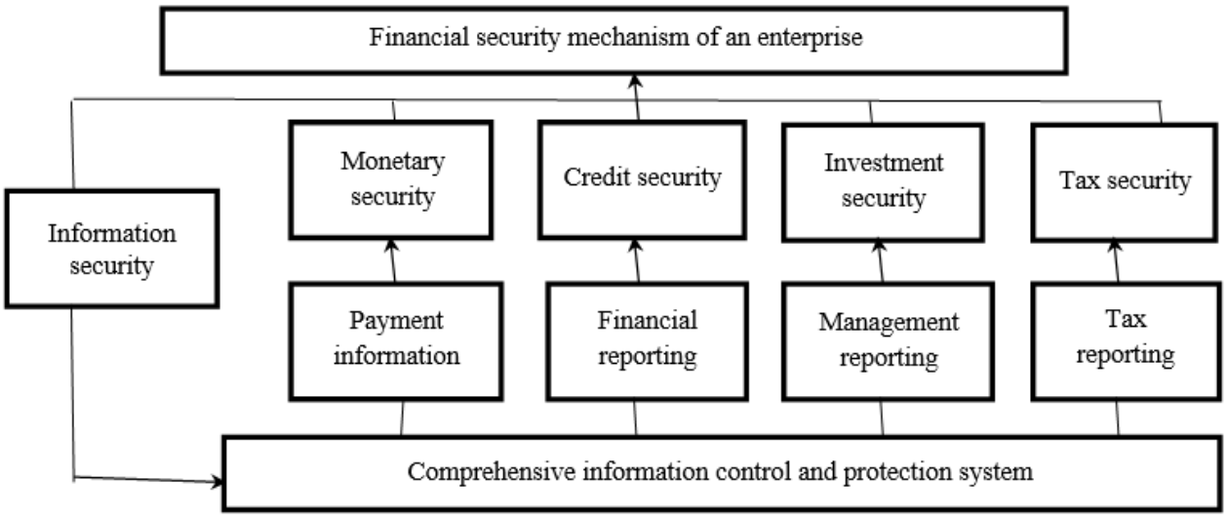
1. Electronic payment systems: this area is especially vulnerable, as unauthorized access to information held by employees of the enterprise or the servicing bank associated with such systems may create opportunities for manipulation of the enterprise's financial activities.
2. Systems for accessing the enterprise's trade secrets stored on electronic media.
3. Software that is used by the enterprise for its own operational processes and may have weaknesses.
4. Management and accounting information circulation systems and control of access to such systems by enterprise employees and third parties.

5. Control of the use of the enterprise's operational information by employees to prevent its inadmissible use for insider purposes.

These areas are of significant interest to stakeholders and require careful management and measures to ensure the enterprise's information security.

Information security is integrated with other components of financial security and contributes to the implementation of their functions through a complex system of control and protection of information used by other elements of financial security. The place of information security in the financial security mechanism of an enterprise is illustrated in Figure 2.

Fig. 2. The place of information security in the financial security mechanism of an enterprise [2].



In our opinion, a number of effective measures and strategies should be taken to prevent information risks at an enterprise:

Create an information security policy: Development of a clear policy that defines the rules, procedures and responsibilities for information security in the enterprise.

Employee education and training: Ensuring that all employees are informed and trained on information security, including password policies, threat awareness, and incident reporting procedures.

Network and infrastructure protection: Usage of software and hardware to protect the network, including firewalls, antiviruses, intrusion detection tools and data encryption.

Regular security audits: Conducting regular information security audits to identify potential problems and vulnerabilities in systems and processes.

Data backup and recovery: Ensuring that backup systems are available to back up data and allow for its recovery in the event of loss or damage.

Restriction of access: Establishing a „no more rights than necessary" principle to ensure access to information only for those who are authorized to do so.

Incident detection and response: Development of procedures and plans to detect and resolve information security incidents immediately.

Physical infrastructure protection: Ensuring the physical security of server rooms, communications equipment and other critical assets.

Continuous software updates and patching: Regularly updating operating systems, software and applications to close vulnerabilities and prevent intrusions.

Security monitoring and analysis: Continuously monitoring network activity and analyzing event logs to detect anomalies.

These measures will help reduce information security risks and provide reliable protection for enterprise data and infrastructure.

When studying the information support for the financial security of any enterprise, special attention

should be paid to the modern aspects of information security. The COVID-19 pandemic has had a significant impact on the operation of businesses around the world. Quarantine measures and restrictions have forced many companies to organize remote work for individual employees, departments or even the entire organization. This has caused major changes in the internal processing and exchange of information for internal use by the enterprise.

The pandemic has also led to unpredictable situations and rapidly changing working conditions. Businesses have faced challenges such as insufficient technical support and insufficient equipment for remote work. These complications, coupled with the large amount of work that was done online, created a fertile environment for the growth of cybercrime and cyberattacks.

Ensuring information security at this stage becomes an especially urgent task. Enterprises should strengthen their cyber defenses and consider adapting to the rapidly changing information environment. Regularly training staff on information security and improving protective measures such as antiviruses, firewalls and intrusion detection software can help reduce the risk of information attacks. It is also important to have incident response plans in place and to respond immediately to any threats to information security [3, 4].

In these unpredictable times of changing business conditions, information security is becoming a top priority to ensure the success of businesses and prevent cyber attacks.

The COVID-19 pandemic has been a key factor in the emergence of new challenges and threats to enterprise information security. The introduction of remote work for employees has led to a number of complex tasks being addressed simultaneously. These included ensuring reliable and fast internet connection, controlling staff working hours, arranging virtual meetings, separating personal and work responsibilities, and protecting information not only within the enterprise but also on employees' personal devices.

The criminals soon adapted to the new realities and started using mass distribution of email containing information about COVID-19, but including malicious files and links. It was recorded that the highest volume of such mailings was in the USA (38.4%), Germany (14.6%) and France (9.2%) [5]. The number of attacks on home routers also increased, and brute force attacks on various remote access services, such as RDP, SSH, and FTP, accounted for almost 90% [5].

More and more organizations are using platforms such as Zoom, Cisco Webex, Google Meet, Microsoft Skype and others for online meetings. However, this has also led to new types of attacks, such as Zoom Bombing and others, where unauthorized individuals join meetings and personal conversations.

Companies such as Microsoft and Zoom are actively working on cyber defense measures to protect information. But enterprise management also needs to actively develop and implement systems to protect information from external threats. Given the above-mentioned research on modern threats, managers should also pay attention to the digital literacy of their employees, as it is becoming increasingly important to ensure the security of information in the digital environment.

Conclusions

The results of this research demonstrate that enterprises do not always have a clear and systematic plan for the implementation of information technology, which would help them to effectively interact with a set of tools to ensure financial security.

This involves the important task of developing and implementing a unified methodology for analyzing the functional components of the financial security system. This approach will allow enterprises to better understand what information technologies and tools are needed to maintain their financial stability. It will also facilitate the creation of a unified mechanism for controlling and protecting information, which will ensure the synergy of all components of the enterprise's financial security and reduce the risks associated with the informatisation of activities.

The results of the theoretical and analytical studies conducted so far convincingly confirm that information support has become an integral part of the financial security of an enterprise. The current conditions in which enterprises of various industries operate are so dynamic and require prompt decisions that it is necessary to develop up-to-date information systems to ensure financial security.

However, cyberattacks and threats from criminals remain the main obstacles to the creation of an inte-

grated enterprise information system. According to research conducted by software vendors and the European Union Agency for Cybersecurity, information security violations have been identified in both large and medium-sized enterprises in various industries.

For enterprises, the annual costs of protecting information, ransoming databases from criminals, and restoring lost information and reputation are becoming a continuous source of losses. This necessitates further development of the area related to information support for financial security.

Given the rapid development of technology and the spread of access to public information, opportunities are being created for a more detailed analysis of the identified violations, in particular, online in various countries. This possibility of processing large amounts of data allows us to better understand the cyber insurance market, the impact of cyberattacks on stock prices, and calculations of the costs of ransoming stolen information (including encryption keys, etc.). This makes it possible to more accurately assess the losses caused by such incidents.

References:

1. MELIKHOVA, T. O. (2018). *Analysis of available methods for assessing the level of economic security of an enterprise for conducting modern diagnostics of its financial condition. Innovative economy*, 1 (73), pp. 223-226. Available at: http://inneco.org/index.php/innecoen/article/view/414
2. NOSOVA, Ye., MUHUIEV, K., & RUSINOV, V. (2021). *Informatsiina skladova u mekhanizmi finansovoi bezpeky pidpryiemstv*a [Information component in the mechanism of enterprise financial security]. *Zovnishnia torhivlia: ekonomika, finansy, pravo*, *3*, 98–107.
3. DAVYDENKO Nadiia, TITENKO Zoia (2022). *Current problems of financial security of enterprises. Proceedings of the International Scientific Conference „Global Challenges and Sustainable Development of Economics and Business”*, 2022. pp. 19-21. Batumi, Georgia. ISBN – 978-9941-488-62-67.
4. DAVYDENKO N. M., DAVYDENKO A. A. (2022). *Risks and threats to the financial security of enterprises. Stratehiia innovatsiinoho rozvytku ahrarnykh formuvan Ukrainy: analityko-prohnoznyi aspekt: zbirnyk tez dopovidei IV Mizhnarodnoi naukovo-praktychnoi konferentsii, 5-6 zhovtnia 2022 r.* [Strategy of innovative development of agrarian formations of Ukraine: analytical and forecasting aspect: collection of abstracts of the IV International Scientific and Practical Conference, 5-6 October 2022]. Kyiv: NUBiP Ukrainy, 194 p.
5. *The official site of company Positive Technologies (2021), „Cybersecurity threatscape: 2020”*. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (Accessed 10 June 2023).

Date abouth authors:
Nadiia DAVYDENKO, the State Tax University, Irpin city, Kyiv region, Ukraine.
E-mail: davidenk@ukr.net
ORCID: 0000-0001-7469-5536,

Alina BURIAK, the State Tax University, Irpin city, Kyiv region, Ukraine.
ORCID: 0000-0003-0886-317X

Presented on 20.11.2023