

DIGITALES ARCHIV

Zadorozhnyi, Zenovii-Mykhaylo; Muravskiy, Volodymyr; Shevchuk, Oleg et al.

Article

Innovative accounting methodology of ensuring the interaction of economic and cybersecurity of enterprises

Reference: Zadorozhnyi, Zenovii-Mykhaylo/Muravskiy, Volodymyr et. al. (2021). Innovative accounting methodology of ensuring the interaction of economic and cybersecurity of enterprises. In: Marketing i menedžment innovacij (4), S. 36 - 46.
https://mmi.fem.sumdu.edu.ua/sites/default/files/529-2021-03_Zadorozhnyi_0.pdf.
doi:10.21272/mmi.2021.4-03.

This Version is available at:
<http://hdl.handle.net/11159/6883>

Kontakt/Contact

ZBW – Leibniz-Informationszentrum Wirtschaft/Leibniz Information Centre for Economics
Düsternbrooker Weg 120
24105 Kiel (Germany)
E-Mail: [rights\[at\]zbw.eu](mailto:rights[at]zbw.eu)
<https://www.zbw.eu/econis-archiv/>

Standard-Nutzungsbedingungen:

Dieses Dokument darf zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden. Sie dürfen dieses Dokument nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen. Sofern für das Dokument eine Open-Content-Lizenz verwendet wurde, so gelten abweichend von diesen Nutzungsbedingungen die in der Lizenz gewährten Nutzungsrechte.

<https://zbw.eu/econis-archiv/termsfuse>

Terms of use:


This document may be saved and copied for your personal and scholarly purposes. You are not to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public. If the document is made available under a Creative Commons Licence you may exercise further usage rights as specified in the licence.

<https://doi.org/10.21272/mmi.2021.4-03>

JEL Classification: M10, M40, M41

Zenovii-Mykhaylo Zadorozhnyi,


D.Sc., Professor, West Ukrainian National University, Ukraine

 ORCID ID, 0000-0002-2857-8504

email: zadoroznuy.zenoviy@gmail.com

Volodymyr Muravskyi,


D.Sc., Associate Professor, West Ukrainian National University, Ukraine

 ORCID ID, 0000-0002-6423-9059

email: vavanm2@gmail.com

Oleg Shevchuk,


Ph.D., Associate Professor, West Ukrainian National University, Ukraine

 ORCID ID, 0000-0002-7352-7001

email: ikaf@ukr.net

Mykhailo Bryk,

Ph.D., Associate Professor, West Ukrainian National University, Ukraine

 ORCID ID, 0000-0002-0861-9057

email: bmm_09@i.ua

Correspondence author: vavanm2@gmail.com

INNOVATIVE ACCOUNTING METHODOLOGY OF ENSURING THE INTERACTION OF ECONOMIC AND CYBERSECURITY OF ENTERPRISES

Abstract. Implementation of computer communication technologies in social and economic processes has led to increased cyberattacks aimed to provide third parties with economic benefits or cause enterprises economic damages. The paper substantiates the impact of cyber risks on the economic security of enterprises, including the influence on the cybersecurity of accounting data as its important component. The aim of the article is to assert accounting as an innovative multilevel mechanism of ensuring the interaction of economic and cyber security. Theoretical and methodological aspects of positing accounting as a set of multi-option methods of implementing economic and cyber security interaction were investigated using institutional and innovational methods of scientific research. Economic and mathematical methods of analysis were used to substantiate the interdependence of global indices of state development. It is proven that the extent of digital competitiveness has the greatest influence on the frequency of cyber threats. At the same time, the development of information and communication technologies, innovativeness of the economy, connectivity, and Internet accessibility affect it to a lesser degree. Five levels of information interaction between economic and cyber security of enterprises are identified, viz: the methodological level: determined the impact of cyber threats on the principles and functions of accounting; the quality level: impact on the quality of accounting information; the methodical level: impact on accounting items and accounting types; the communication level: impact on accounting communication with stakeholders; the reputation level: impact on the business image and enterprise goodwill. If cyber threats are realized at these levels, this adds up to increasing economic losses for the enterprise. The paper argues for implementing a feedback mechanism for economic and cyber security conducted using accounting whose task is to credibly identify and evaluate economic losses arising due to cyber risks. It is proven that the methodology of identifying and evaluating economic losses arising in the enterprise due to cyber threats through accounting requires further scientific investigation.

Keywords: accounting, cybersecurity, economic security of enterprises, impact of cyber threats on economic security.

Introduction. The emergence of the digital economy, the growing number of global hybrid conflicts, social distancing, and remote operation of enterprises in a pandemic have led to increased cyber threats to economic systems at micro and macro levels. Since accounting is the main generator of economic

Cite as: Zadorozhnyi, Z.-M., Muravskyi, V., Shevchuk, O., & Bryk, M. (2021). Innovative Accounting Methodology of Ensuring the Interaction of Economic and Cybersecurity of Enterprises. *Marketing and Management of Innovations*, 4, 36-46. <http://doi.org/10.21272/mmi.2021.4-03>



information, accounting information requires foremost cybersecurity. Most cyber risks inherent to the activities of economic entities are associated with the theft of accounting information or the reduction of its quality parameters. The economic security of the enterprise is ensured by complying with the qualitative requirements for accounting information. The quality of information depends on its compliance with the expectations of stakeholders. Violation of any of the quality parameters of the accounting system could lead to loss of its usefulness and, consequently, economic significance for internal and external users. In most cases, the enterprise suffers economic losses if incorrect accounting information is in operation. Management decisions based on false (distorted or corrupted) accounting information cause damage to the economic security of the enterprise. The actions of internal users operating accounting information are related to the enterprise's economic activities, while the external users affect the functioning of other economic entities. Thus, non-compliance with the qualitative parameters of the accounting system causes economic damages twice: first, through direct losses due to the actions or inaction of managers (owners and founders) and, second, through indirect losses or lost economic benefits that could have been extracted from cooperation with external stakeholders. As a result, there is a direct link between the economic and cyber security of enterprises. In practice, the relationship between economic and security activities involves the study of accounting mechanisms to identify the impact of cyber threats on the economic security of the enterprise.

Literature Review. At the enterprise level, economic security characterizes the current level of protection of the enterprise's most important interests from unfair competition, excessive pressure from regulatory authorities, incompetent decisions, imperfect regulatory framework, and the ability of the enterprise to withstand information threats (Horbachenko, 2020). The impact of cyber risks on enterprise economic security is the subject of scientific research of many scholars. In particular, Rodrigues et al. (2019) argued that the need to ensure cybersecurity is a side effect of the digitalization of the economy. According to scientists, it is important to develop effective measures to prevent and eliminate cyber risks by predicting the economic consequences of cybersecurity breaches. B. Rajput (2020) considered the phenomenon of «cybercrime in the economic sector», which has arisen in recent years due to the connection between cyber risks and economic consequences of their manifestation. The scientist concluded that such crimes would continue to grow due to the increasing integration of economic and cyberspace. Exploring the economic consequences of various cyber risks, Shitova and Shitov (2019) pointed out that all modern cybercrime focuses on obtaining certain economic benefits such as global espionage, financial attacks, card fraud, information theft and phishing, network attacks and traffic interception to steal intellectual property, cryptographers and extortionists, cryptojacking, etc. Researchers have also investigated ways to ensure enterprise cybersecurity to minimize the economic losses of the enterprise. For example, Horbachenko (2020) substantiated the expediency of creating a single national cybersecurity system, which would unite the information space of enterprises into a single integrated system that would be a full-fledged component of national security at the state level. Marasigan (2019) highlighted the importance of instigating institutional changes in the economy at the micro and macro levels to overcome cyber barriers and threats to the operation of enterprises. Wilson (2014) identified the organizational, methodological, software, and hardware support as critically important for a cybersecurity system. It is crucial for ensuring the sustainable economic security of the enterprise. Rue and Pfleeger (2009) proposed different models of economic assessment of cyber risks. Scientists have explained the various mechanisms of cybersecurity's impact on the economic condition of the enterprise in terms of determining the economic losses resulting from the manifestation of cyber risks. Similarly, Patterson and Gergely (2020) developed a method for determining the economic efficiency of enterprise cybersecurity and its setup by analyzing the impact of cyber risks on the enterprise's economic losses or costs (capital and current).

Thus, most scientists associate the need for cybersecurity with the growing pervasiveness of information and communication technologies in information processes. However, the connection between

the intensification of cybersecurity and the increasing implementation of information processing technologies in social and economic processes was refuted by analyzing global rating data (Global Cybersecurity Index, 2018) (Fig. 1).

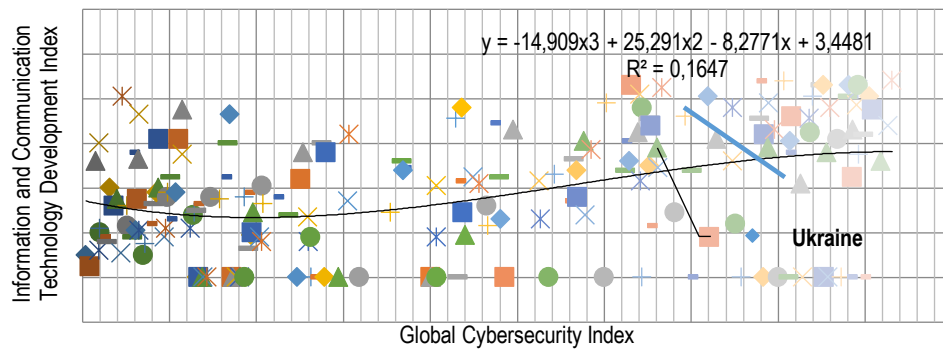


Figure 1. The relationship between the level of cybersecurity and ICT development of countries
Sources: developed by the authors based on (Global Cybersecurity Index, 2018).

The approximate and smoothed trend line built using data on the relationship between the ICT development index and the cybersecurity index makes it possible to identify an imbalance between these indicators for many countries. Significant positional deviation of the values from the average trend line shown in Fig. 1 shows the lack of a direct relationship between ICT development and the level of cybersecurity in most countries. A more homogeneous result was obtained when comparing the ratio of the cybersecurity index alternately with the innovation index (Fig. 2) and the connectivity index (Fig. 3).

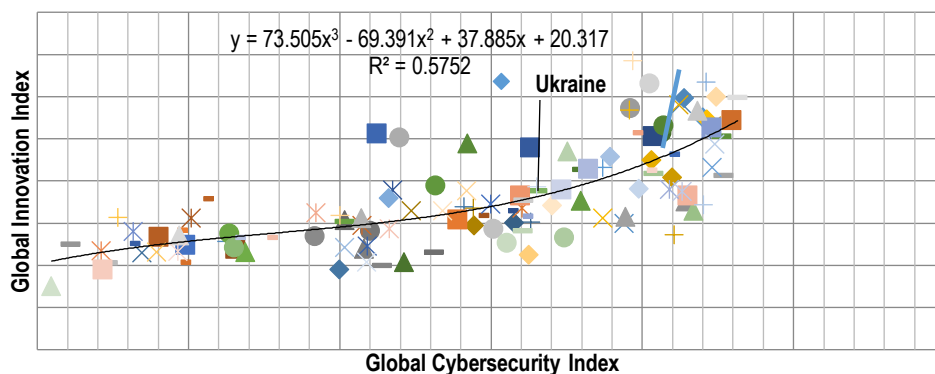


Figure 2. The relationship between the level of cybersecurity and the level of innovation of countries

Sources: developed by the authors based on (Global Innovation Index, 2018; Global Cybersecurity Index, 2018).

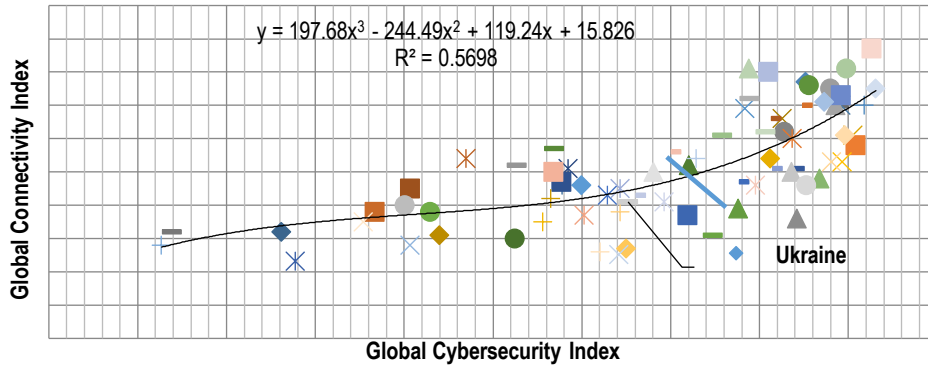


Figure 3. The relationship between the state of cybersecurity and connectivity of countries
 Source: calculated based on (Global Connectivity Index, 2018; Global Cybersecurity Index, 2018).

Thus, the increased attention to measures of ensuring cybersecurity is precipitated by innovations and connectivity at the micro and macro levels. The more innovations are introduced, and the more network infrastructure develops in national socio-economic processes, the bigger the need for an effective cybersecurity system. The level of innovation and development of network infrastructure determines the digital competitiveness of the country. Figure 4 shows a direct relationship between the level of cybersecurity and countries' digital competitiveness, as evidenced by only slight deviations of analytical data from the average trend line. It should be noted that some countries with low indicators of innovation and digitalization of socio-economic processes occupy high positions in the ranking of cybersecurity. For example, Ukraine's indicators for Innovation Index is 38.52; Connectivity index – 43; Digital Competitiveness Index – 51.29, all with a fairly high Cybersecurity Index of 0.661. Thus, it is explained by the need to combat ongoing cyber threats due to hybrid foreign influence.

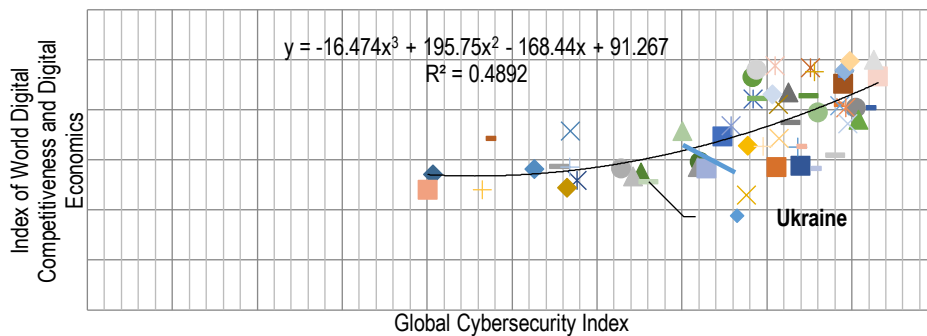


Figure 4. The relationship between the level of cybersecurity and the digital competitiveness of countries

Sources: developed by the authors based on (World Digital Competitiveness Ranking, 2018; Global Cybersecurity Index, 2018).

The digital competitiveness of countries is the basis for the development of a digital economy. When most socio-economic processes are digitized, their cybersecurity must be ensured. Accounting is the information basis for the digital economy. Accounting data becomes an important cybersecurity target in terms of the relationship with the national economic security, various industries, and individual economic

entities. Moroz and Tsal-Tsalko (2017) defined cybersecurity in terms of the accounting policy of the enterprise that ensures its economic security. They have defined it as protecting the enterprise's vital interests and accounting information from internal and external threats, i.e., protection of the enterprise, its human and intellectual potential, technologies, profits, added and market value. Remarkably, the above is provided by a system of special legal, economic, organizational, information, technical, and social measures. V. A. Nekhai and V. V. Nekhai (2017) considered information security an important component of economic security, which requires accounting information to be cybersecured for its quality parameters to be met. Yevdokymov (2011) overviewed reliability, the qualitative characteristic of accounting information, concerning ensuring the economic security of the enterprise. In his opinion, reliability is a characteristic of information that provides confidence in the appropriateness of its assumptions about errors and trends and the truth of intentions to provide all data in a veritable form; it meets the principles of verifiability, credibility, and neutrality. In addition, it should be noted that ensuring the reliability of accounting information in the digital economy involves the ability of accounting systems to avoid and resist cyber threats. However, such studies are partial and fragmentary, not allowing authors to establish the multifaceted nature of the connection between economic and cyber security of enterprises.

Therefore, the accounting mechanism of ensuring a multifaceted interaction between economic and cyber security has not been scientifically investigated appropriately, which determines this study's purpose. The article aims to assert accounting as an innovative multilevel mechanism for ensuring the interaction of economic and cybersecurity.

Methodology and research methods. The institutional approach was used to fulfill the established purpose of this paper in general. In contrast, the concept of institutional changes was used to evaluate the modernization of accounting through the introduction of information and communication technologies, particularly in detecting and eliminating cyber threats. Besides, this approach was used to reveal the accounting essence as a type of socio-economic activity and identify its multifaceted connections to the economic and cybersecurity of the enterprise in the institutional societal system.

Emphasis is placed on the use of economic and mathematical modeling. The polynomial trend line, built using approximated and smoothed data, reveals interdependencies in countries' rankings of ICT development, innovation, connectivity, digital capability, and cybersecurity. The identification of positional deviations of these indicators from the average trend line makes it possible to conclude the relationship between the level of cybersecurity of countries, the development of the digital space, and the country's economy. As the results of the rating of national cybersecurity are published biennially, all other statistical data use the indicators of 2018 to ensure comparability.

The idea of accounting's important socio-economic role and significance is at the core of the innovative approach to the theoretical and methodological principles of accounting. The hypothesis of the innovative accounting nature was posited as a set of methods to ensure the interaction of enterprises' economic and cyber security.

Results. Accounting principles are its fundamental basis. The study of accounting principles allows identifying empirical relationships, patterns of development, and accounting features, which are influenced by current trends in information and communication technologies development. It is possible to substantiate the interaction between enterprises' economic and cyber security by analyzing accounting principles. The increasing number and difficulty of cyber risks require continuous adaptation and transformation of accounting principles to internal and external conditions of an enterprise's operation. The increasing number and difficulty of cyber risks require continuous adaptation and transformation of accounting principles to internal and external conditions of an enterprise's operation. Thus, the ways of practically implementing (adhering to) them are optimized to ensure the enterprise's economic security. As a result, cyber risks exert direct and reverse influence on economic entities' financial and economic performance through accounting principles. Table 1 presents the peculiarities of adhering to fundamental

accounting principles in the conditions of simultaneously ensuring economic and cybersecurity, which is the first fundamental methodological level of their interaction.

Table 1. Adherence to the principles of accounting and financial reporting in terms of ensuring economic and cyber security

Principles of accounting and financial reporting	Manifested risks to economic and cyber security in case of non-compliance	Information consequences of cyber threats	Economic consequences of cyber threats
Transparency	Accounting information is distorted or substituted in its transfer process to internal and external users due to incomplete (unreliable) reflection of economic and financial operations in the system of accounts and reports. Enterprise loses information independence and autonomy due to unauthorized information system breaches by a third party for continuous monitoring of information processes in accounting and management.	Falsification of accounting data when transmitting to internal and external users	Enterprise employees or third parties obtaining economic benefits
Autonomy	Managerial decisions are ill-timed due to violation of the order of preparation and submission of data and implementation of accounting policies The financial and economic activity of the enterprise is blocked, suspended (disrupted); the enterprise is brought to bankruptcy.	Continuous unauthorized access to accounting data	Industrial espionage, reduced economic independence
Orderliness	Revenues are underreported or expenditures are overstated to avoid taxes, paying dividends, etc.	Ill-timed processing of accounting data	Violation of management timeliness
Continuity	Accounting data is distorted at the time of its initial recording by misrepresenting the nature of economic operations.	Blocking of information flows	Decrease in market value, raider capture, unfair competition
Accountability	Risks of electronic transactions are increased due to the substitution of fiat money with cryptocurrency outside national currency systems to ensure confidentiality of monetary operations.	Falsification of accounting data to avoid creditor obligations	Financial losses of economically connected stakeholders-creditors
Prevalence of essence over form		Falsification of accounting data at the time of its initial recording	Enterprise employees or third parties obtaining economic benefits
Single monetary unit		Hacker attacks to access electronic money services	Theft of funds

Sources: developed by the authors.

Adherence to the fundamental principles of accounting allows the enterprise to implement its functions to ensure the proper quality of accounting information. The quality of information produced by accounting depends on its ability to meet the requirements and expectations of internal and external users. Cyber

risks aim to reduce or negate the usefulness of accounting information due to non-compliance with its quality parameters. The proper quality of accounting information determines the quality of the interaction between economic and cyber security of enterprises. The main qualitative parameters of accounting data targeted by cyber risks are credibility, timeliness, availability, feasibility, reliability, comparability, and others. Regardless of the information subordination of qualitative parameters of accounting data or their grouping by various classification criteria, the economic security of the enterprise depends on the frequency of cyber threats. In particular, cyber risks focus on reducing the quality of accounting information through follows:

- credibility (making incorrect (erroneous) management decisions);
- timeliness (making belated management decisions);
- accessibility (inability to obtain or perceive information in the process of making management decisions);
- feasibility (blocking the necessary management decisions);
- reliability (inability to make management decisions due to lack of trust in information);
- comparability (making unreasonable management decisions due to inability to assess and analyze accounting indicators);
- other qualitative parameters of accounting data (damage to the enterprise management).

Thus, the manifestation of cyber risks is the reason for the reduced efficiency of the management system, which leads to the enterprise suffering economic damage. All qualitative parameters of accounting data are ultimately related to its confidentiality in ensuring the enterprise's economic and cyber security. Accounting data is nominally divided into public and confidential on the distinction between financial and managerial accounting. Identification of accounting items and their division into types determines the methodical level of the interaction between economic and cyber security of the enterprise.

Confidentiality of managerial accounting data is precipitated by the exclusively internal use and need to ensure that unauthorized persons do not access it. Lack of proper cybersecurity for managerial accounting data could lead to third parties using it to gain a competitive advantage in the market, attract buyers and suppliers on more favorable commercial terms, optimize the technological side of operations, revise personnel, pricing, sales policy, etc. Violation of confidentiality ultimately leads to economic losses for the enterprise. Economic damages caused by the manifestation of cyber risks are associated with losing operating profits due to loss of markets, suspension of operation, disruption of logistics cycles, disruptions to the rhythm of production, loss of intellectual property.

Additionally, the use of false internal accounting information may lead to erroneous management decisions. The higher level of management, the larger the potential economic losses from making incorrect management decisions. The greatest threat to the economic security of the enterprise may be posed by ineffective strategic management caused by the use of accounting data altered by cyber attacks.

The intensity and frequency of cyber threats also depend on the accounting item type. In particular, most cyberattacks are aimed at stealing money and its equivalents. Cyber threats are equally likely to manifest concerning the production and related calculations and manufacturing technologies (performance of works, provision of services) and fixed assets of the enterprise to damage critical infrastructure and suspend the enterprise operations, etc. However, accounting items such as inventories and small current assets are rarely cyber-threatened. Although financial accounting information is not a trade secret, it also requires effective cybersecurity. As the financial statements are officially disclosed, there is a risk of distortion or substitution of data. Stakeholders make management decisions on their financial interests and the operations of the economic entity based on reporting information. To discredit the company, its financial statements may be modified as a result of a cyber-attack. Malicious actions of third parties may cause economic damage to the company at the time of accounting data transfer or its storage location. Disclosure of false information about the entity's activities may result in the loss of the

economic interest of stakeholders. In particular, investors may suspend further investment in the issuer's financial instruments; financial institutions may refuse to lend; other creditors may demand early returns of accounts payable; contractors may refuse to cooperate, etc. As a result, an enterprise with distorted financial statements may suffer indirect financial damage that threatens economic security.

The level of communicative interaction between the enterprise's economic and cyber security is also connected with the communication with stakeholders. Cyberattacks at this level are aimed at blocking communications and transmitting false or incomplete accounting data to users. Stakeholders may consider such actions to be breaches of communication regulations or mistake the data altered by a cyber threat for authentic information. For example, cyber threats targeting the company's communications with fiscal institutions may lead to false accounting information reaching the recipient. If the accounting data recorded in the enterprise's books as the tax base for accrued taxes (fees) and the data sent to the tax authority differ, this may result in financial sanctions. The tax agent then suffers economic losses from fines for failure to report, late or incomplete information sent to the fiscal authority about financial and economic activities. In the absence of effective cybersecurity of communications with regulatory institutions, threats to the economic security of the enterprise increase due to repeated penalties for violating fiscal regulations.

Direct cyber risks threaten banking communications. If the attackers gain access to the electronic transaction accounting system, they could steal funds from the bank and electronic accounts. The extent of economic damage from the manifestation of such cyber risks could be reliably determined. Unauthorized access to the accounting system for non-cash payments threatens the economic security of the enterprise due to the possibility of losing all such funds. If the theft concerns electronic money or cryptocurrencies, it is impossible to search for attackers and recover lost funds. Effective preventive cybersecurity is crucial given the confidentiality and impersonality of electronic transactions, as combating already active cyber threats is difficult. Economic entities that use accounting and management outsourcing services are also vulnerable to significant economic losses. Active cyber threats could significantly modify accounting data in the process of communication from sender to outsourcer (Balaziuk et al., 2020). The outsourcing firm carries out further information processing based on the received distorted data, leading to them unwittingly creating false reports. The increased number of stages of accounting data processing, related to the transfer to the outsourcer, makes it very difficult to establish the reliability of accounting. Meanwhile, the repeated processing of newly credible accounting data after eliminating cyber threats requires additional costs and time. Cyber threats related to outsourcing also increase the likelihood of losing confidential information due to the need for continuous electronic communications, which could cause economic damage to the company. Thus, the number of delegated accounting functions simultaneously affects the enterprise's economic and cyber security.

Communication with audit firms may be subject to similar cyber threats. Suppose the auditor receives incomplete information about the financial and economic activities of the enterprise. In that case, they may choose to give a negative audit report or refuse to provide it at all. The use of such audit information may lead to a negative business reputation in the auditor's eyes or other recipients of audit reports. A blow to business reputation has a negative impact on the economic security of the enterprise.

Should all cyber risks become a reality, ultimately, the business image of the enterprise is ruined, which determines the reputation level of the interaction between economic and cyber security. Hackers may directly inflict damage on an enterprise's reputation to cause economic damage and suspend the operation of the economic entity, or indirectly while pursuing personal, in most cases financial, goals. In any case, the company subjected to cyberattacks loses the confidence of employees, contractors, investors, creditors, public and state institutions. PR losses inevitably make a dent in the economic security of the enterprise.

Oversight and fiscal institutions, social and environmental organizations may impose financial sanctions, block the enterprise's assets, or consider its activities illegal. Information interaction with such business entities is considered «toxic», which automatically hinders its financial and economic activities.

Accounting stakeholders, in such cases, lose economic interest in the economic entity, suspend cooperation, postpone the fulfillment of contractual obligations, etc. Herewith, it may cause insolvency, reduced liquidity, and wavering the financial stability of the enterprise. The damage to the business image of the enterprise inevitably leads to the loss of its market value. The company's securities are depreciated, the value of intangible assets decreases. Ultimately, the growing number and intensity of cyber threats reduce the company's goodwill. More details on the impact of the quality of accounting information and the use of computer and communication technologies on the goodwill of an economic entity are offered in the research of (Zadorozhnyi et al., 2018). The largest and most systematic cyberattacks could lead to a unique phenomenon – negative goodwill when the company's market value is lesser than the total fair value of its assets. Bankruptcy or reorganization of the enterprise is the final objective of cyber threats aiming to damage economic security. As a result, the reputation level covers all previous information levels of the interaction of economic and cybersecurity (Fig. 5).

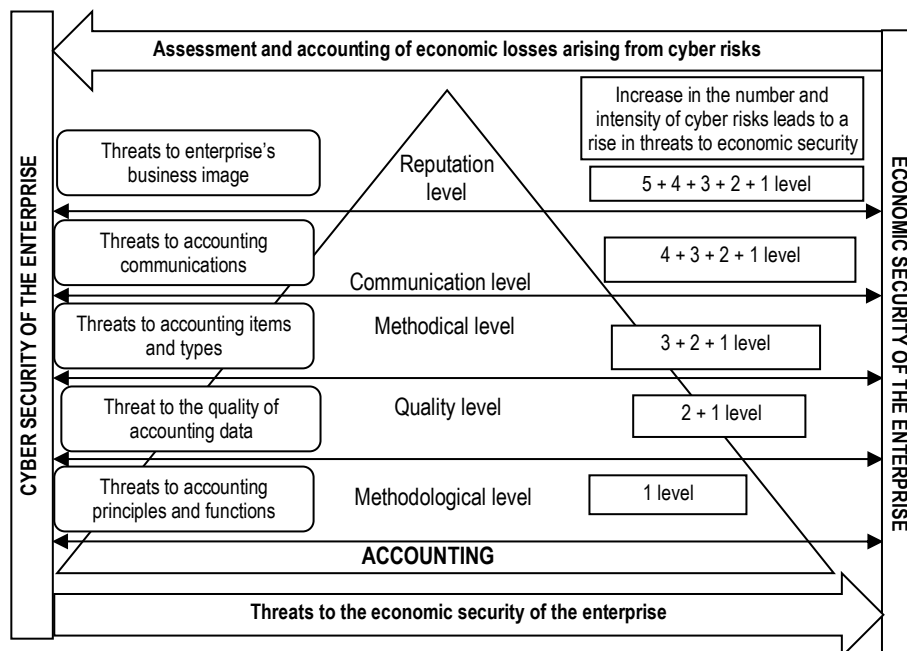


Figure 5. Innovative multilevel accounting methodology for the interaction of economic and cyber security of enterprises

Sources: developed by the authors.

Each subsequent interaction level of economic and cybersecurity of enterprises accumulatively covers the previous levels. The implementation of accounting techniques also shows the feedback between the enterprise's economic security and cyber security. With the help of accounting methods for analyzing economic processes, it is possible to identify and assess losses from the manifestation of cyber risks reliably. Economic losses from the growing number and intensity of cyber risks could differ significantly depending on the level of information interaction between economic and cyber security. The company incurs significant costs associated with the manifestation of cyber risks at the highest reputational level. These are difficult for accounting to identify and assess. Therefore, it requires further research.

Conclusions. Implementing computer and communication technologies in all socio-economic processes has led to the growing number and intensity of cyber threats to enterprise operations. The ultimate goal of cyber threats is to obtain economic benefits for third parties or cause economic damage to businesses. There is a direct relationship between cyber risks and the economic condition of the enterprise. Accounting should be considered an innovative mechanism of ensuring the interaction between the economic and cyber security of the enterprise. Accounting links are present at five accumulative levels and explain the impact of cyber risk activity on the increase in threats to the economic security of economic entities. At the methodological level, the cyber threats concern the principles and functions of accounting; at the quality level – the quality of accounting data; at the methodical level – accounting items and types; at the communication level – accounting communications with stakeholders; at the reputation level – business image of the enterprise, which leads to economic losses for the enterprise. At the same time, the accounting methods create the conditions for the feedback between economic and cyber security, which consists of reliable identification and assessment of economic losses from the manifestation of cyber risks. The largest losses, which are difficult to account for, are manifested at the highest reputation level, requiring further research to improve the accounting of the economic consequences of cyber risks.

Author Contributions: Z.-M.Z., M. M., O. S., M. B. contributed equally to the research development, the literature, data collection, research methodology, and concluding sections.

Funding: This research received no external funding.

References

- Balaziuk, O.Yu., Sysoieva, I.M., & Pilyavets, V.M. (2020). Control and accounting aspects of introducing agile methodology for software development projects. *Financial and credit activity: problems of theory and practice*, 3 (34), 94-102. [\[Google Scholar\]](#) [\[CrossRef\]](#)
- Global Connectivity Index. (2018). GCI Ranking Table. Retrieved from [\[Link\]](#)
- Global Cybersecurity Index. (2018). ITU Publications. Retrieved from [\[Link\]](#)
- Global Innovation Index. (2018). Retrieved from [\[Link\]](#)
- Horbachenko, S. (2020). Cyber security as a component of economic security of Ukraine. *Galician economic journal*, vol. 66, no 5, pp. 180-186. [\[CrossRef\]](#)
- Marasigan, R. (2019). The Role of Ideas that shape the Institutional Change in Cybersecurity: Economic barriers of cyber-attacks. Policy in a Changing World Tackling Global Issues At: Roppongi, Tokyo Japan. [\[CrossRef\]](#)
- Moroz, Yu. Yu., & Tsal-Tsalko, Yu. S. (2017). Accounting policy of the enterprise and its cybersecurity. *Accounting, analysis and control in the context of modern concepts of managing the economic potential and market value of the enterprise*. ZhNAEU. 4(1), 8–11. Retrieved from [\[Link\]](#)
- Nekhai, V. A., & Nekhai, V. V. (2017). Information security as a component of economic security of enterprises. *Scientific Bulletin of the International Humanities University*, 24(2), 137-140. [\[Google Scholar\]](#)
- Patterson, W., & Gergely, M. (2020). Economic Prospect Theory Applied to Cybersecurity. In *International Conference on Applied Human Factors and Ergonomics* (pp. 113-121). Springer, Cham. [\[Google Scholar\]](#) [\[CrossRef\]](#)
- Rajput, B. (2020). Exploring the Phenomenon of Cyber Economic Crime. *Cyber Economic Crime in India*, 53-78. [\[Google Scholar\]](#) [\[CrossRef\]](#)
- Rodrigues, B., Franco, M., Parangi, G., & Stiller, B. (2019). SEconomy: a framework for the economic assessment of cybersecurity. In *International Conference on the Economics of Grids, Clouds, Systems, and Services* (pp. 154-166). Springer, Cham. [\[Google Scholar\]](#) [\[CrossRef\]](#)
- Rue, R., & Pflieger, S. L. (2009). Making the best use of cybersecurity economic models. *IEEE Security & Privacy*, 7(4), 52-60. [\[Google Scholar\]](#) [\[CrossRef\]](#)
- Shitova, Y. Y., & Shitov, Y. A. (2019). Contemporary Trends in Economic Cybersecurity. *The world of new economy*, 13(4), 22-30. [\[Google Scholar\]](#) [\[CrossRef\]](#)
- Wilson, K. (2014). Cybersecurity Economics: How Much Cybersecurity is Enough?. *Australian intellectual property journal*, 7-9. [\[Link\]](#)
- World Digital Competitiveness Ranking IMD. (2018). Retrieved from [\[Link\]](#)
- Yevdokymov, V. V. (2011). Reliability of accounting information as a prerequisite for ensuring the economic security of the enterprise. *Herald of ZhSTU*, 3 (57), 46-50. [\[Google Scholar\]](#)

Zadorozhnyi, Z. V., Muravskiy, V. V., & Sudyn, Yu. A. (2018). Goodwill assessment in enterprise management: innovative approaches using computer and communication technologies. *Marketing and management of innovation*, 4, 43-53. [[Google Scholar](#)] [[CrossRef](#)]

Зеновій-Михайло Задорожний, д.е.н, професор, Західноукраїнський національний університет, Україна

Володимир Муравський, д. е. н. професор, Західноукраїнський національний університет, Україна

Олег Шевчук, к.е.н., доцент, Західноукраїнський національний університет, Україна

Михайло Брик, к.е.н., доцент Західноукраїнський національний університет, Україна

Інноваційна облікова методика забезпечення взаємозв'язку економічної та кібербезпеки підприємств

Імплементация компьютерно-коммуникационных технологий в социально-экономические процессы спрочинила активизацию кибератак, ориентованих на отримання економічної выгоды третьими лицами або заподіяння економічної шкоды підприємствам. У рамках роботи обгрунтовано вплив киберрисиков на економічну безпеку підприємств, важливою складовою якої є киберзащит облікової інформації. Мета статті полягає у позиціонування бухгалтерського обліку як інноваційного багаторівневого механізму забезпечення взаємовпливу економічної та кібербезпеки. Теоретичні й методичні аспекти позиціонування обліку як сукупності багатоваріантних методик реалізації взаємовпливу економічної та кібербезпеки досліджувалися із використанням загальних методів наукових досліджень – інституційного та інноваційного; для обгрунтування взаємозалежності глобальних індексів розвитку країн використано економіко-математичні методи аналізу. Доведено, що найбільший вплив на активизацию киберзагроз здійснює стан цифрової спроможності, дещо менший – рівень розвитку інформаційно-коммуникационных технологий, інноваційність економіки, мережева готовність та підключення до Інтернету. Визначено п'ять рівнів інформаційного взаємовпливу економічної та кібербезпеки підприємств: методологічний рівень – визначає вплив киберзагроз на принципи та функції обліку; якісний рівень – на якість облікової інформації; методичний рівень – на облікові об'єкти та види обліку; комунікаційний рівень – та облікові комунікації зі стейкхолдерами; репутаційний рівень – на діловий імідж та гудвіл підприємства. Встановлено, що реалізація киберризиков на зазначених рівнях адитивно призводить до зростання економічних втрат підприємств. Автори аргументували необхідність реалізації зворотного інформаційного зв'язку економічної та кібербезпеки за допомогою бухгалтерського обліку, завдання якого полягає в достовірній ідентифікації та оцінці економічних втрат від киберризиков. Напрямок подальших наукових досліджень є методика облікової ідентифікації та оцінки економічних втрат підприємств унаслідок прояву киберзагроз.

Ключові слова: облік, кібербезпека, економічна безпека підприємств, вплив киберзагроз на економічну безпеку.