© V. V. Muravskyi, V. Ya. Farion, A. V. Hrytsyshyn

Отримано: 07 листопада 2021 р.

Прорецензовано: 22 листопада 2021 р.

Прийнято до друку: 01 грудня 2021 р.

e-mail: vavanm2@gmail.com

DOI: 10.25264/2311-5149-2021-23(51)-103-109

Muravskyi V. V., Farion V. Ya, Hrytsyshyn A. V. Quality of accounting information and principles of its cyber protection. *Наукові записки Національного університету «Острозька академія». Серія «Економіка» : науковий журнал.* Острог : Вид-во НаУОА, грудень 2021. № 23(51). С. 103–109.

УДК: 657.8:004

JEL-класифікація: M41, M42, D24

ORCID-ідентифікатор: https://orcid.org/ 0000-0002-6423-9059

Volodymyr Muravskyi,
Doctor of Economics, Associate Professor, Professor of Accounting and Taxation Department,
West Ukrainian National University

Volodymyr Farion,
PhD, Associate Professor, Associate Professor of Accounting and Taxation Department,
West Ukrainian National University

Anna Hrytsyshyn,
PhD, Teacher of Accounting and Taxation Department,
West Ukrainian National University

QUALITY OF ACCOUNTING INFORMATION AND PRINCIPLES OF ITS CYBER PROTECTION

Activation of variable cyber risks in accounting requires the development of standardized effective means of their elimination. Ehe cyber protection to ensure the quality of accounting information accounting information, very important is observance of the unified principles of cybersecurity of enterprises. The purpose of the article lies in separation of the fundamental principles of cybersecurity of accounting information for the purposes of quality provision of information interests of stakeholders. It has been proved that the priority in the development of the latest computer and communication technologies and the manifestation of cyber threats is the qualitative characteristic of accounting information – its reliability. The reliability of records should be positioned as the absence of errors, distortions, inaccuracies caused by third parties, it guarantees availability and confidentiality. A list of fundamental principles of cybersecurity to ensure the quality of accounting information includes: confidentiality, integrity, accessibility, completeness, sanction, adressness, reliability and comparability. The principles of cybersecurity are the foundation in the development of guidelines for cybersecurity of enterprises while preventing, avoiding and eliminating the consequences of threats to the security of accounting information. With the further improvement of computer and communication technologies and the evolutionary complication of cyber threats to the functioning of enterprises, further scientifical researches concerning the fundamental principles of accounting information cybersecurity are needed.

Keywords: *accounting, cybersecurity, principles of cybersecurity, quality of accounting information.*

Муравський Володимир Васильович,
доктор економічних наук, доцент, професор кафедри обліку і оподаткування
Західноукраїнського національного університету

Фаріон Володимир Ярославович,
кандидат економічних наук, доцент, доцент кафедри обліку і оподаткування
Західноукраїнського національного університету

Грицишин Анна Володимирівна,
кандидат економічних наук, викладач кафедри обліку і оподаткування
Західноукраїнського національного університету

ЯКІСТЬ ОБЛІКОВОЇ ІНФОРМАЦІЇ ТА ПРИНЦИПИ ЇЇ КІБЕРЗАХИСТУ

Активізація варіативних кіберризиків в обліку потребує вироблення стандартизованих дієвих засобів їхнього усунення. Для забезпечення кіберзахисту облікової інформації важливим є дотримання уніфікованих принципів кібербезпеви підприємств. Доведено, що пріоритетною в умовах розвитку новітніх комп'ютерно-комунікаційних технологій і прояву кіберзагроз є якісна характеристика облікової інформації – її надійність. Надійність облікових даних слід позиціонувати як відсутність помилок, викривлень, неточностей, спричинених сторонніми особами, а також гарантує доступність та конфіденційність. Визначено перелік фундаментальних принципів кіберзахисту облікової інформації, до яких належать конфіденційність, цілісність, доступність, повнота, санкціонованість, адресність, достовірність і порівнюваність. Принципи кібербезпеки є фундаментом у виробленні методичних інструкцій з кіберзахисту підприємств для попередження, уникнення та усунення наслідків загроз безпеці та якості облікової інформації.

Ключові слова: *облік, кібербезпека, принципи кібербезпеки, якість облікової інформації.*

© V. V. Muravskyi, V. Ya. Farion, A. V. Hrytsyshyn
ISSN 2311-5149
ОБЛІК, АНАЛІЗ ТА АУДИТ

Муравский Владимир Васильевич,
доктор экономических наук, доцент, профессор кафедры учета и налогообложения Западноукраинского национального университета
Фарион Владимир Ярославович,
кандидат экономических наук, доцент, доцент кафедры учета и налогообложения Западноукраинского национального университета
Грицишин Анна Владимировна,
кандидат экономических наук, преподаватель кафедры учета и налогообложения Западноукраинского национального университета

КАЧЕСТВО УЧЕТНОЙ ИНФОРМАЦИИ И ПРИНЦИПЫ ЕЕ КИБЕРЗАЩИТЫ

Активизация вариативных киберрисков в учете требует выработки стандартизированных действенных средств для их устранения. Для обеспечения киберзащиты учетной информации важно соблюдение унифицированных принципов кибербезопасности предприятий. Доказано, что приоритетной в условиях развития новейших компьютерно-коммуникационных технологий и проявления киберугроз является качественная характеристика учетной информации – ее надежность. Надежность учетных данных следует позиционировать как отсутствие ошибок, искажений, неточностей, вызванных посторонними лицами, а также гарантирует доступность и конфиденциальность. Определен список фундаментальных принципов киберзащиты учетной информации, к которым относится: конфиденциальность, целостность, доступность, полнота, санкционированность, адресность, достоверность и сравнимость. Принципы кбербезопасности являются фундаментом в выработке методических инструкций по киберзащите предприятий для предупреждения, избегания и устранения последствий угроз безопасности и качества учетной информации.
Ключевые слова: *учет, кибербезопасность, принципы кибербезопасности, качество учетной информации.*

Introduction. In the information society and its economic dimension – digital economy, information is the main subject of work of business entities. Computer and communication technology, the use of which leads to cyber risks, is increasingly used as a means of work. Attackers are interested in information systems of enterprises to cause economic damage or getting gain. Information that contains commercial interest becomes mainly the object of cyber incidents.

The activities of attackers are also focused on distortion of accounting information. Due to submission of partial or incorrect records to stakeholders, it is possible to cause economic damage to both senders and recipients of information. On the basis of incorrect accounting information, ineffective management decisions are made. Similarly, obtaining untimely accounting information or blocking access to information resources leads to delayed management of enterprises.

Taking into account the variability of cyber risks,it is necessary to develop universal principles of of prevention, avoiding and eliminating the consequences of threats to the security of accounting information. Regardless of the type of cyberattack, it is important to focus on universal principles of prevention, avoidance and elimination of the consequences of threats to the security of accounting information. The principles are the basis for developing guidelines for cybersecurity of accounting information. The use of standardized rules of cyber security of enterprises provides effective and risk-free management of economic entities.

Analysis of recent research and publications. The principles of processing and preparation of accounting information are actively studied by scientists. Most of the authors position the quality of accounting information as a defining characteristic of information resources. However, the necessity for ensuring cybersecurity of enterprises, actualizes a slightly different approach to determining the fundamental field of accounting. In the first place in the study of the principles of preparation of accounting information the reliability as the ability to avoid and eliminate cyber threats are put forward. For example, V.V. Yevdokimov defines the principle of reliability along with availability and feasibility as a prerequisite for ensuring the economic security of enterprises [1]. Reliability as an important characteristic of functioning of information systems is considered by O. Saydjari in the context of the organization of an effective system of cyber security of enterprises [2]. Instead L. O. Kyrylieva, A. O. Postavny offer the principle of confidential accounting information as a basis for cybersecurity of enterprises [3], which is a somewhat limited view on cybersecurity.

Mariana Hentea defines the basic conceptual principles of cybersecurity in consisting of: risk, vulnerability, threat, attack, impact, consequences and control [4]. However, such scientific approach makes it possible to identify the conceptual concepts used in the cybersecurity of accounting information, but not the principles. Marc Dupuis and Karen Renaud discuss the ethical principles of cybersecurity related to overcoming the fear of cyber threats [5]. Paul Rosenzweig has developed ten principles of cybersecurity of information, which are mainly related to the active development of Internet technologies [6]. However, the given principles are outdated, based on the modern development of innovative computer and communication technologies, and theyneed to be clarified. Thus, Jinsil

Seo and others explained the impact of modern information processing technologies (including virtual reality technologies) on the transformation of the principles of cybersecurity of enterprises [7]. A similar view is given by Raj Badhwar on the need to revise conservative principles of cybersecurity in conditions of implementation of artificial intelligence technologies [8].

Quite a thorough study was conducted by S.F. Lehenchuk, I.M. Tsaruk and T.P. Nazarenko, who position "integrity", "confidentiality" and "accessibility" as the principles of cybersecurity of accounting information [9]. It is worth noting that the above list of principles is basic, but not complete, as it does not take into account the multifaceted nature of cyber threats to enterprises. In particular, Gurdip Kaur, Ziba Lashkari and Habibi Lashkari Arash complement the principles of cybersecurity, integrity, confidentiality and accessibility related to the principles of accountability and reliability [10]. The same principles, only in a different interpretation, are considered by Anne Kohnke and Dan Shoemaker [11].

The generalization of scientific developments makes it possible to stratify the basic principles of cyber protection of a specific type of information resources, which is the accounting information that determines the purpose of the study.

The purpose of the article is to highlight the fundamental principles of cybersecurity of accounting information for the purposes of quality assurance of information interests of stakeholders.

Results. The scientific positioning of commercial secrets in the activities of economic entities directly depends on the development of the market economy and institutional transformations of the society. For developing countries, the concepts of trade secrets and confidentiality of information are inherent. All indicators of financial and economic activity are classified as a secret under conditions of unfair competition, legal unregulation of economic processes, excessive state regulation of enterprises, etc. This encourages management to consider all the information that has nothing to do with the secret as an economic category [12, 13].

And vice versa, in economically developed countries, a part of confidential information that has commercial importance for an enterprise is a trade secret that requires establishment ofeffective cybersecurity. In this case, the accounting system is advisable to be considered from an institutional standpoint as an identifier and differentiator of information that is a trade secret. Through the separation of accounting on financial and management, the information that has a commercial interest for the management of an enterprise and requires limited accessis separated. Therefore, accounting in terms of its division into financial and management has an important mission to determine the list of trade secrets and ensure cyber protection of confidential accounting information.

Legislative consolidation of the division of accounting into financial (public accounting information) and management (limited accounting information) forms the primary legal field for separation of information containing trade secrets. However, the classification from the standpoint of cybersecurity is quite conditional, as financial accounting information can also be confidential. Primary accounting documents and accounts are in most cases common to different types of accounting. In addition, researches on the integration of accounting in conditions of automated processing of accounting information which eliminates some species differences are being conducted more and more actively.

Accounting information about economic, scientific and technical, financial, investment, marketing activity contains trade secrets. The use of accounting information ensures uninterrupted economic activity, obtaining positive financial results and achieving competitive advantages in the market. Getting this information to outsiders can lead to economic losses. In case of the use of accounting information that has lost confidentiality, possible non-compliance with financial and economic plans for tactical and strategic planning of enterprises may arise.

The detailed analytical accounting data can also be used by attackers for causing economic damage or in commercial purposes. When composing and compressing financial accounting data in the accounting registers, later – in the financial statements, the detailed requisites of business transactions are lost. However, the primary data in intermediate analytical tables and documents fully identify the facts of economic events and phenomena, and therefore require limited access. For example, information about suppliers and buyers, delivery dates, popularity of certain products (works, services), cost for innovation and technical development, the state of wear of equipment, etc. may be of interest to competitors.

Additional cyber threats may arise when accounting information reaches attackers during several reporting periods. With the use of the methods of dynamic analysis, it is possible to identify trends in the financial and economic activities of an enterprise. Based on a forecast of business entities development,the strategies for harming an enterprise that has lost confidential information are built.

At the same time, not all information can be recognized as a trade secret, regardless of the will of accounting and management staff. First of all, the constituent information that identifies business entities, their location, founders and owners, areas of economic activity is not subject to classificationas a secret. All types of financial statements, in accordance with the list established by the national legislation of countries or international associations, are

public. Similarly, data on the tax base, accrued taxes and fees, as well as debt repayment to fiscal institutions cannot be a commercial secret. Other activities of economic entities related to environmental, social and public interests may not be classified as a secret. The list of accounting information that is prohibited from restricting access may increase for public, financial, investment enterprises, as well as state-owned institutions.

To ensure the protection of confidential information, a company, represented by its management, as the main generator and owner of trade secrets, determines the list of confidential information. In addition, accounting and management professionals have the right to determine the list of persons who may own, deal with, use such information, regulate the rules of information processing and access to it, as well as establish other conditions for trade secrets [13].

Effective protection of commercial secrets involves accounting and control of access of persons to confidential information. It is advisable to fixa person, time, place and content of information that is positioned as a commercial secret. In case of loss of confidential accounting information, it is possible to identify a list of suspects, which determines the principle of sanctioning.

Sanctioning in the work with accounting information is controlled through the system of granting rights to transformational actions. That is, with the use of personalized logins and passwords, digital keys, identification of an employee granting of rights for processingrecords is carried out. Sanctioning of information processing is a guarantee for ensuring the integrity of the information model of enterprise operations. Violation of the principle of sanctioning in the processing of accounting information occurs as a result of theft, substitution, selection of means of identification of persons. Unlawful actions lead to unauthorized access to the recordsby third parties, which is not provided by the information regulations of an enterprise.

In order to bring individuals to justice for violating the confidentiality regime, it is necessary to conclude preliminary agreements on non-disclosure of information. Traditionally, a liability agreement is concluded with an employee, which specifies financial sanctions for security breaches, theft, damage to property or non-compliance with functional responsibilities. In case of a breach of contractual relationship regarding the loss of trade secrets, additional disciplinary, administrative and criminal liability of employees may arise.

Disciplinary measures include: reprimand, warning, reproof, transfer to another job, etc. [14]. Administrative liability includes sanctions in the form of fines for a violation, use, disclosure of commercial information in order to cause damage to the business reputation or property of an entrepreneur [15, 59]. Criminal liability is provided for illegal collection of information for the purpose of commercial espionage and for disclosure of commercial secrets, which leads to possible imprisonment and compensation of material and moral damages to the management of an enterprise [16].

Detection of the fact of loss of confidential information requires automatic write-off of the value of trade secrets from the accounts. The fact of cyber threats leads to a decrease in the value of intangible assets, as well as goodwill. It is important to take actions to overcome the effects of cyber threats, which requires a review of new tactics and strategies for an enterprise development. Loss of confidential information foresees informing all persons and entities involved in commercial secrets. It is also necessary to improve the organizational structure of an enterprise, including accounting and security departments. The identification of employees who have violated the security regime requires their prosecution. The speed of action determines the timeliness of ending the impact of cyber risks and minimizing their consequences. Monitoring of the security regime is carried out on the basis of control of access to accounting information, which determines the principle of availability in the cyber security of an enterprise.

Availability of accounting information is the ability of accounting professionals and stakeholders to access information at the right time. In conditions of full automation of processing of the accounting information the round-the-clock mode of maintenance of availability is necessary. Availability is realized through the provision of records from a variety of sources on different media. Through communication channels, records are transmitted between stages of their transformation and are displayed to stakeholders. Cyber threats are aimed at blocking access to recirds, which violates the principle of availability.

Quite often, the termination of access to accounting information is due to unintentional factors that have accidental character. For example, power disconnexion or electricity interruptions, Internet outages, hardware or software failures, imperfect business communications, temporary disability, or dismissal of employees responsible for processing records can disrupt availability. Blocking access to records can be the result of intentional actions by attackers. The result of cyberattacks on web resources, databases, communication channels or other types of software and hardware of enterprises is the inability of interested parties to obtain accounting information within a specified period of time.

The consequence of blocking access to accounting information is non-compliance with the time regime of its transmission to the next stage of processing or consumption. The timeliness of the information process is violated

and the cycles of accounting information processing are shifted. The time lag between the stages of collecting records and making management decisions can increase to critical values, at which the value of information for stakeholders is lost.

Blocking of information access has catastrophic consequencesespecially for management accounting, which leads to transformation of useful accounting information into absolutely irrelevant data sets. Such data is not useful for users, as it reflects events with a significant time lag. In other words, accounting information is not operational, which levels the benefits of using computer and communication technology.

The principle of **addressness** is connected with the availability of accounting information. Accounting information must be delivered to the place of its consumption in accordance with the time and content requirements. The addressness of accounting information reflects its intended purpose for reaching a specific recipient. Therefore, the direction of accounting data should be considered in conjunction with the classification of stakeholders. Financial accounting information is addressed mainly to external users, management accounting – to external users.

If information is sent to the wrong user, its value is lost. The user can get records that he does not need. Instead, records that are useful to him may be mistakenly addressed to another stakeholder. The purpose of cyberattacks for violatingaddressnessof accounting information is to create communication chaos, which ultimately leads to blocking of useful communications.

Ensuring availability of accounting information requires functioning of the accounting department in a continuous mode. Continuity should be implemented in relation to the following: the work of software and hardware of an enterprise, establishment of communication channels, prevention of power outages, functioning of the personnel of an enterprise, prevention and prompt elimination of consequences of cyberattacks, etc.

In case when it is impossible to block access to the records, cyberattacks focus on harming its integrity. The **integrity** of accounting information is the ability to provide interested parties with complete information in its original form without unauthorized changes. The accounting data that have passed all stages of processing in accordance with the established methodology, internal regulations and rules of the adopted accounting policy, job descriptions of accounting and management specialists are integral. Comprehensive accounting information most fully and accurately corresponds to the social and economic reality in which the company operates, after all processing procedures.

Integrity is directly related to the **completeness** of accounting information, which proves its compliance with the information requests of stakeholders. Complete accounting information is comparable to information needs of its users. Stakeholders can be satisfied only with complete accounting arrays, otherwise accounting information is incomplete. In other words, integrity is the evidence of the complete reliability of information at the time of consumption, which means absence of loss or unauthorized changes to some of its elements.

The reasons for violation of integrity of accounting information are accidental or intentional actions of interested parties. Accidental are mistakes in the work of accounting and management staff of an enterprise, violation of the algorithm or obsolescence of software and hardware, insufficient competence of persons in the process of processing and acquaintance with information are accidental. Intentional actions for violation of integrity of information of an enterprise system are results of cyberattacks by attackers. Third parties may intercept information messages in order to distort them, which will lead to misinformation of stakeholders. Violation of integrity of accounting data may also be the evidence of concealment of violations by personnel of an enterprise or manipulation of information to obtain economic benefits. In particular, based on distortion of financial accounting data, it is possible to attract investors, obtain loans, reduce dividend payments, optimize the accrual and payment of taxes in an illegal manner.

Failure in complying with the principle of integrity in the process of preparing management accounting information can lead to incorrect management. Due to the lack of completeness of accounting information, stakeholders may not have enough information to make management decisions. Management decisions have to be made in conditions of complete or partial uncertainty. Violation of integrity of management accounting information is also a cause of uncertainty among stakeholders about the reliability of the reports provided. To confirm the accuracy of accounting information, a company's management or stakeholders may attract audit services. The task of the audit in such conditions is to provide confidence in the accounting information and conduct a security audit to monitor the state of cyber security of an enterprise.

For audit control of cyber protection of accounting information it is necessary to ensure its verifiability. The ability to be verified (the principle of **verifiability**) determines the ability to verify the accuracy of accounting information from various sources. Information that is true is reliable. Accounting and cybersecurity professionals need to have ablity to compare accounting information from a variety of sources, regulatory and legaldocuments, actual social and economic events, etc.

The most complete list of means of ensuring integrity of accounting information wasprovided by S.F.Lehenchuk, T.P. Nazarenko and I.M. Tsaruk, among which effective measures are:

– formation and use of an adequate system of control of accounting data, which foresees independent means of checks and counterbalances;

– establishment of personal responsibility for accounting specialists for ensuring proper data control;

– development of a mechanism for identifying discrepancies between primary documents, accounts and reports, and the necessary conditions should be created for corrective actions if necessary;

– ensuring proper cyber protection of accounting and other information systems of an enterprise, which are used for the formation of accounting information;

– Improving the interface of accounting software in order to implement control functions that provide synchronization and coordination of accounting data in different subsystems;

– use of reliable, stable and secure communication channels for transmission of records [9].

The relationship of the fundamental principles of cybersecurity of accounting information is shown in Fig. 1.

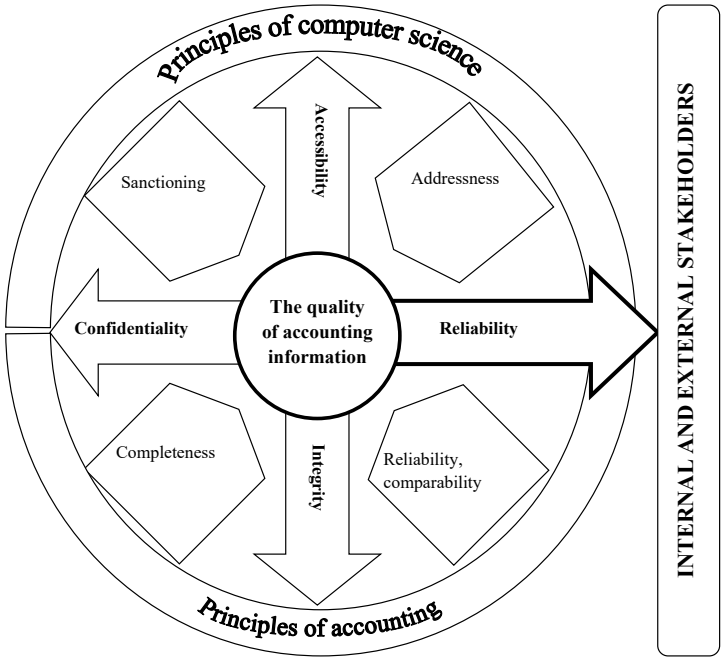

Fig. 1. Principles of cybersecurity of accounting information

Source: developed by the authors.

The principles of cybersecurity of accounting information are supplemented by other principles of fundamental scientific theories. On the outer radius of the conceptual combination of the basic principles of cybersecurity of accounting information (confidentiality, accessibility, integrity) are the theoretical principles of accounting and the principles of computer science. Adherence to all these principles of cybersecurity ensures the reliability of accounting information. Reliability is the property of information to be unmistakable, independent, unprejudiced, adequate to social and conomic realities. Reliability is a super principle in cybersecurity, which testifies the absence of errors, distortions, inaccuracies caused by third parties, it guarantees the availability and confidentiality of accounting informationas well as. Only reliable information can be used unconditionally by stakeholders. The principle of reliability is formed at the intersection of subject areas of other principles. Obtaining reliable accounting information is the ultimate goal of the combined operation of accounting and security systems. With the further development of computer and communication technologies and the evolutionary complexity of cyber threats, it is possible to supplement the fundamental principles of cyber security to ensure the reliability of accounting information.

Conclusions. Activization of variable cyber threats requires development of effective methods of cyber defense. In order to unify the means of cybersecurity of enterprises, it is necessary to focus on single fundamental principles of cybersecurity of accounting information. The main principle in the secured value of accounting information is its reliability. Reliability of accounting information indicates the absence of errors, distortions, inaccuracies caused by third parties, as well as it guarantees availability and confidentiality.

The principles of confidentiality, integrity and accessibility are connected with the reliability of records. Adherence to these principles ensures that high-quality accounting information reaches internal and external stakeholders without losing the company's trade secrets. The theoretical foundation of cybersecurity of accounting information is supplemented by the principles of completeness, sanction, adressness, reliability and comparability. These principles are the basis for the development of guidelines for cybersecurity of enterprises to prevent, avoid and eliminate the consequences of threats to the security of accounting information. Very important for obtaining reliable accounting information is adherenceof the theoretical principles of accounting and computer science. However, with the further improvement of computer and communication technologies and the evolutionary complication of cyber threats to the functioning of enterprises, it is possible to supplement the list of fundamental principles of cyber protection of accounting information.

References:

1. Yevdokymov, V. V. (2011). Nadiinist bukhhalterskoi informatsii yak peredumova zabezpechennia ekonomichnoi bezpeky pidpryiemstva [Reliability of accounting information as a prerequisite for ensuring the economic security of the enterprise]. Visnyk ZhDTU – Bulletin of ZhSTU. № 3 (57). 46-50. [in Ukrainian]

2. Saydjari, O. (2019). Engineering trustworthy systems: A principled approach to cybersecurity. Communications of the ACM. 62. 63-69. 10.1145/3282487. [in English]

3. Kyrylieva, L.O., Postavnyi, A.O. (2010). Orhanizatsiini aspekty obliku nou-khau ta komertsiinoi taiemnytsi v innovatsiinii systemi pidpryiemstva [Organizational aspects of accounting for know-how and trade secrets in the innovation system of the enterprise]. Ekonomichna stratehiia i perspektyvy rozvytku sfery torhivli ta posluh – Economic strategy and prospects for trade and services. 2. 123-130. [in Ukrainian]

4. Hentea, Mariana. (2021). Principles of Cybersecurity. Building an Effective Security Program for Distributed Energy Resources and Systems: Understanding Security for Smart Grid and Distributed Energy Resources and Systems, 93-127. 10.1002/9781119070740.ch3. [in English]

5. Dupuis, Marc & Renaud, Karen. (2020). Scoping the ethical principles of cybersecurity fear appeals. Ethics and Information Technology. 1-20. 10.1007/s10676-020-09560-0. [in English]

6. Rosenzweig, Paul. (2011). 10 Conservative Principles for Cybersecurity Policy. The Heritage Foundation for Leadership of America. 2513. URL: http://thf_media.s3.amazonaws.com/2011/pdf/bg2513.pdf. [in English]

7. Seo, Jinsil, Bruner, Michael, Payne, Austin, Gober, Nathan, McMullen, Donald & Chakravorty, Dhruva. (2019). Using Virtual Reality to Enforce Principles of Cybersecurity. The Journal of Computational Science Education. 10. 81-87. 10.22369/issn.2153-4136/10/1/13. [in English]

8. Badhwar, Raj. (2021). AI for Cybersecurity. The CISO's Next Frontier. 41-44. 10.1007/978-3-030-75354-2_4. [in English]

9. Lehenchuk, S. F., Tsaruk, I. M., & Nazarenko, T. P. (2021). Pryntsypy zakhystu danykh u systemi obliku: upravlinski aspekty [Principles of data protection in the accounting system: management aspects]. Ekonomika, upravlinnia ta administruvannia – Economics, management and administration, 2(96), 61–69. https://doi.org/10.26642/ema-2021-2(96)-61-69. [in Ukrainian]

10. Kaur, Gurdip, Lashkari, Ziba & Habibi Lashkari, Arash. (2021). Introduction to Cybersecurity. Understanding Cybersecurity Management in FinTech. 17-34. 10.1007/978-3-030-79915-1_2. [in English]

11. Kohnke, Anne, Shoemaker, Dan. (2015). Making Cybersecurity Effective: The Five Governing Principles for Implementing Practical IT Governance and Control. EDPACS. 52. 9-17. 10.1080/07366981.2015.1087799. [in English]

12. Aleksandrov, I.A, Polovian, O.V. (2000) Klasteryzatsiia terytorialnykh utvoren Ukrainy za rivnem ekonomichnoi bezpeky [Clustering of territorial formations of Ukraine by the level of economic security]. Ekonomichna kibernetyka – Economic Cybernetics. № 5-6. 40-47. [in Ukrainian]

13. Perevalova, L.V., Kvasha, S.V. (2011) Zakhyst konfidentsiinoi informatsii: problemy ta shliakhy vyrishennia [Protection of confidential information: problems and solutions]. Visnyk Natsionalnoho tekhnichnoho universytetu «Kharkivskyi politekhnichnyi instytut»: Tematychnyi vypusk: Aktualni problemy rozvytku ukrainskoho suspilstva – Visnyk Natsionalnoho tekhnichnoho universytetu «Kharkivskyi politekhnichnyi instytut»: Tematychnyi vypusk: Aktualni problemy rozvytku ukrainskoho suspilstva. № 30. 179 p. [in Ukrainian]

14. Syrotiuk, O. (2010). Pravo na komertsiinu taiemnytsiu [The right to trade secrets]. Balans – Balance. № 95. 57–59. [in Ukrainian]

15. Marchuk, U. (2012). Komertsiina taiemnytsia: pravova rehlamentatsiia, vidpovidalnist i zakhody shchodo yii zberezhennia [Trade secret: legal regulations, responsibilities and measures to preserve it]. Bukhhalterskyi oblik i audyt – Accounting and auditing. № 5. 49-54. [in Ukrainian]

16. Dykyi, A.P., Semenchuk, M.V. (2005). Komertsiina taiemnytsia yak skladova ekonomichnoi bezpeky pidpryiemstva [Trade secret as a component of economic security of the enterprise]. Visnyk Zhytomyrskoho derzhavnoho tekhnolohichnoho universytetu. Ekonomichni nauky – Bulletin of Zhytomyr State Technological University. Economic sciences. № 4 (34). 75-82. [in Ukrainian]