UDC 657.6:008

Zadorozhnyi Z.
Doctor of Economics, Professor,
Vice-Rector of Scientific Research Ternopil National Economic University, Ukraine;
e-mail: zadoroznuy.zenoviy@gmail.com; ORCID ID: 0000-0002-2857-8504
Muravskyi V.
Doctor of Economics, Associate Professor,
Professor at the Department of Accounting and Taxation,
Ternopil National Economic University, Ukraine;
e-mail: vavanm@gmail.com; ORCID ID: 0000-0002-6423-9059
Shevchuk O.
Doctor of Economics, Associate Professor,
Head of the Department for International Students,
Ternopil National Economic University, Ukraine;
e-mail: ikaf@ukr.net; ORCID ID: 0000-0002-7352-7001
Muravskyi V.
Lecturer at the Department of Economic Cybernetics,
Ternopil National Economic University, Ukraine;
e-mail: vasylmur@gmail.com; ORCID ID: 0000-0002-9625-9572

THE ACCOUNTING SYSTEM AS THE BASIS FOR ORGANISING ENTERPRISE CYBERSECURITY

Abstract. The increasing number of cyberattacks as part of the hybrid influence on social and economic processes and the threat of confidential information leaks dictate the need to ensure cybersecurity for enterprises, sectors and branches of the economy. Since most economic information is produced by the accounting system, its cybersecurity is a priority.

The review of literature on enterprise cybersecurity has indicated that the researchers increasingly define the accounting system as the target of cybersecurity measures. This approach is scientifically limited, as it does not consider that the accounting system may be the subject ensuring the cybersecurity of enterprises in the conditions of rapid development of latest computer and communication technologies. The aim of the article is to investigate the prospects of organising accounting when it is acting as the subject in a platform for ensuring the cybersecurity of enterprises.

It is substantiated that accounting should be used as the basis for ensuring cybersecurity, given that accounting is the main producer of economic information, much of the accounting information is confidential, modern accounting specialists are qualified in multiple different areas of expertise, numerous cyberattacks are perpetrated via accounting software, and the regulatory nature of accounting standards pertaining to information processes.

The prospects of reorganising the accounting department of enterprises and transforming the operational responsibilities of accounting specialists to focus on ensuring the cybersecurity of enterprises are explored. It is proposed to use the accounting policy of the enterprise and the internal regulations linked to it as the basis for the development of cybersecurity regulations. The necessity of introducing permanent security audit to accounting and control activities of the enterprise is proved. It proposed that internal controllers (accountants) or external specialists from audit firms monitor and test the cybersecurity system of enterprises that will facilitate efficient prevention, avoidance and elimination of information barriers and threats to the effective operation of economic entities.

Keywords: accounting, cybersecurity, security audit, information security, information risks and barriers, accounting policy.

Formulas: 0; fig.: 3; tabl.: 1; bibl.: 19.

Задорожний З.-М. В.
доктор економічних наук, професор, проректор з наукової роботи,
Тернопільський національний економічний університет, Україна;
e-mail: zadoroznuy.zenoviy@gmail.com; ORCID ID: 0000-0002-2857-8504
Муравський В. В.
доктор економічних наук, доцент, професор кафедри обліку і оподаткування,
Тернопільський національний економічний університет, Україна;
e-mail: vavanm@gmail.com; ORCID ID: 0000-0002-6423-9059
Шевчук О. А.
кандидат економічних наук, доцент,
начальник відділу роботи з іноземними студентами,
Тернопільський національний економічний університет, Україна;
e-mail: ikaf@ukr.net; ORCID ID: 0000-0002-7352-7001
Муравський В. В.
викладач кафедри економічної кібернетики,
Тернопільський національний економічний університет, Україна;
e-mail: vasylmur@gmail.com; ORCID ID: 0000-0002-9625-9572

ПОЗИЦІОНУВАННЯ СИСТЕМИ ОБЛІКУ ЯК БАЗИСУ В ОРГАНІЗАЦІЇ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВ

Анотація. Зростання активності кібератак як частина гібридного впливу на соціально-економічні процеси і загроза втрати конфіденційної інформації визначили потребу забезпечення кібербезпеки підприємств, секторів та галузей економіки. Оскільки більшість економічної інформації продукується системою бухгалтерського обліку, пріоритетним є її кіберзахист.

Аналіз літературних джерел із проблематики кіберзахисту підприємств засвідчив активізацію наукових досліджень у напрямі визначення системи бухгалтерського обліку як об'єкта забезпечення кібербезпеки. Такий підхід є науково обмеженим, оскільки не враховує суб'єктність бухгалтерського обліку в забезпеченні кібербезпеки підприємств в умовах розвитку новітніх комп'ютерно-комунікаційних технологій. Мета статті полягає в дослідженні перспектив організації бухгалтерського обліку з його суб'єктним позиціонуванням як платформи забезпечення кібербезпеки підприємства.

Обґрунтовано доцільність визнання системи бухгалтерського обліку на підприємстві як центру забезпечення кібербезпеки у зв'язку з: продукуючою природою бухгалтерського обліку як основного генератора економічної інформації; конфіденційністю значної частки облікової інформації; мультикваліфікованістю сучасних облікових фахівців із різних галузей знань; активністю кібератак через бухгалтерське програмне забезпечення; регламентувальною природою облікових нормативних документів щодо інформаційних процесів.

Досліджено перспективи реорганізації облікової служби підприємства і трансформації функціональних обов'язків фахівців з обліку з акцентом на організацію кіберзахисту підприємств. Запропоновано використовувати облікову політику підприємства і пов'язані з нею внутрішні регламенти за основу розроблення нормативного регламентування кібербезпеки. Доведено необхідність імплементації перманентного безпекового аудиту в обліково-контрольні процеси на підприємстві. Здійснення контролю і тестування системи кібербезпеки підприємств пропонуємо виконувати внутрішнім контролерам (обліковим працівникам) або зовнішнім фахівцям з аудиторських фірм, що сприятиме оперативному попередженню, уникненню та усуненню інформаційних бар'єрів і загроз ефективному функціонуванню суб'єктів господарювання.

Ключові слова: облік, кібербезпека, безпековий аудит, інформаційний захист, інформаційні ризики та бар'єри, облікова політика.

Формул: 0; рис.: 3; табл.: 1; бібл.: 19.

ISSN 2306-4994 (print); ISSN 2310-8770 (online)

Introduction. Ensuring the cybersecurity of economic systems is an important element of protection against the hybrid influence on state and non-state institutions. Cybersecurity of enterprises, sectors and industries entails information protection and prevention of organisational, technological, PR and investment losses. Given that the accounting system generates economic information, it is necessary to involve accounting specialists in the issues of enterprise cybersecurity. The accounting system as one of the enterprise management functions is a primary source of the information processes, therefore it takes priority in cyber protection.

At first, the need for ensuring cybersecurity was viewed as merely an element of information cycle of the enterprise in order to prevent losses in consumer value of accounting data, third parties accessing accounting data, or unauthorised employee use of information resources, etc. This purely informational approach to cybersecurity is partial and does not allow for the systematic provision of cyber security for businesses, industries or national economic systems.

The catalyst for comprehensive scientific applied research on the security of accounting data was the repeated cyber threat of international scope in the course of the hybrid wars. The scale and global nature of the cybersecurity issue determine the need to ensure the informational and economic security of countries. The European countries like Britain, France, Lithuania, Estonia and Spain have the highest level of cyber security. Due to the increased cyber influence that national information environments have been subjected to in the recent years, most European countries have made efforts to better their global cybersecurity ratings. In particular, Lithuania climbed 36 places in the rating, Serbia — 31, Slovenia — 35, Slovakia — 52 [1]. Ukraine is ranked 32nd among the countries of the European continent (globally — 54th), which is an unacceptable result compared to the other countries, although the rating did go up 4 spots in 2018 (*Tabl. 1*).

Table 1

European countries ranked by Cybersecurity Index

Country	Score	Regional Rank 2018	Global Rank 2018	Global Rank 2017	Dif. 2018/2017
United Kingdom	0.931	1	1	12	+11
France	0.918	2	3	8	+5
Lithuania	0.908	3	4	56	+52
Estonia	0.905	4	5	5	+0
Spain	0.896	5	7	19	+12
Norway	0.892	6	9	11	+2
Luxembourg	0.886	7	11	36	+25
Netherlands	0.885	8	12	15	+3
Georgia	0.857	9	18	8	-10
Finland	0.856	10	19	16	-3
….					
Poland	0.815	17	29	33	+4
…					
Moldova	0.662	31	53	72	+19
Ukraine	**0.661**	**32**	**54**	**58**	**+4**

Note: compiled by the author on the basis of data from [1].

Ukraine's advance in the global cybersecurity rating is explained by the increased attention to data protection at the micro-level. Most big businesses of national importance have opened vacancies or entire departments for employees whose operational responsibilities include ensuring cybersecurity. However, gradually all enterprises regardless of size or scope experienced the need to ensure the cybersecurity of economic operations because of the frequent hacks, commercial secrets theft, virus modules embedded in software allowing benefit through fraudulent means and so on.

Literature review and problem statement. Many scientists have researched the problems of accounting data security in conditions of active cyber threats at micro and macro levels. In particular, Yu. Moroz and Yu. Tsal-Tsalko formulated a comprehensive definition of

«cybersecurity» from the accounting point of view. They define it as the security from internal and external threats of the enterprise's vital interests, human and intellectual capital, trade secrets, proprietary technologies, profits, added and market value, information created by the accounting system and provided for by special legal, economic, organisational, informational and technical measures [2, p. 9]. S. Viter and I. Svitlyshyn determined the fundamental principles of measures for accounting data cybersecurity, namely: software support, protection of confidential information, personal responsibility, confidentiality, comprehensiveness, and control over access to accounting data [3, p. 501].

Most scientists attribute the need for cybersecurity at micro and macro levels to the increasing development of computer and communication technologies. Due to the digitalisation of socio-economic processes and the emergence of cyberspace, there have been more and more criminal acts aimed at causing harm and illegal financial gain. The need for more active cyber security as a result of increased level of information processing technologies in social and economic activities has been disproven by the latest global research [1].

The analysis of the relationship between ICT development and the level of cybersecurity allows us to conclude that there is an imbalance between these indicators in many countries. In other words, there is no direct dependence of the development of cybersecurity systems on the level of digitisation of socio-economic processes in the country. The frequency and types of cyber threats thus are given priority when justifying the urgency of bolstering the cybersecurity of a country. Therefore, the main factor driving the improvement of cybersecurity is not the level of digitisation of socio-economic activities, but rather the likelihood of information barriers and risks.

This position is properly argued in the research of Diane Janvrin and Tawei Wang who have traced the chronology of the concept «cybersecurity» and its development in accounting terms. The scientists have concluded that 2019, considering the high number of cyberattacks, was the turning point in the development of research on the security of accounting systems at enterprises [4, p. A2]. Elina Haapamäki and Jukka Sihvonen have confirmed that the research on accounting elements of cybersecurity of enterprises has intensified. They have noted a growing number of scientific papers dedicated to the security topics in 2008—2020, which is proportional to the number of cyberattacks [5, p. 810].

Nevertheless, the identification and classification of measures combatting information barriers and threats to the operation of the enterprise's accounting system remains the most discussed issue. For example, V. Shpak distinguishes four groups of such measures: legal, technical, software and organisational [6, p. 182—184]. S. Denga and Y. Veryga differentiate active and passive methods of minimising threats to accounting information systems. Active methods include prevention of computer fraud and sabotage, passive — reduction of errors by accounting specialists and breakdowns of accounting software and hardware [7, p. 62]. I. Grabchuk proposes methods of logical (ensuring informational security of the enterprise as a part of corporate culture) and physical security (data encryption and physical protection of hardware) [8, p. 23].

However, scientific and applied research that is more systemic is required to understand the economic aspect of information security. It entails determining the relationship between the types of cyber threats and methods of combatting them. In particular, Tim Eaton, Jonathan Grenier, and David Layman have substantiated the need for a correlation study on information barriers classification in accounting and the specific methods of risk management at the enterprise [9, p. C1]. Yu. Popivniak has also distinguished between organisational, personnel, technological and legal cyber threats and corresponding ways of eliminating them in the conditions of using new information technologies such as blockchain, cloud storage, etc. [10, p. 156]. The influence of blockchain technology on cybersecurity of the accounting system has been researched by Sebahattin Demirkan, Irem Demirkan and Andrew Mckee. Using the accounting system in the USA, the scientists predicted an increase of Big Data sets and substantiated the importance of structuring and managing them with blockchain technology in order to ensure information security [11, p. 189].

Framework of operational responsibilities of accounting personnel in the event of cyberattacks is an important direction of research that establishes the role of accounting in ensuring

ISSN 2306-4994 (print); ISSN 2310-8770 (online)

security. For instance, Laura Schaffner Georg, Hugh Grove, Anthony Holder and Mac Clouse have developed instructions for avoiding, overcoming and minimising the effects of the cyber impact on economic systems of the enterprise [12, p. 6]. Similarly V. Rozheliuk has outlined the measures aimed at minimising internal, accidental and external threats to cybersecurity. Whilst doing so, she defined cybersecurity of the enterprise as a set of actions carried out by accounting personnel with the purpose of archiving data, maintaining the professionalism level of accounting specialists, building an effective communication system between the enterprise and the stakeholders, creating optimal work conditions for accountants, and so on [13, p. 137].

John Pendley has justified the involvement of accounting specialists in the development of information technologies (software and hardware) dealing with cybersecurity. According to the scientist, effective operation of the cybersecurity system for economic processes is impossible without the participation of accounting and control specialists [14, p. 55]. Some researchers have concluded that tech specialists (system administrators, programmers, corporate architects, database administrators, etc.) are incapable of ensuring the system cybersecurity that emphasises the optimisation of economic operations at enterprises. Thomas Heaton Spitters has published a booklet dedicated solely to instructing accountants on how to act in the event of cyber threats. The scientific paper is one of the first attempts of systematically analyse the accounting aspect of security processes [15, p. 4].

Most scientific papers treat the accounting system as the object protected by the cybersecurity of the enterprise. This approach is scientifically limited, as it does not consider that the accounting system may be the subject ensuring the cybersecurity of enterprises in the conditions of rapid development of latest computer and communication technologies. It is recommended to associate the cybersecurity functions with the accounting system of the enterprise in order to optimize the information and security processes.

Ensuring cybersecurity involves not only protecting accounting data, but also making accounting the actor in the security processes. A hypothesis of scientific and applied research is proposed, according to which accounting is the basis for ensuring cybersecurity of enterprises and the integrator of methodological and organisational actions aimed at maintaining information and economic security of economic entities, branches and sectors of the economy. The necessity of using accounting as the basis for organising cybersecurity has determined the aim and the objectives of the scientific article to confirm the proposed scientific hypothesis.

The aim of the article is to investigate the peculiarities of organising the accounting system as the central subject ensuring the cybersecurity of enterprises.

Research results. The proposed hypothesis on viewing the accounting system as a platform for organising cybersecurity is supported by the empirical experience of enterprises that practise information security measures.

The underlying rationale for the scientific hypothesis determines that:

- the accounting system is the main producer of economic information, therefore the accounting processes should be prioritised in cybersecurity matters;
- much of the accounting information (excluding the data produced by financial accounting) contains trade secrets as it is used for the operational, tactical and strategic planning by the management;
- the latest hacker attacks and fraudulent schemes have been conducted through accounting and management software (*Pety. A* virus in the *M. E. Doc* program, power outages because of hacker attacks), which explains the importance of protecting the accounting system;
- modern accountants are multi-qualified professionals who combine economic, technical and legal knowledge and can perform cybersecurity functions at the enterprise;
- the regulatory framework for the accounting system defines most information processes at the enterprise and some regulations may contain guidelines on ensuring cybersecurity.

Expounding on the aforementioned hypothesis of developing the methodology and framework of accounting geared towards maintaining cybersecurity of the enterprise requires a complex of scientific and applied research and development. Organization of cybersecurity using

the accounting system as the basis entails the expansion of the operational responsibilities of the accounting and internal control departments or an addition of the cybersecurity specialist post to the enterprise's staff. The feasibility of organisational transformations must be justified by their economic effectiveness, regardless of the size and scope of the business. According to the Internet Security Threat Report, 80% of cybercrime targeted small businesses through mail services, social networks, and cloud services in 2019 [16]. The main reason cyberattacks centre on small-scale business is the lack of specialists and departments ensuring cyber security. Therefore, the likelihood that these cyberattacks will be successful on such businesses is higher. Specialists on accounting or control can successfully perform the cybersecurity functions at small enterprises.

Therefore, cybersecurity specialists should divided into 3 groups: specialists on information security (accounting staff), control department specialists (testing information systems on vulnerability to breaches, cybersecurity analysts, internal controllers, security auditors, inspectors on confidential information security), and technical support staff (system administrators, computer network administrators, programmers of specialised systems and web technology).

It would be prudent to instruct the employees of the first category in the course of the accounting specialists' professional training. The second group may consist of the accounting personnel who have practical experience in the field of cyber security and have acquired additional multidisciplinary skills and knowledge. Only the employees of the third group would be trained in the 'tech field' that does not envision obtaining in-depth knowledge of the economic disciplines, including accounting, analysis and control.

Thus, the operational responsibilities of accounting specialists of the first and the second group include: identifying vulnerabilities of the information systems and modelling the likely scenarios of cyber threats and risks related to them; verifying the reliability of security system operation, developing security measures in the event of unforeseen circumstances; classifying accounting information as restricted (commercial and trade secrets, other confidential information); developing regulations, policies and procedures in the framework of accounting information security; implementing developed security measures, testing the system in order to evaluate its effectiveness, and making adjustments as needed; assigning the necessary security details to the accounting computer system users; teaching the rules of continuous information processing to information system users; ensuring that information system users and company staff adhere to the rules of working with accounting information [3, p. 501].

It is important to regulate the operational responsibilities of cybersecurity in the employee handbook of accounting specialists and to define liability for violations of enterprise cybersecurity. Such responsibility may be not only administrative but also criminal, as the actions of accounting specialists may harm both the cyber security of a single enterprise and the national security of an entire sector of the economy.

Additionally it is recommended to recognize the responsibility for effective cyber security of the enterprise in the Ethics Code of Professional Accountants used in Ukraine. In particular, the meaning of confidentiality — one of the accounting services principles stipulating that accounting information must not be disclosed to third parties — should be expanded to include the definition of the accounting specialist as the organiser of data security. Security privileges should be documented in the employee handbook along with any changes to the accounting policy of the enterprise. The procedure for protecting accounting data must be outlined in the main the regulatory document of accounting — the accounting policy of the enterprise.

If the economic entity employs a significant number of employees, has a complex management structure and operates on a large scale, it is possible to create separate regulatory documents on ensuring cybersecurity so long as they maintain information compatibility and cohesion with the accounting policy of the enterprise. In that case, the accounting policy is the element integrating all internal regulations on ensuring cybersecurity. An internal legal framework of the organization and the methodology of cybersecurity may be formed through the system of accounting, together comprising the accounting policy of the enterprise (*Fig. 1*).

ISSN 2306-4994 (print); ISSN 2310-8770 (online)

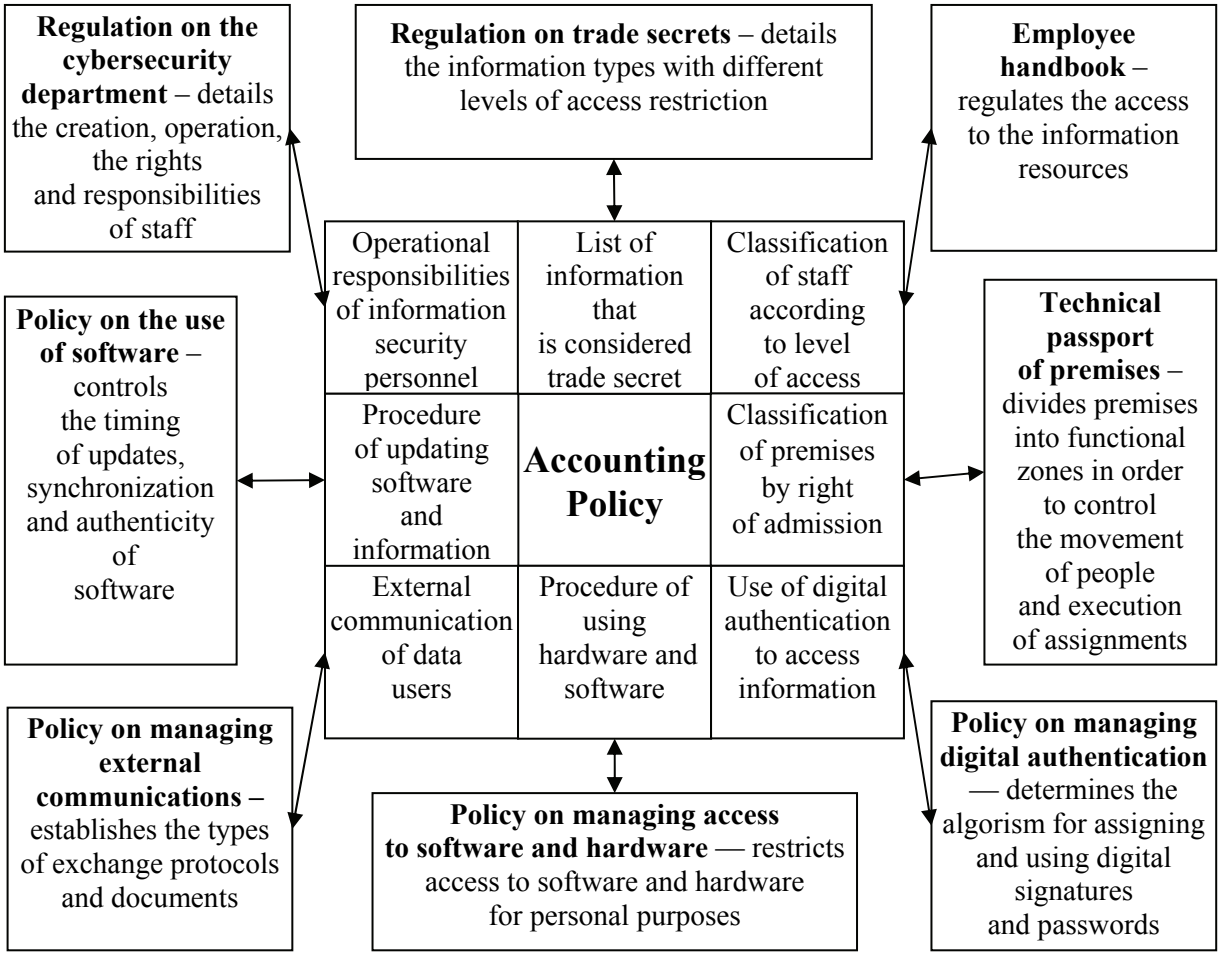

Fig. 1. **Security protocols documented in the enterprise accounting policy and internal regulations**

It is proposed to document several security protocols in the accounting policy and certain internal regulations of the enterprise. These include: the list of information that constitutes trade secret; the procedure of updating software and the methodology of cloud synchronisation of information; external communications done by the data users; procedures of using software and hardware; algorism of assigning and using digital authentication to access information; classification of premises by right of admission and organisation of enterprise sites; hierarchal classification of employees by level of access to information resources of the enterprise, and so on.

Combining all regulations on cybersecurity in the accounting policy will ensure that the enterprise operation goals, its accounting, analytical, control and management systems correspond to effective cyber security. Usefulness of any change in an accounting or management can be assessed by the influence it has on the cybersecurity of the enterprise — either strengthening or weakening it. The integrated document (set of documents) on regulating cybersecurity is the main guideline for conducting internal and external security audit. It is recommended to monitor the cybersecurity system continuously in order to evaluate the quality of information security at the enterprise. According to a study by Cyber Edge Group, it has been discovered that 78% of cyberattacks on enterprises employing cybersecurity specialists were successful (approximately 63% of all enterprises were subject to such threats) in 2019 [17, p. 12]. In other words, a cybersecurity system is not a guarantee that the enterprise will have comprehensive protection against all threats. The structure of cybersecurity system may have weaknesses the detection of which requires engaging the services of security audit.

Internal accounting specialists may be authorised to conduct continuous security audit, or this function may be outsourced to external independent auditor and consulting firms. The main task of security audit is to provide a comprehensive systemic evaluation of information risks that

should be used as the basis for ensuring the cybersecurity of enterprises since much of the accounting information is confidential, modern accounting specialists are qualified in multiple different areas of expertise, numerous cyberattacks are perpetrated via accounting software, and internal regulations document information processes. Effective cyber security requires the enterprise to review the operational responsibilities of accounting specialists so that they acquire additional skills and abilities, document their responsibilities in the employee handbooks, establishing liability for violating cyber security, and improve internal and external regulations that pertain to information and security processes.

The main regulation documenting the method of processing and protecting information is the accounting policy of the enterprise. The accounting policy or additional derivative internal regulations should determine the procedure for identifying trade secrets, managing access to information with digital authentication, using software and hardware in order to automate accounting and management, external communication with the stakeholders, and the security of physical and information networks of the enterprise. Additionally, the accounting policy should provide for the creation of the security audit service or the involvement of independent external auditors from consulting and auditing firms to monitor the cybersecurity of the enterprise. Conducting security audits helps to better prepare the management of the enterprise detect cyber threats by developing efficient ways to predict, prevent and eliminate them.

Prospects for further research and development. In terms of ensuring effective cybersecurity of enterprises, it is necessary to further research the models of interaction between internal and external audit services and the accounting department for the purposes of efficient distribution of accounting data and apprising the actual performers of the management decisions in order to react to active cyber threats rapidly.

Література

1. Global Cybersecurity Index (GCI) 2018 / International Telecommunication Union. Geneva : ITU Publications, 2019. 86 p.
2. Мороз Ю. Ю., Цаль-Цалко Ю. С. Облікова політика підприємства та її кібербезпека. *Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства* : зб. наук. пр. Житомир : ПП «Рута», 2017. Т. IV, Ч. І. С. 8—11.
3. Вітер С. А., Світлишин І. І. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство*. 2017. № 11. С. 497—502.
4. Janvrin D., Wang T. Implications of Cybersecurity on Accounting Information. *Journal of Information Systems*. 2019. Vol. 33. № 3. A1-A2.
5. Haapamäki E., Sihvonen J. Cybersecurity in accounting research. *Managerial Auditing Journal*. 2019. № 34. 808-834.
6. Шпак В. А. Організація захисту облікової інформації. *Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації*. 2015. № 2. С. 181—187.
7. Деньга С. М., Верига Ю. О. Захист інформації в комп'ютерних інформаційних системах бухгалтерського обліку. *Бухгалтерський облік і аудит*. 2004. № 5. С. 59—65.
8. Грабчук І. Л. Організація захисту облікової інформації в умовах гібридної війни. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу*. 2018. № 3 (41). С. 20—24.
9. Eaton T., Grenier J., Layman D. Accounting and Cybersecurity Risk Management. *Current Issues in Auditing*. 2019. Vol. 13. № 2.
10. Попівняк Ю. М. Кібербезпека та захист бухгалтерських даних в умовах застосування новітніх інформаційних технологій. *Бізнес Інформ*. 2019. № 8. С. 150—157.
11. Demirkan S., Demirkan I., Mckee A. Blockchain technology in the future of business cyber security. *Journal of Management Analytics*. 2020. Vol. 7. Is. 2. P. 189—208.
12. Georg Schaffner Laura, Grove Hugh, Holder Anthony, Clouse Mac. Cybersecurity Guidance for Accountants and Executives. *Internal Auditing*. 2018. Vol. 33. № 5. P. 5—20.
13. Рожелюк В. М. Заходи забезпечення захисту облікової інформації. *Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації.* 2013. № 2 (12). С. 335—340.
14. Pendley J. Finance and Accounting Professionals and Cybersecurity Awareness. *Journal of Corporate Accounting & Finance*. 2018. № 29. P. 53—58.
15. Spitters Thomas Heaton CPA. A Supplement to Cybersecurity Breviary for Accountants. Kindle Edition. San Francisco : Baume Verlag, 2019.
16. Symantec. *Internet Security Threat Report.* Mountain View : Symantec Corporation. 2019. February. Vol. 24.
17. 2019 Cyberthreat Defense Report. Annapolis : CyberEdge Group, 2019. 50 p.
18. Summary Report / Telstra Security Report 2019. Paddington : Telstra Corporation Limited, 2019. 19 p.
19. Risk committees. The Institute of Chartered Accountants in England and Wales. URL : https://www.icaew.com/technical/corporate-governance/committees/risk-committees.

Статтю рекомендовано до друку 31.08.2020

.

ISSN 2306-4994 (print); ISSN 2310-8770 (online)

References

1. Global Cybersecurity Index (GCI) 2018. (2019). International Telecommunication Union. Geneva: ITU Publications. 86 p.
2. Moroz, Yu. Yu. & Tsal-Tsalko, Yu. S. (2017). Oblikova polityka pidpryiemstva ta yii kiberbezpeka [Accounting policy of the enterprise and its cybersecurity]. *Oblik, analiz i kontrol v umovakh suchasnykh kontseptsii upravlinnia ekonomichnym potentsialom i rynkovoiu vartistiu pidpryiemstva — Accounting, analysis and control in the conditions of modern concepts of management of economic potential and market value of the enterprise, Vol. IV*, I, 8—11 [in Ukrainian].
3. Viter, S. A., & Svitlyshyn, I. I. (2017). Zakhyst oblikovoi informatsii ta kiberbezpeka pidpryiemstva [Protection of accounting information and cybersecurity of the enterprise]. *Ekonomika i suspilstvo: elektronne fakhove vydannia — Economy and society: electronic professional publication, 11*, 497—502 [in Ukrainian].
4. Janvrin, D., & Wang, T. (2019). Implications of Cybersecurity on Accounting Information. *Journal of Information Systems, Vol. 33*, 3. A1-A2. doi:10.2308/isys-10715.
5. Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal, 34*, 808—834. doi:10.1108/MAJ-09-2018-2004.
6. Shpak, V. A. (2015). Orhanizatsiia zakhystu oblikovoi informatsii [Organization of protection of accounting information]. *Bukhhalterskyi oblik, analiz ta audyt: problemy teorii, metodolohii, orhanizatsii — Accounting, analysis and audit: problems of theory, methodology, organization, 2,* 181—187 [in Ukrainian].
7. Denha, S. M., & Veryha, Yu. O. (2004). Zakhyst informatsii v kompiuternykh informatsiinykh systemakh bukhhalterskoho obliku [Information protection in computer information systems of accounting]. *Bukhhalterskyi oblik i audyt — Accounting and audit, 5*, 59—65 [in Ukrainian].
8. Hrabchuk, I. L. (2018). Orhanizatsiia zakhystu oblikovoi informatsii v umovakh hibrydnoi viiny [Organization of protection of accounting information in a hybrid war]. *Problemy teorii ta metodolohii bukhhalterskoho obliku, kontroliu i analizu — Problems of theory and methodology of accounting, control and analysis, 3* (41), 20—24. doi:10.26642/pbo-2018-3(41)-20-24 [in Ukrainian].
9. Eaton, T., Grenier, J., & Layman, D. (2019). Accounting and Cybersecurity Risk Management. *Current Issues in Auditing, Vol. 13*, 2. doi:10.2308/ciia-52419.
10. Popivniak, Yu. M. (2019). Kiberbezpeka ta zakhyst bukhhalterskykh danykh v umovakh zastosuvannia novitnikh informatsiinykh tekhnolohii [Cybersecurity and protection of accounting data in the application of the latest information technologies]. *Biznes Inform — Business Inform, 8,* 150–157. doi:10.32983/2222-4459-2019-8-150-157 [in Ukrainian].
11. Demirkan, S., Demirkan, I., & Mckee, A. (2020). Blockchain technology in the future of business cyber security. *Journal of Management Analytics, Vol. 7*, Is. 2. 189—208. doi:10.1080/23270012.2020.1731721.
12. Georg Schaffner Laura, Grove Hugh, Holder Anthony, & Clouse Mac. (2018). Cybersecurity Guidance for Accountants and Executives. *Internal Auditing, Vol. 33*, 5, 5—20.
13. Rozheliuk, V. M. (2013). Zakhody zabezpechennia zakhystu oblikovoi informatsii [Measures to ensure the protection of accounting information]. *Bukhhalterskyi oblik, analiz ta audyt: problemy teorii, metodolohii, orhanizatsii — Accounting, analysis and audit: problems of theory, methodology, organization, 2* (12), 335—340 [in Ukrainian].
14. Pendley, J. (2018). Finance and Accounting Professionals and Cybersecurity Awareness. *Journal of Corporate Accounting & Finance, 29*, 53—58. doi:10.1002/jcaf.22291.
15. Spitters Thomas Heaton CPA. (2019). A Supplement to Cybersecurity Breviary for Accountants Kindle Edition. San Francisco: Baume Verlag.
16. Symantec. (2019). *Internet Security Threat Report*. Mountain View: Symantec Corporation.
17. 2019 Cyberthreat Defense Report. (2019). Annapolis: CyberEdge Group.
18. Summary Report. (2019). Telstra Security Report 2019. Paddington: Telstra Corporation Limited. 19 p.
19. Risk committees. The Institute of Chartered Accountants in England and Wales. Retrieved from https://www.icaew.com/technical/corporate-governance/committees/risk-committees.

The article is recommended for printing 31.08.2020