UDC 657.6:008

JEL classification: M41, M42, D24

DOI: https://doi.org/10.35774/visnyk2022.01.097

Володимир МУРАВСЬКИЙ,
доктор економічних наук, доцент,
професор кафедри обліку і оподаткування,
Західноукраїнський національний університет,
вул. Львівська, 11, м. Тернопіль, 46020, Україна,
e-mail: vvvmur@gmail.com
ORCID ID: https://orcid.org/0000-0002-6423-9059

Олег ШЕВЧУК,
кандидат економічних наук, доцент,
начальник відділу по роботі з іноземними студентами,
Західноукраїнський національний університет,
вул. Львівська, 11, м. Тернопіль, 46020, Україна,
e-mail: ikaf@ukr.net
ORCID ID: http://orcid.org/0000-0002-7352-7001

Василь МУРАВСЬКИЙ,
викладач кафедри економічної кібернетики та інформатики,
Західноукраїнський національний університет,
вул. Львівська, 11, м. Тернопіль, 46020, Україна,
e-mail: vasylmur@gmail.com
ORCID ID: https://orcid.org/0000-0002-9625-9572

Віктор ЛАПШИНСЬКИЙ,
аспірант кафедри обліку і оподаткування,
Західноукраїнський національний університет,
вул. Львівська, 11, м. Тернопіль, 46020, Україна,
e-mail: viktorlapsinskij@gmail.com
ORCID ID: https://orcid.org/0000-0003-3938-0189

УДОСКОНАЛЕННЯ ОБЛІКОВОЇ ПОЛІТИКИ ПІДПРИЄМСТВА ДЛЯ ЗАБЕЗПЕЧЕННЯ ЙОГО КІБЕРЗАХИСТУ

Муравський В., Шевчук О., Муравський В., Лапшинський В. Удосконалення облікової політики підприємства для забезпечення його кіберзахисту. *Вісник Економіки*. 2022. Вип. 1. С. 97–109. DOI: https://doi.org/10.35774/visnyk2022.01.097

Muravskyi V., Shevchuk O. Muravskyi V., Lapsinskyi V. Udoskonalennia oblikovoi polityky pidpryiemstva dlia zabezpechennia yoho kiberzakhystu [Improving the accounting

policy of the enterprise for its cyber protection]. *Visnyk ekonomiky – Herald of Economics,* 2022, 1, 97–109. DOI: https://doi.org/10.35774/visnyk2022.01.097

Вступ. *Облікова політика підприємства – це основний документ, що регламентує порядок обробки облікової інформації та формування звітності. В умовах гібридних загроз, пандемічних очікувань суспільства, глобальних економічних викликів зростає важливість кіберзахисту інформації. Тому в обліковій політиці та внутрішніх регламентних документах доцільно відображати методику інформаційного захисту в умовах автоматизації обліку та управління.*

Мета статті *полягає в дослідженні перспектив організації кіберзахисту підприємства через регламентацію дій персоналу в обліковій політиці та інших внутрішніх розпорядчих документах.*

Методи. *У процесі дослідження безпекових регламентів в обліковій політиці використані загальнонаукові емпіричні, логічні та історичні методичні прийоми пізнання дійсності. Дослідження базуються на основі загальних методів вивчення економічних процесів, фактів та явищ з позиції бухгалтерського обліку та кібербезпеки підприємств. Інформаційною базою дослідження є нормативно-правові документи щодо регламентації бухгалтерського обліку, наукові праці вітчизняних та зарубіжних учених у частині кіберзахисту підприємства тощо.*

Результати. *Розроблено безпекові положення у складі облікової політики для регламентації обробки облікових даних щодо: визначення комерційної таємниці підприємства; порядку оновлення програмного забезпечення та методики інформаційної синхронізації з хмарними сервісами; здійснення зовнішніх комунікацій з користувачами інформації; порядку використання програмного і технічного забезпечення; алгоритму розподілу та застосування електронних ключів для доступу до інформації; класифікації приміщень за правом допуску та організації системи охорони території підприємства. Запропоновано порядок відображення в обліковій політиці підприємства часових критеріїв проведення перевірок стану інформаційного захисту, протоколів обміну даних, обмінних типів документів, сертифікатів і ліцензій на використання програмного забезпечення, що сприятиме гарантуванню безпеки облікової інформації у процесі виконання обов'язків обліковими та управлінськими фахівцями.*

Перспективи. *Ґрунтовних досліджень потребує методика визначення комерційної таємниці підприємства та розподілу облікової інформації за критерієм конфіденційності.*

Ключові слова: *облік, облікова політика, автоматизація обліку, кіберзахист, кібербезпека.*

Формули: 0; рис.: 2; табл.: 0; бібл.: 15.

Volodymyr MURAVSKYI,
D.Sc (Economics), Associate Professor
Professor of the Department of Accounting and Taxation,
West Ukrainian National University,
11 Lvivska st., Ternopil, 46020, Ukraine,

e-mail: vvvmur@gmail.com
ORCID ID: https://orcid.org/0000-0002-6423-9059

Oleg SHEVCHUK,
PhD, Associate Professor,
Head of the department for work with foreign students,
West Ukrainian National University,
11 Lvivska st., Ternopil, 46020, Ukraine,
e-mail: ikaf@ukr.net
ORCID ID: http://orcid.org/0000-0002-7352-7001

Vasyl MURAVSKYI,
Lecturer in the Department of Economic Cybernetics and Informatics,
West Ukrainian National University,
11 Lvivska st., Ternopil, 46020, Ukraine,
e-mail: vasylmur@gmail.com
ORCID ID: https://orcid.org/0000-0002-9625-9572

Viktor LAPSINSKYI,
Graduate student of the Department of Accounting and Taxation,
West Ukrainian National University,
11 Lvivska st., Ternopil, 46020, Ukraine,
e-mail: viktorlapsinskij@gmail.com
ORCID ID: https://orcid.org/0000-0003-3938-0189

IMPROVING THE ACCOUNTING POLICY OF THE ENTERPRISE FOR ITS CYBER PROTECTION

Introduction. *Accounting policy of a company is the main document that regulates the procedure of processing of accounting information and formation of reporting. In the conditions of hybrid threats, pandemic expectations of the society, global economic challenges, the importance of cybersecurity of information is growing. Therefore, in the accounting policy and internal regulations it is advisable to reflect the method of protection of information in terms of automation of accounting and management.*

The purpose of the article *lies in the research of the prospects of the organization of cyber security of an enterprise through the regulation of personnel actions in accounting policies and other internal administrative documents.*

Methods. *In the process of the research of security regulations in accounting policy the generally scientific empirical, logical and historical methodological methods of cognition of reality were used. The research is based on general methods of studying economic processes, facts and phenomena from the standpoint of accounting and cybersecurity of enterprises. The information basis of the research is normative-legal documents on accounting regulation, scientific works of domestic and foreign scientists in the part of cyber security of an enterprise, etc.*

Results. *Security provisions as part of the accounting policy have been developed to regulate: the algorithm for processing accounting data concerning determination of trade secrets of an enterprise; the procedure for updating software and methods of information synchronization with cloud services; implementation of external communications with users of information; the order of use of software and hardware; the algorithm of distribution and application of electronic keys for access to information; the classification of premises by the right of admission and organization of the system of information protection of the territory of an enterprise. The order of reflection of time criteria for carrying out checks of the condition of information protectionin the accounting policy of an enterprise, protocols of data exchange, exchange types of documents, certificates and licenses for use of software has been suggested.*

Perspectives. *The method for determining a trade secret of an enterprise and the distribution of accounting information according to the criterion of confidentiality requires thorough research.*

Keywords: *accounting, accounting policy, accounting automation, cyber protection, cybersecurity.*

Formulas: 0, fig.: 2, tabl.:0, bibl.: 15.

JEL classification: M41, M42, D24.

Introduction. The main regulatory document in the field of information circulation at the micro level is the accounting policy of an enterprise. It is one of the first regulations formed during the creation of any business entity, and a guide for accounting and management professionals in the implementation of accounting principles and reporting. The document on accounting policy is dominant in the regulatory and legal regulation of accounting, as it is referred to by other internal regulations.

The conditions of operating that arise from the organizational and legal form, industry, business size, etc. are indicated in the accounting policy. Important significance in the regulation of information processes has the reflection of the organizational structure of an enterprise, which directly affects the order of processing of accounting information and the formation of reporting indicators.

The accounting policy is used to providethe proof of illegal actions of the accounting and management personnel of an enterpriseby the controlling institutions. This regulatory document contains indefeasible instructions that define one of the variable methods and ways of processing accounting information. More and more companies regulate not only the methodology of financial accounting and related tax calculations, but also the peculiarities of management accounting. The accounting policy for management accounting will indicate the centers of responsibility and cost price centers, the methods for calculating and determining the cost of production, the order of formation of management reporting, etc. Therefore, with the complication of social and economic processes, the emergence of new objects of accounting, the digitalization of the economy, the need for improving accounting policies arise.

Literature Review. The level of innovation and development of network infrastructure determines the digital competitiveness of the country. Fig. 1 shows a direct relationship between the level of cybersecurity and digital competitiveness of countries, as evidenced

ISSN 2786-4537 (print). Вісник економіки № 1, 2022 р.
ISSN 2786-4545 (online). Herald of Ternopil National Economics № 1, 2022

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: Digital Competitiveness Index - 51.29 with a fairly high Cybersecurity Index of 0.661, which is explained by the need to combat ongoing cyber threats due to hybrid foreign influence [1, 2].

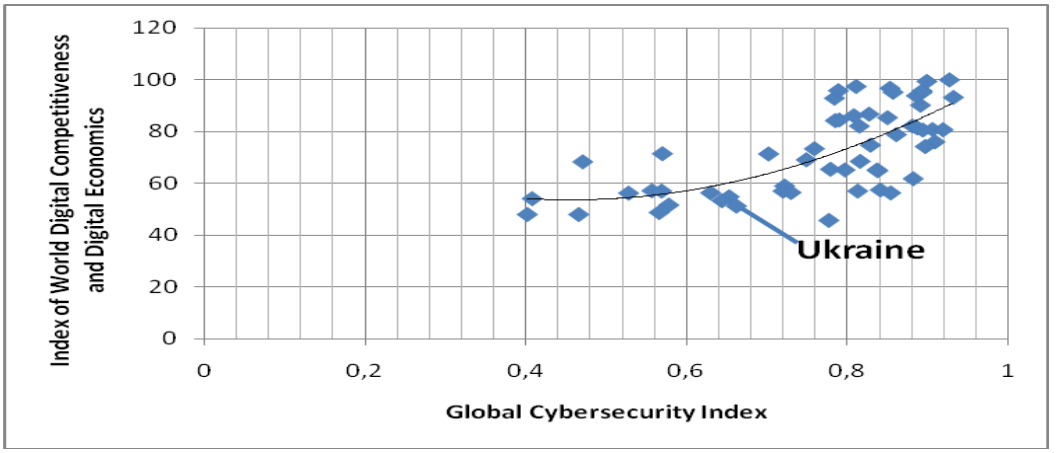

Fig. 1. The relationship between the level of cybersecurity and the digital competitiveness of countries

Source: calculated on the basis of (World Digital Competitiveness Ranking, 2018 [1]; Global Cybersecurity Index, 2018 [2])

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 target of cybersecurity in the terms of the relationship with the national economic security, various industries and individual economic entities. Further development of the institute of accounting regulation requires the expansion of the subject field of accounting policy. In the document on accounting policy of an enterprise it is expedient to foresee security aspects of processing of accounting information, formation and providing reports to stakeholders.

Yu.S. Tsal-Tsalko and Yu.Yu. Moroz define cybersecurity in the accounting system as the protection of the information system of an enterprise from internal and external threats, i.e. protection of an enterprise, its human and intellectual potential, information, technology, profit, added and market value of an enterprise, which is provided by a system of special actions of legal, economic, organizational, informational-technical and social character, influencing the formation of accounting policies [3, p. 9]. One of the first scientists who explained the influence of the information society and digital economy on the formation and implementation of accounting policy were M.S. Pushkar and M.T. Shchyrba [4].

The list of components of the accounting policy in terms of its objects, subjects, goals and tasks, levels of regulation has been provided in the scientific work of I. Herasymovych [5]. The study allows to form a comprehensive understanding of the accounting policy and its significance for the operation of an enterprise in terms of transformation and digitalization of social and economic processes. Sofiia Kafka proposed to subordinate informationally various internal regulations (graphs, documents circulation, accounting automation projects and job descriptions of accounting staff) to the company's accounting policy [6].

Salim Alibha et. all continued the study who substantiated the impact of accounting policies on errors in the processing of accounting information and formation of reports. In the authors' opinion, there exists a clear distinction between errors in information processing and changes in accounting principles or metods of valuation [7]. The need for expanding the provisions of the accounting policy (Accounting Policy 2.0) was explored by Kim Jihyun, based on the transformation of US law [8].

Steven Harrast also proposed a list of provisions for the robotization of production processes and full automation of information processes, which should be reflected in the accounting policy of an enterprise [9]. Olena Lagovska and Gabriella Loskorikh explained the difference in the formation of accounting policies of IT companies from other sectors of the economy [10]. The scientists have developed an accounting policy scheme for companies, whichoperate in the field of IT business. N. Drokina & Gulnara Kaipova determining the content of accounting policies, paid considerable attention to the provisions of automated accounting [11]. In the opinion of the scientists, the method of automated processing of accounting information should be reflected in the document on the accounting policy of an enterprise.

However, researchers focus their research on the software and hardware provisions of accounting policies for cybersecurity of an enterprise. However, the organizational aspects of cybersecurity remain beyond the attention of scientists, which determines the relevance of researches in the direction of security components of the accounting policy of an enterprise. As a result, in the accounting policy of an enterprise it is expedient to take into account security provisions for the organization of proper cyber protection of the information system of an enterprise. Security regulations are a set of requirements, rules, restrictions, procedures and responsibilities of personnel for processing and transmission of accounting information in order to achieve and maintain the state of maximum information and cybersecurity of an enterprise.

Purpose. The purpose of the article lies in the research of the prospects for the organization of cyber security of an enterprise through the regulation of personnel actions in accounting policies and other internal administrative documents.

Results. The information security of an enterprise directly depends on the effective accounting policy of an enterprise. Clear regulation in the accounting policy of accounting and management specialists for the collection, registration, processing and transmission of information significantly minimizes information threats. In the case of inadequate attention of the company's management to the communication links in the internal and external information environment, there are opportunities to manipulate registration information and steal it in order to cause damage to the company or to obtain illegal benefits. "Weak points" in the information integrity of an enterprise can be used by third parties for gaining access

ISSN 2786-4537 (print). Вісник економіки № 1, 2022 р.
ISSN 2786-4545 (online). Herald of Ternopil National Economics № 1, 2022

to trade secrets of an enterprise. Information security must be necessarily complex, it must take into account all communication channels and connections between the participants in the accounting process, forsee the implementation of legal, technical, software and organizational measures regulated by the accounting policy of an enterprise.

If the business entity is characterized by the presence of a significant number of employees, the complexity of the management structure, significant volumes of economic activity, a possible option for the formation of separate regulatory documents in cybersecurity with the implementation of information compatibility and unity with accounting policies. An accounting policy in this case can be an integrator of all internal cybersecurity regulations. Thanks to the accounting system, the internal legal field of organization and methods of cybersecurity can be formed, which together comprise the accounting policy of an enterprise [12].

The information scheme of safety provisions, which are fixed in the internal normative documents and accounting policy, is presented in Fig. 2.

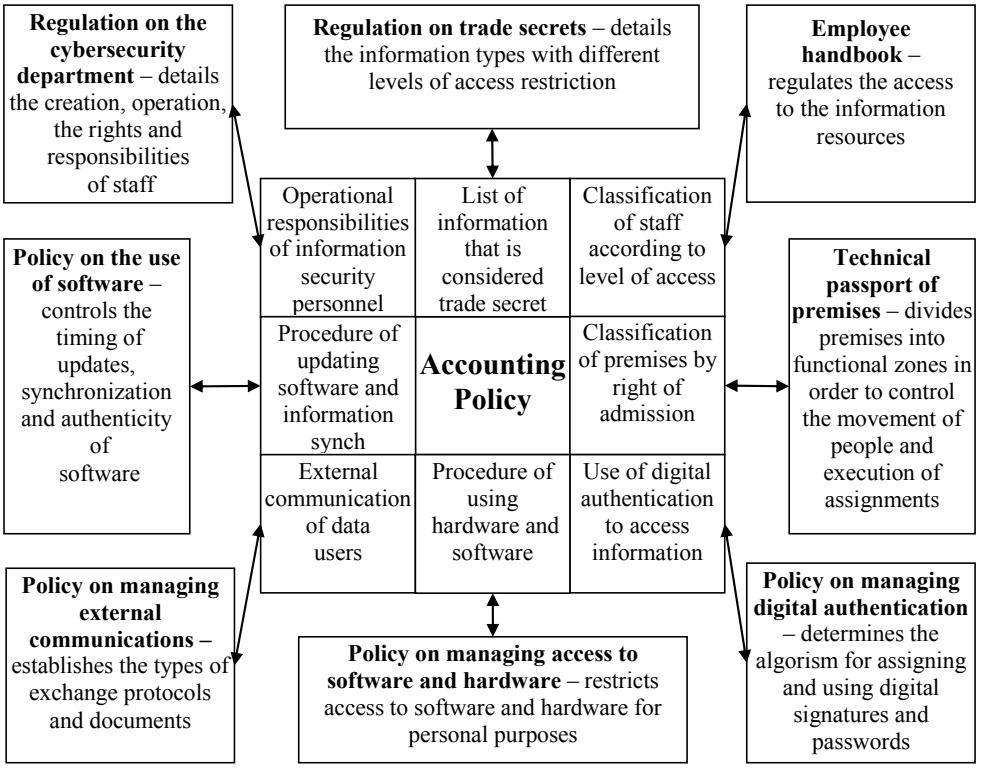

Fig. 2. Security regulations in the accounting policy of an enterprise and internal normative documents

Source: developed by the authors

The basis of a complex system of information securityat an enterprise is the full distribution of access rights to accounting information. It is advisable for all accounting and administrative employeesdepending on the position and hierarchical level in the management systemto

limit physical access to the data base through the mechanism of individual digital signature. With the purpose of ensuring distributed access to accounting information, it is necessary for a company to develop Regulations on trade secrets. According to K.P. Borymska and N.V. Kinzerska, it is necessary to clearly indicate in the Regulations what information is a trade secret, the procedure for classifying them as such, storage conditions, as well as employees of an enterprise who can pass confidential information to representatives of state organizations [13, p.17].

All personnel of an enterprise must be divided into the level of rights for access. It is advisable to place a table of conformities of each employee to the individual security level in the Regulations on trade secrets. The amount of the given information should be sufficient for performing functional responsibilities or making effective management decisions. The job descriptions of each employee indicate the level of access to trade secrets and the responsibility for its disclosure. As a result, accounting information is limited to accounting and management professionals only in the scope of their direct functional authorities. With the growth of hierarchical level of management,the volume of available accounting information for an acquaintance increases.

It is necessary to indicate in the accounting policy of an enterprise the term of validity of powers in authorised access of employees to trade secrets. The duration of access rights is directly proportional to the level in the management hierarchy. For employees with lower qualifications, it is necessary to significantly reduce the calendar time and access to accounting information. Only with the growth of experience and professional skills it is advisable to increase the level of information trust in a person. Adjustment ofa temporary access to trade secrets will ensure the avoidance of leakage of confidential registration information due to high turnover rate of personnel or temporary employed agents of information malefactors.

With the purpose of preventing unauthorized persons from entering the territory of an enterprise, an automated access system is used. It is recommended to equip all premises of an enterprise with technical tracking devices. Similar to functioning of the system of staff access to accounting information, it is advisable to organize control over the movement of employees throughout an enterprise. The accounting policy should foresee the classification of premises by the right of admission of different groups of employees. Thanks to the system of the automated access mode the control over unauthorized movement of the personnel is provided. It is prohibited for persons to enter premises that do not belong to their direct competence and are not intended for the performance of functional powers.

It is also advisable to control the access of employees to computer and communication equipment. Computer, telecommunications and network systems are owned by the company, which requires its use only for performing work tasks. To prohibit completely the use of software and hardware by the staff for personal goals is quite difficult. It is advisable to determine in the accounting policy the procedure for using the technical and software infrastructure of an enterprise in order to prevent leakage of confidential information through unauthorized information services. Therefore, it is necessary to prohibit access from work computers to certain software, web resources and e-mails that can be used by malefactorsfor violation of the information security of the business entity.

ISSN 2786-4537 (print). Вісник економіки № 1, 2022 р.
ISSN 2786-4545 (online). Herald of Ternopil National Economics № 1, 2022

The additional internal regulations must provide a list of all software and hardware in terms of access rights that can be used by the company's staff. In the "Software access control policy" document it is advisable to indicate the following prohibitions: to change and copy files belonging to other users; install third-party software on computers and on the network; send any documents by e-mail to other persons and organizations; to place personal announcements, petitions, advertising offers, etc. [14, p.318]. It is definitely recommended to mention the possibility of monitoring and verification of the content of all information sent from technical devices and computer programs of the business entityby the company's management.

The distributed access system is implemented through a digital signature mechanism. Each employee is provided with a personal electronic key, which is supplemented by a login and password. The digital key is entered into the employee's software on all technical devices performing functional duties. Personal computers and mobile devices can be used by personnel inside and outside an enterprise. The digital key is exclusively personalized in order to identify each person who is responsible for the implementation of information procedures. Thanks to the system of digital signatures, it is possible to control all information resources and technical devices that the accounting or management specialist dealt with. It is recommended for a company to adopt the Regulations on the use of digital signatures, which regulate the process of assigning and using access keys to accounting information.

The electronic key system is actively used with the purpose of protection and identifying information communications with the country's fiscal service. Therefore, most companies already have sufficient infrastructure to use digital signatures in information processes. It is recommended to supplement the existing system of authentication of officials by obligatory assignment of identified electronic keys to all accounting and management employees. Digital signatures identify the employee in the process of internal and external communications.

For external information links, it is important to specify the selected communication channels. In order to prevent the theft of confidential data, it is important to regulate information flows in the accounting policy of an enterprise. If the communication takes place directly with the counterparty, it is necessary to conclude an agreement with each business entity (institution) on the scheme of organization of information relations. The general conditions of the agreements are synchronized with the accounting policy of an enterprise on the procedure, technology and software and hardware of information exchange. Communication ties with external users through the use of an intermediary operator requires connection of a company to common telecommunications channels. The company's management must select and reflect the method of communication in the accounting policy.

As K.P. Borymska and N.V. Kinzerska note, there are special operators on the market that offer a range of services for inter-corporate exchange of electronic information: 1) services for the organization of permanent data exchange – "connection to the network"; 2) services for transfer of accounting information (after connection) – "communication services" [13, p.19]. A distinctive feature of external communication methods is the number of acts of information exchange. When using the method of communication "connection to the network", the accounting department of an enterprise receives accounting information

immediately after it is sent from the sender. In other case ("communication services"), it is recommended to indicate in the accounting policy the time of connection of the software to the communication channels in order to download / unload the accounting information accumulated from the moment of the previous information exchange.

Threatening for information security in automated accounting system can be knavish modifications of special softwear. Computer programs can be modified or they can be substituted by malefactorsfor stealing confidential accounting information. Information protection at an enterprise provides constant control over the authenticity of the software through the mechanism of obtaining and controlling electronic certificates from developers. It is advisable to make an agreement with software manufacturers on the periodic confirmation of the certificate of authenticity. The accounting policy should specify the frequency with which each computer program is inspected for authenticity and integrity. It is obligatory to confirm the electronic certificate by the developer after each update of the program.

Software for the purposes of automation of accounting must be alloted with the following properties: compatibility with other computer programs, prompt correction of errors and corrections without suspending the accounting process, restoration of results in case of software and hardware damage. Special attention from the point of view of protection of accounting information requires the possibility of information synchronization of software products from different manufacturers. With the purpose of organization of free information exchange, it is necessary to specify in the accounting policy of a company the type of a protocol or the format of the exchange file that will be used for synchronization. Determining the type of communication channels when establishing a connection between software will allow to minimize the information threats for the loss of information or theft through the use of unknown exchange protocols. The accounting policy regulates the order of simultaneous use of computer programs, which will not allow accounting and management professionals to make mistakes in the process of performing functional duties [15].

Similarly, it is necessary to determine the methodology and those responsible for making changes to the algorithm of the software. Accountants with a high level of confidence in trade secrets of an enterprise should be given the right to correct errors and update computer programs in accordance with changes in national legislation or other environmental factors. It is also necessary for an enterprise to determine the order of permanent testing of software products for their relevance and correctness in the accounting policy. At certain intervals, accounting and management professionals need to be instructed how to enter and process the modelled accounting information that has the probabilistic character. In other words, the economic situation in the process of functioning of an enterprise is modeled with the corresponding reflection in the system of accounting and management. After confirming the effectiveness of automated actions, the information is removed from the system in order to avoid the impact on the real economic performance of the entity. There is only a report, which is passed for acquaintance to the management of an enterprise.

Conclusions and prospects for future research. In the accounting policy of an enterprise or in separate internal regulations it is offered to fix: the list of the information which is a trade secret; the procedure for updating software and methods of information synchronization with cloud services; implementation of external communications with users of information; the procedure for using software and hardware; algorithm of distribution

ISSN 2786-4537 (print). Вісник економіки № 1, 2022 р.
ISSN 2786-4545 (online). Herald of Ternopil National Economics № 1, 2022

and application of electronic keys for access to information; classification of premises by the right of admission and organization of the system of protection of the territory of an enterprise; classification of employees according to the hierarchical level of access to information resources of an enterprise, etc.

Information protection in conditions of automation of accounting and management involves a combination of organizational actions of employees of an enterprise, which should be reflected in the accounting policy and internal regulations. The security provisions of the regulation of processing of accounting data require establishment of an effective division of functional powers of staff and granting of access rights to confidential information. Access to databases is realized through the issuance of personal digital signatures, logins and passwords. Thanks to the technologies of authorization, the responsibility and track of the staff's actions concerning data processing and transmission is established.

Through reflecting the time criteria for conducting checks of the state of information security, data exchange protocols, exchange types of documents, certificates and licenses for the use of software at an enterprise, the reliability of accounting information in the process of performing functional and accounting responsibilities by accounting and management specialists is guaranteed.Broadening and combination of functional powers of accountants in conditions of automation of accounting and organization of electronic communications is the subject of further researches.

Література

1. World Digital Competitiveness Ranking IMD 2018. URL: https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2018
2. Global Cybersecurity Index (GCI) 2018. / International Telecommunication Union. Geneva: ITUPublications. 86 p. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
3. Цаль-Цалко Ю. С., Мороз Ю. Ю. Облікова політика підприємства та її кібербезпека. Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства : зб. наук. праць, т. IV, ч. I, Житомир : ПП «Рута», 2017. С. 8–11.
4. Пушкар М. С., Щирба М. Т. Теорія і практика формування облікової політики : моногр. Тернопіль : Карт-бланш, 2010. 260 с.
5. Герасимович І. А. Організація облікової політики сучасного підприємства. Інвестиції: практика та досвід. 2018. № 7. С. 49–53.
6. Kafka, Sofiia. The stages of accounting policies formation. *The actual problems of regional economy development.* 2017. № 1. P. 156–164. DOI: http://doi.org/10.15330/apred.1.13.156-164.
7. Alibhai, Salim, Bakker, Erwin, Balasubramanian, T., Bharadva, Kunal, Chaudhry, Asif, Coetsee, Danie, Johnstone, Chris, Kuria, Patrick, Naidoo, Christopher & Ramanarayanan, J. Accounting policies, changes in accounting estimates and errors. *Interpretation and Application of IFRS® Standards. Wiley.* 2021, 117–137. DOI: http://doi.org/10.1002/9781119818663.ch7.

8. Kim, Jihyun. Accountability Policy 2.0: A New Direction of Accountability Policies Based on Every Student Succeeds Act in the U.S. *The Korean Educational Administration Society.* 2021. № 39. P. 69–94. DOI: http://doi.org/10.22553/keas.2021.39.2.69.
9. Harrast, Steven. Robotic process automation in accounting systems. *Journal of Corporate Accounting & Finance.* 2020. № 31. P. 4. DOI: http://doi.org/10.1002/jcaf.22457.
10. Lagovska, Olena & Loskorikh, Gabriella. Formation of Accounting Policy in IT Enterprises. *Modern Economics.* 2020. № 19. P. 108-113. DOI: http://doi.org/10.31521/modecon.V19(2020)-18.
11. Drokina, N. & Kaipova, Gulnara. Formation of accounting policy content. *Chronos Journal.* 2020. DOI: http://doi.org/10.31618/2658-7556-2020-40-1-3.
12. Zadorozhnyi Z.-M., Muravskyi V., Shevchuk O. and Muravskyi V. The accounting system as the basis for organising enterprise cybersecurity. *Financial and credit activity: problems of theory and practice.* 2020. № 3. P. 147–156. DOI: http://doi.org/10.18371/fcaptp. v3i34.215462.
13. Боримська К. П., Кінзерська Н. В. Концептуалізація захисту бухгалтерської інформації при міжкорпоративному електронному документообороті торговельних підприємств: проблемні аспекти. Вісник ЖДТУ. Серія: економічні науки. 2013. № 3 (65). С. 16–25.
14. Мілян К. В., Грицюк Ю. І. Особливості організації інформаційної безпеки корпоративної мережі промислової компанії. Науковий вісник НЛТУ України. 2013. Вип. 23 (4). С. 314–328.
15. Деньга С. М., Верига Ю. А. Захист інформації в комп›ютерних інформаційних системах бухгалтерського обліку. Бухгалтерський облік і аудит. 2004. № 5. С. 59–65.

References

1. World Digital Competitiveness Ranking IMD 2018. https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2018 [in English].
2. Global Cybersecurity Index (GCI) 2018 / International Telecommunication Union. Geneva : ITUPublications. 86 p. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf [in English].
3. Tsal-Tsalko Yu.S. and Moroz Yu.Yu. (2017). Oblikova polityka pidpryiemstva ta yii kiberbezpeka [Accounting policy of the enterprise and its cyber security], Accounting, analysis and control in the conditions of modern concepts of management of the economic potential and market value of the enterprise, Vol. IV, Part I, 8-11 [in Ukrainian].
4. Pushkar M.S., Shchyrba M.T. (2010). Teoriia i praktyka formuvannia oblikovoi polityky : monohrafiia [Theory and practice of accounting policy: a monograph.]. Ternopil : Kart-blansh, 2010. 260 p. [in Ukrainian].

5. Herasymovych, I. (2018). Orhanizatsiia oblikovoi polityky suchasnoho pidpryiemstva [Organization of accounting policies of the modern enterprise]. *Investytsiyi: praktyka ta dosvid,* 7, 49-53 [in Ukrainian].
6. Kafka, Sofiia. (2017). The stages of accounting policies formation. *The actual problems of regional economy development,* 1, 156-164. DOI: http://doi.org/10.15330/apred.1.13.156-164 [in English].
7. Alibhai, Salim, Bakker, Erwin, Balasubramanian, T., Bharadva, Kunal, Chaudhry, Asif, Coetsee, Danie, Johnstone, Chris, Kuria, Patrick, Naidoo, Christopher & Ramanarayanan, J. (2021). Accounting policies, changes in accounting estimates and errors. *Interpretation and Application of IFRS® Standards. Wiley,* 117-137. DOI: http://doi.org/10.1002/9781119818663.ch7 [in English].
8. Kim, Jihyun. (2021). Accountability Policy 2.0: A New Direction of Accountability Policies Based on Every Student Succeeds Act in the U.S. The Korean Educational Administration Society, 39, 69-94. DOI: http://doi.org/10.22553/keas.2021.39.2.69 [in English].
9. Harrast, Steven. (2020). Robotic process automation in accounting systems. *Journal of Corporate Accounting & Finance*, 31, 4. DOI: http://doi.org/10.1002/jcaf.22457 [in English].
10. Lagovska, Olena & Loskorikh, Gabriella. (2020). Formation of Accounting Policy in IT Enterprises. *Modern Economics*, 19, 108-113. DOI: http://doi.org/10.31521/modecon.V19(2020)-18 [in English].
11. Drokina, N. & Kaipova, Gulnara. (2020). Formation of accounting policy content. Chronos Journal. DOI: http://doi.org/10.31618/2658-7556-2020-40-1-3 [in English].
12. Zadorozhnyi, Z.-M., Muravskyi, V., Shevchuk, O. and Muravskyi, V. (2020). The accounting system as the basis for organising enterprise cybersecurity. *Financial and credit activity: problems of theory and practice,* 3, 147-156. DOI: http://doi.org/10.18371/fcaptp. v3i34.215462 [in English].
13. Borymska, K. P. and Kinzerska, N. V. (2013) Kontseptualizatsiia zakhystu bukhhalterskoi informatsii pry mizhkorporatyvnomu elektronnomu dokumentooboroti torhovelnykh pidpryiemstv: problemni aspekty [Conceptualization of the protection of accounting information in the inter-corporate electronic document circulation of trade enterprises: problem aspects], *Bulletin of ZHSTU – Visnyk ZHDTU,* 3 (65), 16-25 [in Ukrainian].
14. Milian, K.V. and Hrytsiuk, Yu.I. (2013). Osoblyvosti orhanizatsii informatsiinoi bezpeky korporatyvnoi merezhi promyslovoi kompanii [Features of the organization of information security of the corporate network of an industrial company]. *Naukovyi visnyk NLTU Ukrainy - Scientific Bulletin of NLTU of Ukraine,* 23 (4), 314-328 [in Ukrainian].
15. Denha, S. M. and Veryha, Yu. A. (2004). Zakhyst informatsii v komp`yuternykh informatsiinykh systemakh bukhhalterskoho obliku [Protection of information in computer information systems accounting]. *Bukhhalterskyi oblik i audyt - Accounting and auditing,* 5, 59-65 [in Ukrainian].

Статтю отримано 15 грудня 2021 р.
Article received December 15, 2021.