WEST UKRAINIAN NATIONAL UNIVERSITY

55th Anniversary
of WUNU

Volodymyr Muravskyi

ACCOUNTING AND CYBERSECURITY

Monograph

Scientific Editor
Doctor of Economics, Professor
Z.-M. Zadorozhnyi

2021

UDC 657:004
ISBN 978-0-578-33183-6

Reviewers:

Lehenchuk Serhiy Fedorovych, Doctor of Economics, Professor, Head of the Department of Information Systems in Management and Accounting of Zhytomyr Polytechnic State University;

Sadovska Iryna Borysivna, Doctor of Economics, Professor, Head of the Department of Accounting and Taxation of Lesya Ukrainka Volyn National University;

Shyhun Maria Mykhailivna, Doctor of Economics, Professor, Head of the Department of Accounting and Consulting, Kyiv National Economic University named after Vadym Hetman.

Under scientific editorial supervision of Doctor of Economics,
Professor Z.-M. Zadorozhnyi

Recommended for publication by the decision of the Academic Council of West Ukrainian National University (Protocol № 3, November 16, 2021)

Muravskyi, Volodymyr. Accounting and Cybersecurity: Monograph. Scientific Editor – Z.-M. Zadorozhnyi. Kindle Publishing, KDP, Seattle. USA. 2021. 200 p.

ISBN 978-0-578-33183-6

The monograph examines the theoretical and applied aspects of the development of accounting to ensure cybersecurity of enterprises. The positioning of the accounting system as a platform for the organization of economic and information security of enterprises is proposed. The classification of cyber risks in accounting and users of accounting information is improved to prevent and eliminate cyber threats. A method of accounting for individual accounting objects using information and communication technologies to ensure cybersecurity of enterprises is developed. The organizational features of accounting in the context of the organization of cybersecurity of enterprises are considered.

The monograph will be useful for accounting professionals, scientists, teachers, graduate students, doctoral students, students of economic and technical specialties and anyone interested in the problems of computerization of accounting, control, management.

INDEX

PREFACE

Emergence of the digital economy, the growing number of global hybrid conflicts, social distancing and remote operation of enterprises in a pandemic has led to an increase in cyber threats to economic systems at micro and macro levels. The active development of computer and communication technologies in the digital economy has led to a variety of cyber threats aimed at providing third parties with economic benefits or causing enterprises economic damages due to the expansion of facilities and vulnerabilities in information system of enterprises. Since accounting is the main generator of economic information, accounting information requires foremost cybersecurity. Ensuring cybersecurity involves not only protecting accounting data, but also making accounting the actor in the security processes. It is necessary to involve accounting specialists in the issues of enterprise cybersecurity.

Cybersecurity of enterprises, sectors and industries entails information protection and prevention of organisational, technological, PR and investment losses using accounting techniques. 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. Ensuring effective cybersecurity of enterprises requires improvement of the theory, methodology, applied and organization of accounting.

Therefore the monograph consists of three chapters: "Theoretical foundations of the relationship between accounting and cybersecurity of enterprises", "Improving accounting methods for the purposes of cybersecurity of enterprises", "Organization of accounting to ensure cyber protection of enterprises". The monograph is intended to be used by researchers, lecturers, teachers, doctoral and post-graduate students of economic and technical specialties specialties of higher education institutions as well as for managers, accountants, economists and cybersecurity professionals at the enterprises.

CONCLUSIONS

1. 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. The accounting system 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 cybersecurity 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 cybersecurity, 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.

2. Activization of 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.

3. The need for effective cybersecurity of accounting data requires adaptive consideration of various cyber threats. The type of cyber risks can determine the significant differences in measures to prevent, avoid and eliminate potential consequences. Therefore, it is advisable to group the cyber risks of accounting data using the classification criteria of intent, mode, information and financial interest, location, instigator, origin, goal, target, scale, form of manifestation, legality, aspect, duration, latency, probability, and consequences.

Classification by other criteria related to the activities of criminals or stakeholders is not very informative for the purposes of protection against cyber threats. The increasing complexity of information processes and advancements in computer and communication technologies precipitate the need for improvements in the suggested classification of cyber threats to accounting data, and therefore, further scientific research.

4. The implementation of computer and communication technologies in all socio-economic processes has led to the growing number and intensity of cyber threats to enterprise operation. The ultimate goal of cyber threats is to obtain economic benefits for third parties or to cause economic damage to businesses. There is a direct relationship between cyber risks and the economic condition of the enterprise.

Accounting should be considered an innovative mechanism of ensuring the interaction between the economic and cybersecurity of the enterprise. Accounting links are present at five accumulative levels and explain the impact of cyber risk activity on the increase in threats to the economic security of economic entities. At the methodological level, the cyber threats concern the principles and functions of accounting; at the quality level – the quality of accounting data; at the methodical level – accounting items and types; at the communication level – accounting communications with stakeholders; at the reputation level – business image of the enterprise, which leads to economic losses for the enterprise. At the same time, the accounting methods create the conditions for the feedback between economic and cybersecurity, which consists of reliable identification and assessment of economic losses from the manifestation of cyber risks.

5. Activation of cyber threats due to global hybrid conflicts, COVID-19 pandemic, economic imbalances, requires the organization of an effective system of enterprises' cyberdefense. The main object of cyber-attacks in digital economy is accounting information. Cyber threats are manifested at all stages of processing of accounting information and its

transmission to users (stakeholders).For developing effective measures to minimize cyber threats, it is necessary to understand their impact on the functioning of stakeholders in terms of their various types.

The traditional classification of accounting information users is irrelevant for the purposes of enterprises cybersecurity, as it does not take into account the activation of variable cyber threats that requires improving the classification of stakeholders. Users of accounting information should be classified according to the criteria: the ability to manage the activities of the business entity, the right of access, the likelihood of cyber threats, the ability to dispose of access rights, access to accounting objects, functional law, information processing, economic activity, age of individuals, organizational and legal form of legal entities, type of used communication channels, frequency of information acts.

6. Traditional electronic document management in accounting has a number of functional limitations, which is the cause of cybersecurity vulnerabilities of enterprises. To implement effective internal and external electronic communications, it is advisable to implement blockchain technology in document management, which meets modern requirements for cybersecurity of enterprises. The fact of collecting primary data initiates the start of further information processes of processing and distribution of accounting information. Documented data using blockchain technology is fragmented, encrypted and sent in dosed form to internal and external users in accordance with the information needs and access rights to trade secrets. The permissive mode of accounting information processing should be implemented using a system of digital signatures and cloud placement of distributed databases.

The use of blockchain technology in electronic documentation and document management provides: fragmentation, complementarity, scalability, duplication, chronology, confidentiality, distribution, accessibility, openness of accounting information processing, which is the basis for effective cybersecurity of the enterprise. The organization of

cybersecurity in the conditions of distributed structuring of the accounting information promotes openness of document circulation at the enterprise that reduces need for application of isolating information practices. The openness of information exchange using blockchain technology for cybersecurity of information minimizes organizational constraints in the formation of the digital economy and creates favorable conditions for the progressive innovative development of social formation.

7. The need to obtain prompt access to funds through electronic communications, protecting investment after the global financial crisis has led to the emergence of a new type of electronic money – the cryptocurrencies. Cryptocurrencies gain significant popularity due to the advantages of their use, such as: comfort, independence, accessibility, lack of engagement, confidentiality, no documents, full automation of accounting, and cost optimization.

Cash as a means of money turnover is losing popularity progressively in commercial settlements that allows to refuse such organizational structure as a cashier and with that, from documents and accounting professionals responsible for cash transactions. The possibility of integrated support of personal wallets for electronic money in mobile devices provides non-cash settlement for purchased goods (services) similar to bank cards.

Evolutionary development of electronic money, international payment systems, information systems of remote notification and fund management requires adequate changes in the organization and methods of automated management accounting of non-cash transactions. Modern systems of remote management of the "Client-Bank" and "Internet-Bank" accounts are characterized by certain organizational constraints that do not meet the modern notions of non-cash transactions with help of the cryptocurrencies and other electronic money. Combining the functional capabilities of the blockchain technology, positive qualities of the communications "Internet Bank" and "Client-Bank" will allow to create a hybrid system of non-cash payments by cryptocurrencies, electronic money, funds on accounts in a

bank with free conversion of existing funds and opportunities for information exchange with all the participants in settlement operations. Collection of accounting information on settlements with the cryptocurrencies and other electronic money is carried out without formation of the traditional payment documents and bank statements. Electronic information from the hybrid communication system is the foundation for providing cybersecurity, fully automated documenting, formation of accounting records, informing accountants and management of non-cash transfers. Automation of accounting of cash transactions helps to increase the level of cyber defense control over execution of money transactions due to timely and remote informing sharing about the parameters of non-cash payments.

8. Areas of IoT using in the accounting automation and enterprise cybersecurity are: the transformation of accounting, improving the audit control of economic activity and optimization of accounting and control specialists work. The use of IoT devices provides: reducing the participation of the human factor in the processing of accounting information, distancing the capturing and processing of primary data, automation of business documentation, delegation of accounting and security authorities, compliance with quality information and improving the form of accounting for Big data ready.

Along with the significant advantages of the implementation of IoT technology in the activities of enterprises there are disadvantages - active cyber risks. Threats to entities cybersecurity are: theft, substitution and blocking of information, gaining control over the equipment or denial of its operation, increasing the access rights of employees and outsiders to enter the prohibited territorial information boundaries of the enterprise. Prevention and avoidance of cyber threats IoT devices using requires regulation of communication channels of credentials, regulation of access rights to confidential data, use of a policy of permanent password renewal for access to databases and technology sensors, correct distribution of

information flows between different stakeholders. Therefore, the risks of implementing IoT technology are significantly minimized provided the effective organization of accounting with its positioning as a basis for establishing cybersecurity of information flows.

9. To ensure control over the access of employees to information and material flows, automated checkpoint systems are used to admit employees to the premises and buildings of the enterprise. The operation of the system mainly involves the implementation of security functions. However, modern conditions of growing cyber threats caused by the hybrid conflicts around the world and looming biological threat of the COVID-19 pandemic necessitate the introduction of biometric authentication of employees, leading to the transformation in the accounting and control over time worked by the employees, accrual of basic and additional wages, as well as creation of digital primary documents and reports consequently sent to stakeholders.

Biometric employee authentication should be used when they cross between separate functional areas of the enterprise and its individual buildings. The entire territory of the entity should be divided into different functional areas for different groups of staff in order to restrict access to confidential information, which will help ensure a sufficient level of cybersecurity of the enterprise. It is recommended to pay wages in accordance with the time spent within the areas that correspond to the functional duties of the employee or the time spent operating equipment connected to their official duties (including from home). For the purposes of automated accounting and control, functional and time regulations for the implementation of functional responsibilities and stay in certain types of premises are developed in advance for each employee. Regulating the time parameters of employees' work helps to avoid overcrowding on the premises of the enterprise, which helps to minimize biological threats (COVID-19 infection).

It is advisable to introduce one minute as the measure unit to ensure effective accounting and control of the time worked. The use of a more

detailed unit of measure creates an opportunity to account for and control deviations from the standards of working time, ensure self-management of employees, and increase their productivity. Failure to comply with the work schedule may be grounds for review of working conditions or the need for professional retraining of the relevant specialist. On the other hand, information on overtime work (including remote performance of official duties from home) should lead to the accrual of additional compensation and incentive payments to employees.

Information from the system of biometric employee authentication on the performance of functional duties at the employees' workstations at home or work can be used to help optimize the accounting of employee costs. Automation can also be used in accounting for the cost of food, operation of common areas, overhead costs with a clear distribution between production, administrative, marketing and other costs. Information on time worked and wages created by the system of biometric employee authentication is summarised in electronic form and sent to internal and external stakeholders.

10. The progressive development of communication technologies creates new requirements for data transfer speeds. The use of 4G cellular communication and the new generation of 5G is not able to meet the information needs of users of artificial intelligence technologies, total virtualization of communications, unmanned and autopilot vehicles, connection to the Internet of all technical devices, which requires the concept of 6G mobile communications.

An important advantage of the sixth generation of cellular communication is the three-dimensional reliable determination of the subscriber's location and direct information connection between the elements of the cellular network, which allows transformation of accounting of enterprises in various fields. In particular, fundamental changes are made to the accounting of costs with the use of: production equipment connected to the information system of an enterprise, for permanent timely

determination of the cost of industrial products; vehicles with controlled movement by agreed routes and preventive identification of the cost of providing transport services; swarms of unmanned aerial vehicles for aerovisual observation of agricultural and construction works with reliable definition and distribution of income and expenses; technologies for counting the number of visitors to the company's premises to determine the popularity of retail space and advertising in order to inform customers about their value.

At the same time, the information system of enterprises using 6G cellular networks is threatened by significant cyber risks: attacks using artificial intelligence, previously unknown vulnerabilities of “Zero Day”, risks based on quantum calculations, attacks using fast (TeraHertz) equipment, hybrid wars etc. To ensure cybersecurity, it is necessary to use 6G cellular networks to monitor: the location of employees on the territory or premises of an enterprise; routes of movement and performance of works by vehicles; access of persons to production equipment, construction sites or places of agricultural work; the presence of criminals at the scene of offenses in order to prevent the loss of material and information resources of economic entities.

11. 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 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.

12. Shift to digital economy, growing number of global hybrid threats, and remote processing of information caused by the COVID-19 pandemic necessitate accounting to be improved. One of the methods for optimizing accounting is the delegation of accounting functions (outsourcing). Transfer of accounting information and functions is accompanied by active cyber threats. Under conditions of outsourcing accounting, it is necessary to identify cyber risks in terms of variable accounting factors to ensure the enterprise cybersecurity.

The organizational factors of accounting that affect the cybersecurity of enterprises include the subject of accounting, number of employees, uncertainty, remote work, communication with the outsourcer, communication with stakeholders, automation, frequency of information updates. According to the selected organizational options, it is possible to assess the probability of cyber risks in terms of different forms of accounting outsourcing.

Cyber risks are significantly minimized when delegating accounting operations to cloud information-processing services. However, the cloud version of delegation is complicated if there is need for continuous communication of the outsourcer with the management of the company and stakeholders, which make it impossible to recommend such an option of outsourcing for all businesses. Therefore, the optimal form of outsourcing for each business entity is the one with the minimum total probability of cyber risks for all organizational accounting factors.

13. Integrated positioning of accounting and security authority outsourcing is necessary to optimize the functioning of enterprises. Combined delegation of accounting and cybersecurity functions will help synergistically minimize administrative costs, reduce the likelihood of information and financial risks. The integration of outsourcing is possible in two ways, depending on the objects and types of accounting (object model) or the organizational structure of the enterprise (structural model).

The implementation of the object model involves the delegation of processing and cybersecurity of financial accounting information about individual objects of accounting. Operation of management accounting information, which may contain trade secrets, is performed only in the accounting department of the enterprise. According to the structural organizational model, outsourcing of accounting and security powers is possible only for the operation of business units of the enterprise (structural units) with the consolidation of information in the accounting of the parent company. Due to the manifestation of significant cyber risks, a comprehensive delegation of all accounting and security powers in the object and structural model of outsourcing is impossible.

To avoid organizational constraints on the implementation of object and structural options for outsourcing, it is advisable to use a combined (mosaic) model, which is a mosaic delegation of accounting and security functions to many outsourcers. All accounting and cybersecurity powers are divided into subsets and delegated to various outsourcers, which are

informationally combined using blockchain technology. With the help of blockchain technology, disparate accounting information is integrated and transmitted to the accounting and management of the enterprise for further processing. The implementation of the proposed model provides comprehensive outsourcing of accounting and security functions with an effective system of cybersecurity of enterprises.

REFERENCES

1. 2019 Cyberthreat Defense Report (2019). CyberEdge Group. Annapolis: CyberEdge Group. 50 p.

2. Abdelwahab, I., Ramadan, N. & Hefny, H. (2020). Cybersecurity Risks of Blockchain Technology. International Journal of Computer Applications. 177. 8-14. 10.5120/ijca2020919922.

3. Aisenberg, Michael & Editor, Esq. (2018). State and Local ICT Policy: A Framework for Cybersecurity, IOT, Cloud, Block Chain, etc. Sub-Federal Cyber Policy. URL: https://www.researchgate.net/publication/334747029_State_and_Local_ICT_Policy_A_Framework_for_Cybersecurity_IOT_Cloud_Block_Chain_etc.

4. 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.

5. 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. 10.1002/9781119818663.ch7.

6. Alkarawy, H. & AL-Kuwair, E. (2021). Accounting improving the costs and business process management in transportation to a third party. Accounting. 701-708. 10.5267/j.ac.2020.12.006.

7. Al-Mohammed, H. & Yaacoub, E. (2021). On The Use of Quantum Communications for Securing IoT Devices in the 6G Era. 1-6. 10.1109/ICCWorkshops50388.2021.9473793.

8. Almutairi, M. & Riddle, S. (2018). A Framework for Managing Security Risks of Outsourced IT Projects. An Empirical Study. 40-44. 10.1145/3178461.3178476.

9. Alsaqa Zeyad, H., Hussein, A. I., Mohammed Mahmood, S. (2020). The Impact of Blockchain on Accounting Information Systems. Journal of Information Technology Management, 11. 62-80. 10.22059/jitm.2019.74301.

10. Asatiani, A., Apte, U., Penttinen, E., Rönkkö, M. & Saarinen, T. (2019). Impact of accounting process characteristics on accounting outsourcing - Comparison of users and non-users of cloud-based accounting information systems. International Journal of Accounting Information Systems. 34. 10.1016/j.accinf.2019.06.002.

11. Asieieva, Yu. (2020). Problem questions of cyber-addictions classification. Psychology and Personality. 2. 23-40. 10.33989/2226-4078.2020.2.211910.

12. Avtomatyzovana systema kontroliu dostupu [Automated access control system]. Material z Vikipedii – vilnoi entsyklopedii – From Wikipedia, the free encyclopedia. URL: https://uk.wikipedia.org/wiki/Автоматизована_система_контролю_доступу.

13. B2B cross-border transactions on blockchain in various regions worldwide in 2020 with forecasts from 2021 to 2025. Statista. https://www.statista.com/statistics/1228825/b2b-cross-border-transactions-on-blockchain-worldwide/

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

15. Balaziuk, O.Yu., Sysoieva, I.M., Pilyavets, V.M. (2020). Control and accounting aspects of introducing agile methodology for software development projects. Financial and credit activity: problems of theory and practice. 3 (34). 94-102.

16. Bansal, S.K., Batra, R., Jain, N. (2018). Blockchain and the future of accounting, The Management Accountant Journal, No. 6, 60-66.

17. Baranenko, R.V. (2021). Cyber attacks as a form of cyber terrorism. Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences. 1. 45-50. 10.32838/2663-5941/2021.1-1/07.

18. Benaroch, M. (2020). Cybersecurity Risk in IT Outsourcing—Challenges and Emerging Realities. Information Systems Outsourcing. 313-334. 10.1007/978-3-030-45819-5_13.

19. Biometriia [Biometrics]. Material z Vikipedii – vilnoi entsyklopedii – From Wikipedia, the free encyclopedia. URL: https://uk.wikipedia.org/wiki/Біометрія.

20. Bonson, E., Bednarova, M. (2019). Blockchain and its implications for accounting and auditing, Meditari Accountancy Research, Vol. 27 No. 5, 725-740. 10.1108/MEDAR-11-2018-0406.

21. Boonkrong, S. (2021). Biometric Authentication. Authentication and Access Control, 107-132. doi: 10.1007/978-1-4842-6570-3_5.

22. Borymska, K. P. (2013). Zakhyst bukhhalterskoi informatsii v oblikovii politytsi z metoiu opodatkuvannia: orhanizatsiini aspekty [Protection of accounting information in accounting policy for tax purposes: organizational aspects]. Zbirnyk naukovykh prats Natsionalnoho universytetu derzhavnoi podatkovoi sluzhby Ukrainy. – Collection of scientific works of the National University of the State Tax Service of Ukraine. 2013. № 2. 14-21. URL: http://nbuv.gov.ua/UJRN/znpnudps_2013_2_4.

23. 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.

24. Bukhhalterskyi oblik v upravlinni pidpryiemstvom [Accounting in enterprise management] (2017). / O.A. Lahovska, S.F. Lehenchuk, V.I. Kuz,

S.V. Kucher. Zhytomyr: Zhytomyrskyi derzhavnyi tekhnolohichnyi universytet. 416 p. URL: https://learn.ztu.edu.ua/mod/resource/view.php?id=17967.

25. Cai, C.W. (2021). Triple-entry accounting with blockchain: how far have we come?, Accounting Finance. 10.1111/acfi.12556.

26. Chesney, Steve, Roy, Kaushik & Khorsandroo, Sajad. (2021). Machine Learning Algorithms for Preventing IoT Cybersecurity Attacks. 10.1007/978-3-030-55190-2_53.

27. Chikutuma, C. (2016). Integrated Reporting: A Story of Stakeholder Accountability. 5th International Conference on Accounting, Auditing, and Taxation (ICAAT 2016). 10.2991/icaat-16.2016.4.

28. Chukhno, I. S. (2012). Udoskonalennia klasyfikatsii korystuvachiv zvitnosti [Improving the classification of reporting users]. Oblik i finansy. – Accounting and finance. № 1. 85-90. URL: http://nbuv.gov.ua/UJRN/Oif_apk_2012_1_17.

29. Cohen, E. E. (2018). IoT for auditors and accountants; auditing the IoT. Retrieved from https://www.unece.org/fileadmin/DAM/cefact/cf_forums/2018_Geneva/PPTs/IoT_PPTs/12_-_Eric_Cohen_-_IoT_CEFACT.pdf.

30. Coyne, J.G., McMickle, P.L. (2017). Can Blockchains serve an accounting purpose, Journal of Emerging Technologies in Accounting, Vol. 14 No. 2, 101-111, 10.2308/jeta-51910.

31. Cremonini, M. (2020). Cloud Security Risk Management. Cloud Computing Security. 95-114. 10.1201/9780429055126-10.

32. Cullinan, C. & Zheng, X. (2017). Accounting outsourcing and audit lag. Managerial Auditing Journal. 32. 276-294. 10.1108/MAJ-03-2016-1349.

33. Demirkan, Sebahattin, Demirkan, Irem & Mckee, Andrew. (2020). Blockchain technology in the future of business cybersecurity. Journal of Management Analytics. Vol. 7, Issue 2. 189-208. DOI: 10.1080/23270012.2020.1731721.

34. Denha S.M and Veryha Yu.O. (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.

35. Denha, S. M., Veryha, Yu. O. (2004). Zakhyst informatsii v komp`yuternykh informatsiinykh systemakh bukhhalterskoho obliku [Information protection in computer information systems of accounting]. Bukhhalterskyi oblik i audyt – Accounting and auditing. 5. 59-65.

36. Desyatnyuk O., Muravskyi V. and Shevchuk O. (2021). Accounting Automation in Agroindustrial Enterprises Using Drones (UAVs). 11th International Conference on Advanced Computer Information Technologies (ACIT). 337-341. https://doi.org/10.1109/ACIT52158.2021.9548424.

37. Digital resonance: the new factor influencing location attractiveness (2019). The 2019 Kearney Global Services Location Index. URL: https://www.kearney.com/digital-transformation/gsli/2019-full-report.

38. Djenna, Amir, Saidouni, Djamel Eddine & Wafia, Abada. (2020). A Pragmatic Cybersecurity Strategies for Combating IoT-Cyberattacks. 1-6. 10.1109/ISNCC49221.2020.9297251.

39. Drokina, N. & Kaipova, Gulnara. (2020). Formation of accounting policy content. Chronos Journal. 10.31618/2658-7556-2020-40-1-3.

40. 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.

41. 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.

42. Eaton, Tim, Grenier, Jonathan & Layman, David. (2019) Accounting and Cybersecurity Risk Management. Current Issues in Auditing. Vol. 13, No. 2, C1-C9. DOI: 10.2308/ciia-52419.

43. El-Ebiary, Y. & Alawi, N. (2020). The Risks of Accounting Information Systems. International Journal of Engineering Trends and Technology. 2231-2381. 10.14445/22315381/CATI3P220.

44. Estimate of overall cryptocurrency market cap per week from July 2010 to June 2021. Statista. https://www.statista.com/statistics/730876/cryptocurrency-maket-value/

45. Fletcher, J., Gillum, D., Moritz, R., & Schwartz, A. (2020). Demographic and Salary Trends of the 2020 Biosafety Workforce. Applied Biosafety, 3. doi: 10.1089/apb.20.0066.

46. Fubara-Manuel, I. (2020). Biometric Capture. African Diaspora, 12, 1-25. doi: 10.1163/18725465-01201002.

47. Global 5G subscription forecast 2019-2025. Statista. https://www.statista.com/statistics/760275/5g-mobile-subscriptions-worldwide/

48. Global Biometrics in Workforce Management Market 2019. Data Snapshot: Biometrics in the workplace commonplace, but are they secure? URL: https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure.

49. Global Connectivity Index – GCI Ranking Table. https://www.huawei.com/minisite/gci/en/country-rankings.html.

50. Global Cybersecurity Index (GCI) 2018. (2019) / 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.

51. Global Innovation Index 2018. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2018-intro5.pdf.

52. Gomaa, A.A., Gomaa, M.I., Stampone, A. (2019). A transaction on the Blockchain: an AIS perspective, intro case to explain transactions on the

ERP and the role of the internal and external auditor, Journal of Emerging Technologies in Accounting, Vol. 16 No. 1, 47-64, 10.2308/jeta-52412.

53. Grigoreva, L. (2019). Accounting Outsourcing: Theoretical Bases and Methodological Provision. Vestnik NSUEM. 143-154. 10.34020/2073-6495-2019-2-143-154.

54. Gupta, W. (2020). Salary Estimator using Data Science. International Journal for Modern Trends in Science and Technology, 6, 319-322. 10.46501/IJMTST061259.

55. Haapamäki, Elina & Sihvonen, Jukka (2019). Cybersecurity in accounting research. Managerial Auditing Journal. No. 34. 808-834. DOI: 10.1108/MAJ-09-2018-2004.

56. Haque, Md, Haque, Shameemul, Kumar, Kailash & Singh, Narendra. (2021). A Comprehensive Study of Cybersecurity Attacks, Classification, and Countermeasures in the Internet of Things. 63-90. 10.4018/978-1-7998-4201-9.ch004.

57. Harrast, Steven. (2020). Robotic process automation in accounting systems. Journal of Corporate Accounting & Finance. 31. 4. 10.1002/jcaf.22457.

58. Henry Matey, Akwetey, Danquah, Paul, Koi-Akrofi, Godfred & Asampana, Isaac. (2021). Critical Infrastructure Cybersecurity Challenges: IoT in Perspective. International Journal of Network Security & Its Applications. 13. 41-58. 10.5121/ijnsa.2021.13404.

59. 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.

60. Herasymovych, I. (2018). Orhanizatsiia oblikovoi polityky suchasnoho pidpryiemstva [Organization of accounting policies of the modern enterprise]. Investytsiyi: praktyka ta dosvid, 7, 49-53.

61. Honcharuk, M.O. (2012). Kompiuteryzatsiia bukhhalterskoho obliku bezghotivkovykh rozrakhunkiv [Computerization of non-cash accounting]. Problemy teorii ta metodolohii bukhhalterskoho obliku, kontroliu i analizu – Problems of the theory and methodology of accounting, control and analysis, Issue. 2 (23). 47-51.

62. Horbachenko, S. (2020). Cybersecurity as a component of economic security of Ukraine. Galic'kij ekonomičnij visnik. 66. 180-186. 10.33108/galicianvisnyk_tntu2020.05.180.

63. Hoschek, M. (2021). Quantum security and 6G critical infrastructure. Serbian Journal of Engineering Management. 6. 1-8. 10.5937/SJEM2101001H.

64. 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.

65. Huang, R. & Turner, G. (2020). How the UK Can Lead in 5G and 6G Security and Standards. RUSI Newsbrief. Emerging Technologies. 40(7). 10.7945/18ch-1a56.

66. Internet of things (IoT) security threats and concerns worldwide. Statista. URL: https://www.statista.com/statistics/1202640/internet-of-things-security-concerns/

67. Internet Security Threat Report (2019). Symantec. Mountain View: Symantec Corporation. 61 p.

68. Is cybersecurity about more than protection? (2019). EY Global Information Security Survey 2018–19. URL: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2018-19.pdf?download.

69. Janvrin, Diane & Wang, Tawei (2019). Implications of Cybersecurity on Accounting Information. Journal of Information Systems. Vol. 33. No. 3. A1-A2. DOI: 10.2308/isys-10715.

70. Kafka, Sofiia. (2017). The stages of accounting policies formation. The actual problems of regional economy development. 1. 156-164. 10.15330/apred.1.13.156-164.

71. Karajovic, M., Kim, H.M., Laskowski, M. (2019). Thinking outside the block: projected phases of Blockchain integration in the accounting industry, Australian Accounting Review, Vol. 29 No. 2, 319-330, 10.2139/ssrn.2984126.

72. 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.

73. Khan, A., UL Hassan, Naveed, Y., Zhao, J., Niyato, D., Zhang, Y. & Poor, H. V. (2021). Blockchain and 6G: The Future of Secure and Ubiquitous Communication. ArXiv abs/2106.05673. https://www.researchgate.net/publication/352308474_Blockchain_and_6G_The_Future_of_Secure_and_Ubiquitous_Communication.

74. 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. 10.22553/keas.2021.39.2.69.

75. 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.

76. Kokina, J., Mancha, R., Pachamanova, D. (2017). Blockchain: emergent industry adoption and implications for accounting, Journal of Emerging Technologies in Accounting, Vol. 14 No. 2, 91-100, 10.2308/jeta-51911.

77. Kozlowski, S. (2018). An audit ecosystem to support Blockchain-based accounting and assurance book continuous auditing: theory and application, Continuous Auditing: Theory and Application (Rutgers Studies in Accounting Analytics), Emerald Publishing, Bingley, 299-313, 10.1108/978-1-78743-413-420181015.

78. Kumar, Gautam, Singh, Om Prakash & Saini, Hemraj. (2021). Cybersecurity: Ambient Technologies, IoT, and Industry 4.0 Implications. 10.1201/9781003145042.

79. Kuo, Jong-Yih, Liu, Chien-Hung & Lin, Hui-Chi. (2021). Building Graduate Salary Grading Prediction Model Based on Deep Learning. Intelligent Automation & Soft Computing, 27, 53-68. doi: 10.32604/iasc.2021.014437.

80. Kuzlu, Murat, Fair, Corinne & Güler, Özgür. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things. 1. 10.1007/s43926-020-00001-4.

81. 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.

82. Lahovska, Olena & Loskorikh, Gabriella. (2020). Formation of Accounting Policy in IT Enterprises. Modern Economics. 19. 108-113. 10.31521/modecon.V19(2020)-18.

83. Lee Gyung Min, Shim ShinWoo, Cho Byoung Mo, Kim TaeKyu & Kim Kyounggon. (2020). The Classification Model of Fileless Cyber Attacks. Journal of KIISE. 47. 454-465. 10.5626/JOK.2020.47.5.454.

84. 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.

85. Lehenchuk, S. F., Horodysky, M. P.; Maistrenko, N. M. (2021). Protection of Accounting Data in the Conditions of Using Internet of Things: Problems and Prospects of Accounting Digitalization. Oblik i Finansi. 91. 12-19. DOI:10.33146/2307-9878-2021-1(91)-12-19.

86. Li, B., Ponson, G., Ezzahi, Y. (2020). Biometrics Security. doi: 10.13140/RG.2.2.26699.41766.

87. Liakhovych, G., Bezruchuk, S., Ivanenko, V. & Laichuk, S. (2019). SWOT-Analysis Of Accounting Outsourcing. European Cooperation. 3. 7-19. 10.32070/ec.v3i43.50.

88. Liu, M., Wu, K., Xu, J. (2019). How will Blockchain technology impact auditing and accounting: permissionless vs. permissioned Blockchain, Current Issues in Auditing, Vol. 13 No. 2, 19-29, 10.2308/ciia-52540.

89. Liu, Z., Wu, L., Ke, J., Qu, W., Wang, W. & Wang, H. (2019). Accountable Outsourcing Location-Based Services With Privacy Preservation. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2936582.

90. Loboda, N., Chabaniuk, O. & Senyshyn, B. (2020). Outsourcing as a Mechanism for Accounting Innovations at Ukrainian Enterprises. Business Inform. 2. 329-336. 10.32983/2222-4459-2020-2-329-336.

91. Lu, Yang. (2020). Security in 6G: The Prospects and the Relevant Technologies. Journal of Industrial Integration and Management. 5. 271-289. 10.1142/S2424862220500165.

92. Main incidents in the EU and worldwide. ENISA Threat Landscape. (2020). URL: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents.

93. Marasigan, R. (2019). The Role of Ideas that shape the Institutional Change in Cybersecurity: Economic barriers of cyber-attacks. Policy in a

Changing World Tackling Global Issues At: Roppongi, Tokyo Japan. 10.6084/m9.figshare.12086763.

94. 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.

95. Martyniuk, T. (2016). The Informative Function of Accounting in Outsourcing of the Financial and Accounting Services. Zeszyty Naukowe Uniwersytetu Szczecińskiego Finanse Rynki Finansowe Ubezpieczenia. 2. 151-157. 10.18276/frfu.2016.2.80/2-16.

96. Maszczak, T. (2019). Accounting Outsourcing In Micro And Small Entities − Opportunities And Threats. Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. 63. 92-107. 10.15611/pn.2019.8.07.

97. Mercado-Velazquez, Andres, Escamilla-Ambrosio, P. Jorge & Ortiz-Rodriguez, Floriberto. (2021). A Moving Target Defense Strategy for Internet of Things Cybersecurity. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3107403.

98. Milian, K.V., 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.

99. Mobile broadband subscriptions worldwide 2007-2020. Statista. https://www.statista.com/statistics/273016/number-of-mobile-broadband-subscriptions-worldwide-since-2007/

100. Mobile technology share by generation 2016-2025. Statista. https://www.statista.com/statistics/740442/worldwide-share-of-mobile-telecommunication-technology/

101. 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. Part I. 8-11.

102. Muravskyi, V., Muravskyi, V., & Shevchuk, O. (2021). Classification of stakeholders (users) of accounting information for the enterprise cybersecurity purposes. Herald of Economics, 1(99), 83-96. doi:https://doi.org/10.35774/visnyk2021.01.083

103. Muravskyi, V., Pochynok, N., & Farion, V. (2021). Classification of cyber risks in accounting. Herald of Economics, 2, 129-144. doi:https://doi.org/10.35774/visnyk2021.02.129.

104. Muravskyi, V.V. (2017). Vplyv hlobalnykh tekhnolohichnykh tendentsii na orhanizatsiiu obliku [The impact of global technological trends on the organization of accounting]. Visnyk Ternopilskoho natsionalnoho ekonomichnoho universytetu – Herald of Ternopil National Economic University. № 4. 138–148. 10.35774/visnyk2017.04.138.

105. Mustafa, Nasir. (2020). Cyber Risk and Covid-19: Managing Cyber Risks Arising From The Pandemic. Brighttalk Webinar Series. Project: Coronavirus CoV-19 to CoV-20 Pro. 10.13140/RG.2.2.12218.82886.

106. Nassimbeni, G., Sartor, M. & Dus, D. (2012). Security risks in service offshoring and outsourcing. Industrial Management and Data Systems. 112. 10.1108/02635571211210059.

107. Nazarenko, O. & Surovitskaya, A. (2018). Accounting outsourcing: advantages, disadvantages, and peculiarities of introduction. Ekonomika ta derzhava. 50. 10.32702/2306-6806.2018.12.50.

108. Neil, G. (2012). Accounting for Employee Benefits. Counting the Poor: New Thinking About European Poverty Measures and Lessons for the United States. doi: 10.1093/acprof:oso/9780199860586.003.0007.

109. Nekhai, V. A., Nekhai, V. V. (2017). Informatsiina bezpeka yak skladova ekonomichnoi bezpeky pidpryiemstv [Information security as a component of economic security of enterprises]. Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu – Scientific Bulletin of the International Humanities University. 24(2). 137-140.

110. Nicholson, B. & Aman, A. (2012). Managing attrition in offshore finance and accounting outsourcing: Exploring the interplay of competing institutional logics. Strategic Outsourcing: An International Journal. 5. 10.1108/17538291211291765.

111. Number of Blockchain wallet users worldwide. Statista. https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/

112. Number of cryptocurrencies worldwide from 2013 to 2021. Statista. https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

113. O'Leary, D.E. (2017). Configuring blockchain architectures for transaction information in blockchain consortiums: the case of accounting and supply chain systems, Intelligent Systems in Accounting, Finance and Management, Vol. 24 No. 4, 138-147, doi: 10.1002/isaf.1417.

114. Ocheretko, L. & Udovychenko, H. (2020). Improvement of Salary Accounting at the Enterprise. Efektyvna ekonomika, 12. doi: 10.32702/2307-2105-2020.12.101.

115. Patterson, W. & Gergely, M. (2020). Economic Prospect Theory Applied to Cybersecurity. Advances in Human Factors in Cybersecurity. 113-121. 10.1007/978-3-030-52581-1_15.

116. Pendley, John. (2018). Finance and Accounting Professionals and Cybersecurity Awareness. Journal of Corporate Accounting & Finance. 29. 53-58. DOI: 10.1002/jcaf.22291.

117. 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.

118. Petruk, O. M., Novak, O. S. (2017). Sutnist kryptovaliuty yak metodolohichna peredumova yii oblikovoho vidobrazhennia [The essence of cryptocurrency as a methodological prerequisite for its accounting]. Visnyk ZhDTU – Bulletin of ZhSTU, 4 (82). 48-55.

119. Pidsumky 2018 roku v tsyfrakh [Results of 2018 in figures]. URL: https://cyberpolice.gov.ua/results/2018.

120. Pimentel, E., Bouliann, E. (2020). Blockchain in Accounting Research and Practice: Current Trends and Future Opportunities. Accounting Perspectives. 19 (3). 325–361. 19. 10.1111/1911-3838.12239.

121. 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.

122. Popovski, P., Chiariotti, F., Huang, K., Kalør, A., Kountouris, M., Pappas, N. & Soret, B. (2021). A Perspective on Time towards Wireless 6G.

123. Porambage, P., Gür, G., Osorio, D. P. M., Liyanage, M., Gurtov, A. & Ylianttila, M. (2021).The Roadmap to 6G Security and Privacy. IEEE Open Journal of the Communications Society, vol. 2,1094-1122. 10.1109/OJCOMS.2021.3078081.

124. Prakash, Febin, Baskar, Kala & Sadawarti, Harsh. (2019). Cyber Crime: Challenges and its Classification. International Multi-disciplinary Academic Research Conference (IMARC-2019). 2–4.

125. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy. (2017). Zakon Ukrainy [Law of Ukraine "On Basic Principles of Cybersecurity of Ukraine"]. October 5, 2017. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19.

126. 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.

127. Pylypenko, A. (2019). Outsourcing of Accounting Services: Consideration of Contractual Aspects. Scientific Bulletin of the National Academy of Statistics, Accounting and Audit. 30-39. 10.31767/nasoa.3.2019.03.

128. Radchenko, M. A. (2015). Osoblyvosti vidobrazhennia elektronnykh hroshei v obliku [Features of the reflection of electronic money in accounting]. Naukovyi visnyk Uzhhorodskoho universytetu. Seriia : Ekonomika – Scientific Bulletin of Uzhgorod National University. Series: Economics, Issue 1(2). 121-124.

129. Rajput, B. (2020). Exploring the Phenomenon of Cyber Economic Crime. Cyber Economic Crime in India. 53-78. 10.1007/978-3-030-44655-0_4.

130. Rasche, A. & Esser, D. (2006). From Stakeholder Management to Stakeholder Accountability. Journal of Business Ethics. 65. 251-267. 10.1007/s10551-005-5355-y.

131. Revenok V.I., Mamchur O.S. Osnovni aspekty informatsiinykh system z obliku narakhuvannia zarobitnoi platy [The main aspects of information systems for payroll accounting]. Molodyi vchenyi – A young scientist. 2015. № 2 (17). 22-25.

132. Rındasu, S.M. (2019). Blockchain in accounting: trick or treat?, Quality Access to Success, Vol. 20 No. 170, 143-147.

133. Risk committees. The Institute of Chartered Accountants in England and Wales. Retrived from:

https://www.icaew.com/technical/corporate-governance/committees/risk-committees.

134. Rodrigues, B., Franco, M., Parangi, G. & Stiller, B. (2019). SEConomy: A Framework for the Economic Assessment of Cybersecurity. Economics of Grids, Clouds, Systems, and Services, 16th International Conference, GECON 2019, Leeds, UK, September 17–19, 2019. 154-166. 10.1007/978-3-030-36027-6_13.

135. Rohan, Rohani, Funilkul, Suree, Pal, Debajyoti & Thapliyal, Himanshu. (2021). Humans in the Loop: Cybersecurity Aspects in the Consumer IoT Context. IEEE Consumer Electronics Magazine. 99. 1-10. 10.1109/MCE.2021.3095385.

136. 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.

137. 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.

138. Rue, R., Pfleeger, S. (2009). Making the Best Use of Cybersecurity Economic Models. Security & Privacy, IEEE. 7. 52 - 60. 10.1109/MSP.2009.98.

139. Sakharov, P.O. (2017). Okremi aspekty obliku elektronnykh hroshei ta osoblyvosti provedennia yikh analizu ta audytu u bankakh [Some aspects of electronic money accounting and features of their analysis and audit in banks]. Mukachivskyi derzhavnyi universytet – Mukachevo state university, 9. 1192-1197.

140. Samudrage, D. & Jayewardene, D. (2019). Post-Implementation Benefits and Challenges of the Balanced Scorecard: Evidence from the

Finance and Accounting Outsourcing Sector. 10. 86-99. 10.7176/RJFA/10-22-10.

141. Sarkar, S. (2018). Blockchain accounting the disruption ahead, The Management Accountant Journal, Vol. 6, 73-78.

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

143. Schaffner, Georg, Grove, Laura, Holder, Anthony Hugh & Mac, Clouse. (2018). Cybersecurity Guidance for Accountants and Executives. Internal Auditing, Vol. 33, No. 5, 5-20.

144. Schmitt, Michael. (2012). Classification of Cyber Conflict. Journal of Conflict and Security Law. 17 (2). 245-260. 10.1093/jcsl/krs018.

145. Schmitz, J., Leoni, G. (2019). Accounting and auditing at the time of Blockchain technology: a research agenda, The Management Accountant Journal, Vol. 29 No. 2, 331-342, doi: 10.1111/auar.12286.

146. Sectoral thematic threat analysis ETL2020. (2020). ENISA Threat Landscape. European Union Agency for Cybersecurity. URL : https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis/at_download/fullReport. doi: 10.2824/552242.

147. Semenyshena, N., Khorunzhak, N. & Sadovska, I. Evaluation of the Adaptability of the Scientific Theories for the Development of Accounting Institute. Intellectual Economics. 2020. 14(1). P.114-129. 10.13165/IE-2014-1-07.

148. Semenyshena, N., Sysiuk, S., Shevchuk, K., Petruk, I., Benko, I. (2020). Institutionalism in Accounting: a Requirement of the Times or a Mechanism of Social Pressure? Independent Journal of Management & Production, 11(9), 2516-2541. doi: http://dx.doi.org/10.14807/ijmp.v11i9.1440.

149. 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.

150. Shchyrska, A. Yu. (2018). Vymohy korystuvachiv do yakosti oblikovoi informatsii [User requirements for the quality of accounting information]. Ekonomichnyi prostir. – Economic space. № 139. 213-228.

151. Sheehan, Barry, Murphy, Finbarr, Kia, Arash & Kiely, Ronan. (2021). A quantitative bow-tie cyber risk classification and assessment framework. Journal of Risk Research. 1-20. 10.1080/13669877.2021.1900337.

152. Sheldon, M.D. (2018). Using Blockchain to aggregate and share misconduct issues across the accounting profession, Current Issues in Auditing, Vol. 12 No. 2, 27-35, doi: 10.2308/ciia-52184.

153. Shevchuk, O., Desyatnyuk, O., Voitseshyn, V., Bryk, M. & Muravskyi, V. (2020). Control and Accounting of the Transportation Services Self-cost using GPS. 631-634. 10.1109/ACIT49673.2020.9208973.

154. Shitova, Yu. & Shitov, Y. (2019). Contemporary Trends in Economic Cybersecurity. The world of new economy. 13. 22-30. 10.26794/2220-6469-2019-13-4-22-30.

155. 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.

156. Shyshkova, N. L. (2016). Zasoby pidvyshchennia kerovanosti bezpekoiu oblikovoi informatsii [Means to improve the security of accounting information]. Ekonomichnyi visnyk Natsionalnoho hirnychoho universytetu – Economic Journal of the National Mining University. № 3. 119-127. URL: http://nbuv.gov.ua/UJRN/evngu_2016_3_17.

157. Šikanjić, Nedeljko, Avramović, Zoran & Marinković, Dražen. (2021). Cybersecurity IoT Architecture: One Proposed Solution for the

Security Risks and Threats. The 1st International Conference on Maritime Education and Development. pp.325-331. 10.1007/978-3-030-64088-0_29.

158. Sinha, S. (2020). Blockchain – opportunities and challenges for accounting professionals, Journal of Corporate Accounting and Finance, Vol. 31, 65-67, 10.1002/jcaf.22430.

159. Sinno, S. & Hawley, C. (2020). How biometrics can save companies from 'fire and forget'. Biometric Technology Today, 7, 5-8. doi: 10.1016/S0969-4765(20)30095-3.

160. Siriwardhana, Y., Porambage, P., Liyanage, M. & Ylianttila, M. (2021). AI and 6G Security: Opportunities and Challenges. Joint European Conference on Networks and Communications (EuCNC) & 6G Summit. Porto, Portugal. https://www.researchgate.net/publication/350824466_AI_and_6G_Security_Opportunities_and_Challenges

161. Size of the Internet of Things (IoT) security market worldwide from 2016 to 2025. Statista. URL: https://www.statista.com/statistics/993789/worldwide-internet-of-things-security-market-size/

162. Smith, E. (2020). How will IoT benefit the accounting profession? Retrieved from https://www.itproportal.com/features/how-will-iotbenefit-the-accounting-profession.

163. Smith, Kane, Dhillon, Gurpreet & Carter, Lemuria. (2021). User values and the development of a cybersecurity public policy for the IoT. International Journal of Information Management. 56. 10.1016/j.ijinfomgt.2020.102123.

164. Sofiah, Aman, A., Maelah, R., Amiruddin, R. & Hamzah, N. (2013). Management control in accounting outsourcing services. Business Strategy Series. 14. 43-49. 10.1108/17515631311325097.

165. Spitters, Thomas & Heaton, CPA (2019). A Supplement to Cybersecurity Breviary for Accountants Kindle Edition. Baume Verlag, San Francisco. 61 p.

166. Steingartner, William & Galinec, Darko. (2021). Cyber Threats and Cyber Deception in Hybrid Warfare. Acta Polytechnica Hungarica. 18. 25-45. 10.12700/APH.18.3.2021.3.2.

167. Stitilis, D., Rotomskis, I., Laurinaitis, M., Nadvynychnyy, S., Khorunzhak, N. (2020). National Cybersecurity Strategies: Management, Unification and Assessment. Independent Journal of Management & Production. 11 (9). 2341-2354. 10.14807/ijmp.v11i9.1431.

168. Strupczewski, Grzegorz. (2021). Defining cyber risk. Safety Science. 6. 135. 10.1016/j.ssci.2020.105143.

169. Summary Report / Telstra Security Report 2019 (2019). Paddington : Telstra Corporation Limited. 19 p.

170. Sun, Zhenjun, Li, Qi, Liu, Yunfan & Zhu, Yuhao. (2021). Opportunities and Challenges for Biometrics. China's e-Science Blue Book 2020, 101-125. doi: 10.1007/978-981-15-8342-1_6.

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

172. Systema obliku robochoho chasu «STOP-Time 4.0» [Working time accounting system "STOP-Time 4.0"]. (2016). K.:TOV «Kard-Sistems». 62 p.

173. Tan, B.S., Low, K.Y. (2019). Blockchain as the database engine in the accounting system, Australian Accounting Review, Vol. 29 No. 2, 312-318, 10.1111/auar.12278.

174. The 2019 Kearney Global Services Location Index. (2020). Digital resonance: the new factor influencing location attractiveness. URL: https://www.kearney.com/digital-transformation/gsli/2019-full-report.

175. Tiron Tudor, A., Deliu, D., Farcane, N., Donțu, A. (2021). Managing change with and through blockchain in accountancy organizations:

a systematic literature review. Journal of Organizational Change Management. ahead-of-print. 10.1108/JOCM-10-2020-0302.

176. Tsimperidis, Ioannis, Yucel, Cagatay, Katos, Vasilios. (2021). Age and Gender as Cyber Attribution Features in Keystroke Dynamic-Based User Classification Processes. Electronics. 10. 835. 10.3390/electronics10070835.

177. Value of cryptocurrency theft worldwide from 2016 to 2020. Statista. https://www.statista.com/statistics/960226/theft-of-cryptocurrency-value/

178. Viter, S. A., Svitlyshyn, I. I. (2017). Zakhyst oblikovoi informatsii ta kiberbezpeka pidpryiemstva [Protection of accounting information and cybersecurity of the enterprise]. Ekonomika ta suspilstvo : elektronne naukove fakhove vydannia – Economy and society: electronic scientific professional publication. 11. 497–502.

179. Volosovych, S., Klapkiv, L. (2018). Determinanty vynyknennia ta realizatsii kiberryzykiv [Determinants of the origin and implementation of cyber risks]. Zovnishnia torhivlia: ekonomika, finansy, pravo – Foreign trade: economics, finance, law. 3. 101–115. URL: http://nbuv.gov.ua/UJRN/uazt_2018_3_10.

180. Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S. & Zhou, W. (2020). Security and privacy in 6G networks: New areas and new challenges. Digital Communications and Networks. 6. 10.1016/j.dcan.2020.07.003.

181. Wilson, K., Hugh J. (2014). Cybersecurity Economics: How Much Cybersecurity is Enough?. Australian intellectual property journal. 7-9.

182. World Digital Competitiveness Ranking IMD 2018. https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2018.

183. Worldwide spending on blockchain solutions from 2017 to 2025. Statista. https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/

184. Wu, J., Xiong, F., Li, C. (2019). Application of internet of Things and blockchain technologies toimprove accounting, IEEE Access, Vol. 20, 1-10, 10.1109/ACCESS.2019.2930637.

185. Yak pysaty i vymovliaty bitcoin [How to write and pronounce bitcoin]. (2021). Available at https://www.bbc.com/ukrainian/blog-olexandr-ponomariv-41225133.

186. Yanchev, A.V. (2015). Elektronnyi oblik pratsi ta yii oplaty – osnova derzhavnoi stratehii formuvannia liudskoho kapitalu [Electronic accounting of labor and its payment is the basis of the state strategy of human capital formation]. Visny`k XNAU im. V.V. Dokuchayeva – Bulletin of KNAU named after V.V. Dokuchaev, 2. 212-221.

187. Yatsyk, T.V. (2017). Metodyka finansovoho obliku kryptovaliuty yak osoblyvoho vydu elektronnykh hroshei [Methods of financial accounting of cryptocurrency as a special type of electronic money]. Molodyi vchenyi – Young scientist, 2 (42). 349–354.

188. 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 – Herald of ZhSTU. 3 (57). 46-50.

189. Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., & Oppermann I., (Eds.). (2020). 6G White Paper: Research Challenges For Trust, Security And Privacy [White paper]. (6G Research Visions, No. 9). University of Oulu. http://urn.fi/urn:isbn:9789526226804.

190. Zadorozhny, Z., Muravskyi, V. V., Shevchuk, O. A., Sudyn, Y. A. (2018). Management accounting of the settlements with contractors in

innovative environment of business communications. Marketing and Management of Innovations, 2, 103-112. 10.21272/mmi.2018.2-09.

191. Zadorozhnyi, Z. -M., Muravskyi, V. and Muravskyi, V. (2021). Combined Outsourcing of Accounting and Cybersecurity Authorities, 11th International Conference on Advanced Computer Information Technologies (ACIT). 544-547. https://doi.org/10.1109/ACIT52158.2021.9548649.

192. Zadorozhnyi, Z. -M., Muravskyi, V. and Shevchuk, O. (2021). Influence of Organizational Factors and Forms of Accounting Outsourcing on Enterprise Cybersecurity. 11th International Conference on Advanced Computer Information Technologies (ACIT). 540-543. https://doi.org/10.1109/ACIT52158.2021.9548370.

193. Zadorozhnyi, Z.-M., Muravskyi, V. (2020) Analysis of the implementation efficiency of the new computer-communication form of accounting. ACIT'2020: 10th International Conference on Advanced Computer Information Technologies. Deggendorf, Germany, September 16-18. 718-721. https://doi.org/10.1109/ACIT49673.2020.9208973.

194. Zadorozhnyi, Z. V., Muravskyi, V. V., Sudyn, Yu. A. Goodwill assessment in enterprise management: innovative approaches using computer and communication technologies. Marketing and management of innovation. 2018. 4. 43-53. http://doi.org/10.21272/mmi.2018.4-04.

195. Zadorozhnyi, Z., Muravskyi, V., & Shevchuk, O. (2018) Management accounting of electronic transactions with the use of cryptocurrencies. Financial And Credit Activity: Problems Of Theory And Practice, 3(26), 169-177. doi: 10.18371/fcaptp.v3i26.144368

196. Zadorozhnyi, Z., Muravskyi, V., Shevchuk, O. & 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. 10.18371/fcaptp.v3i34.215462.

197. Zadorozhnyi, Z.-M., Muravskyi, V., Pochynok, N., & Hrytsyshyn, A. (2020). Innovation Management and Automated Accounting

in the Chaotic Storage Logistics. Marketing and Management of Innovations, 2, 313-323. http://doi.org/10.21272/mmi.2020.2-23.

198. Zadorozhnyi, Z.-M., Ometsinska, I., & Muravskiy, V. (2021). Determinants of Firm's Innovation: Increasing the Transparency of Financial Statements. Marketing and Management of Innovations, 2, 74-86. http://doi.org/10.21272/mmi.2021.2-06.

199. Zadorozhnyy, Z.-M., Muravskiy, V., Yatsyshyn, S., & Shevchuk, O. (2021). Accounting of wages with the use of biometrics to ensure cybersecurity of enterprises. Financial and Credit Activity: Problems of Theory and Practice, 3(38), 162–172. https://doi.org/10.18371/fcaptp.v3i38.237446.

200. Zhang, J., Wang, Z., Wang, D., Zhang, X., Gupta, B B., Liu, X. & Ma, J. (2021). A Secure Decentralized Spatial Crowdsourcing Scheme for 6G-Enabled Network in Box. IEEE Transactions on Industrial Informatics. 1-11. 10.1109/TII.2021.3081416.

201. Zinkevich, V., Shtatov, D. (2007). Informacionnye riski: analiz i kolichestvennaja ocenk [Information risks: analysis and quantitative assessment]. Buhgalterija i banki – Accounting and banks. 1. 50–55 [In Russian].

202. Zoidze, D. R. (2017). The Outsourcing and Peculiarities of Its Application in the Pharmaceutical Industry Sector. Business Inform. 5, 274–278.

SCIENTIFIC PUBLICATION

Volodymyr Muravskyi

ACCOUNTING AND CYBERSECURITY

Monograph

Format 60x84 1/16. Times New Roman
Offset paper. Duplicator printing.
Sent for printing – November 21, 2021
Order ASIN: 0578331837
Circulation 100 p.

Kindle Publishing, KDP
Box 81226 Seattle,
WA 98108-1226,
USA
2021